aws

Guida per gli sviluppatori

OpenSearch Servizio Amazon

OpenSearch Servizio Amazon: Guida per gli sviluppatori

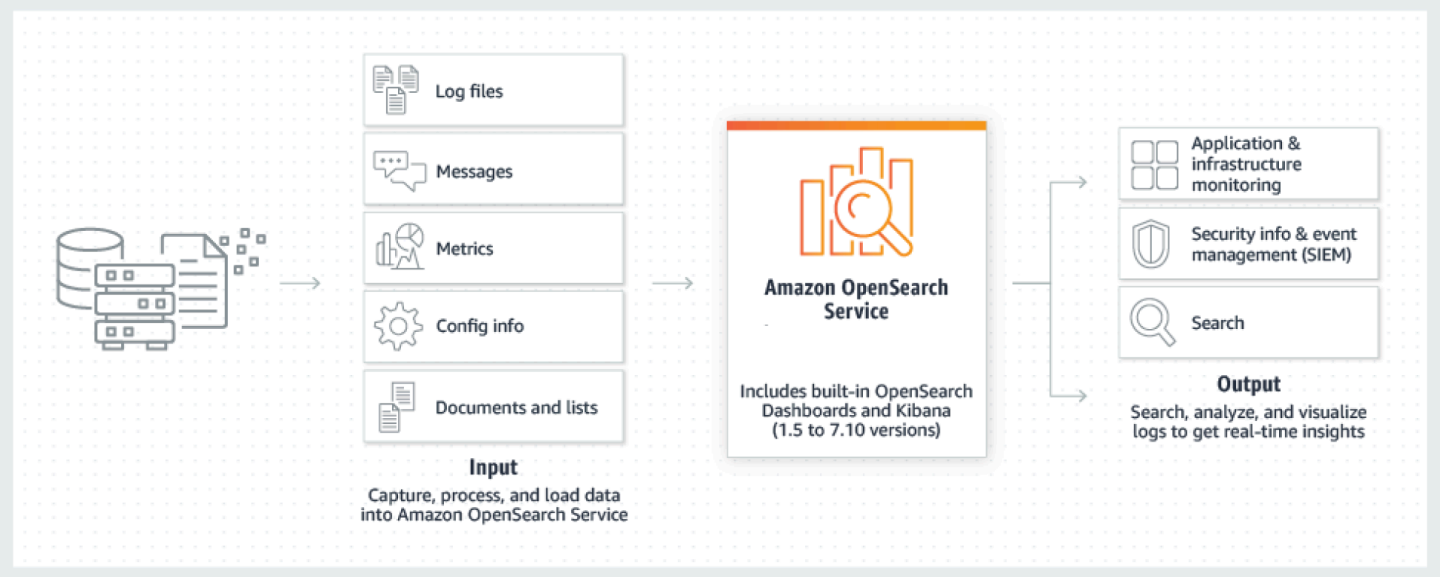
Table of Contents

Che cos'è Amazon OpenSearch Service?

Amazon OpenSearch Service è un servizio gestito che semplifica l'implementazione, il funzionamento e la scalabilità OpenSearch dei cluster nel AWS cloud. Amazon OpenSearch Service supporta OpenSearch un sistema operativo Elasticsearch legacy (fino alla versione 7.10, l'ultima versione open source del software). Quando si crea un cluster, è possibile scegliere il motore di ricerca da usare.

OpenSearchè un motore di ricerca e analisi completamente open source per casi d'uso come l'analisi dei log, il monitoraggio delle applicazioni in tempo reale e l'analisi dei clickstream. Per ulteriori informazioni, consulta la documentazione. OpenSearch

Amazon OpenSearch Service fornisce tutte le risorse per il OpenSearch cluster e lo avvia. Inoltre, rileva e sostituisce automaticamente i nodi di OpenSearch servizio guasti, riducendo il sovraccarico associato alle infrastrutture autogestite. Puoi dimensionare il cluster con un'unica chiamata API o con pochi clic nella console.



Per iniziare a utilizzare OpenSearch Service, è necessario creare un dominio di OpenSearch servizio, equivalente a un cluster. OpenSearch Ogni istanza EC2 nel cluster funge da unico nodo OpenSearch di servizio.

Puoi utilizzare la console OpenSearch di servizio per configurare e configurare un dominio in pochi minuti. Se preferisci l'accesso programmatico, puoi utilizzare gli AWS CLIAWSSDK o Terraform.

Caratteristiche di Amazon OpenSearch Service

OpenSearch Il servizio include le seguenti funzionalità:

Dimensionamento

- Numerose configurazioni di CPU, memoria e capacità di archiviazione, note come tipi di istanza, comprese le istanze Graviton a costi ridotti
- Fino a 3 PB di spazio di archiviazione collegato
- Archiviazione a freddo UltraWarmed economica per dati di sola lettura

Sicurezza

- AWS Identity and Access Management (IAM) controllo degli accessi
- Semplice integrazione con Amazon VPC e i gruppi di sicurezza VPC
- Crittografia dei dati inattivi e node-to-node crittografia
- Autenticazione Amazon Cognito, HTTP basic o SAML per dashboard OpenSearch
- Sicurezza a livello di indice, a livello di documento e a livello di campo
- Log di verifica
- Multi-tenancy di Dashboards

Stabilità

- Più posizioni geografiche per le risorse, note come regioni e zone di disponibilità
- Allocazione dei nodi su due o tre zone di disponibilità nella stessa AWS regione, nota come Multi-AZ
- Nodi master dedicati per l'offload delle attività di gestione del cluster
- Istantanee automatizzate per il backup e il ripristino dei domini di servizio OpenSearch

Flessibilità

- Supporto SQL per l'integrazione con applicazioni di Business Intelligence (BI)
- Pacchetti personalizzati per migliorare i risultati della ricerca

Integrazione con i servizi più diffusi

- Visualizzazione dei dati tramite dashboard OpenSearch
- Integrazione con Amazon CloudWatch per il monitoraggio delle metriche OpenSearch del dominio del servizio e l'impostazione degli allarmi
- Integrazione con AWS CloudTrail per il controllo delle chiamate API di configurazione ai domini di servizio OpenSearch
- Integrazione con Amazon S3, Amazon Kinesis e Amazon DynamoDB per caricare dati di streaming in Service OpenSearch
- Avvisi da Amazon SNS quando i dati superano determinate soglie

Quando utilizzare OpenSearch rispetto ad Amazon Service OpenSearch

Utilizza la tabella seguente per decidere se il OpenSearch servizio Amazon fornito o gestito in modo automatico OpenSearch è la scelta giusta per te.

OpenSearch	OpenSearch Servizio Amazon
• La tua organizzazione è disposta a monitorare e gestire manualmen te i cluster forniti autonomamente e dispone di persone con le competenze adeguate. • Desiderate il controllo completo a livello di compilazione del codice. • La tua organizzazione preferisce, o utilizza esclusivamente, il software open source. • Hai una strategia multi-cloud, che richiede tecnologie che non sono specifiche del fornitore. • Il tuo team è in grado di risolvere qualsiasi problema critico di produzion e.	• Non vuoi gestire, monitorare e mantenere manualmente la tua infrastruttura. • Desideri modi semplici per gestire i crescenti costi di analisi distribuendo i dati su più livelli di storage, sfruttando la durabilità e il basso costo di Amazon S3. • Vuoi sfruttare le integrazioni con altri sistemi Servizi AWS come DynamoDB, Amazon DocumentDB (con compatibilità MongoDB), IAM e. CloudWatch CloudFormation • Desideri accedere facilmente all'assistenza fornita per la manutenzione preventiva e durante i AWS Support problemi di produzione. • Desiderate sfruttare funzionalità come la riparazio ne automatica, la manutenzione proattiva, la resilienza e i backup.

OpenSearch	OpenSearch Servizio Amazon
• Desiderate la flessibilità necessaria per utilizzare, modificare ed estendere il prodotto come preferite. • Desideri accedere immediatamente alle nuove funzionalità non appena vengono rilasciate.	

Amazon OpenSearch Serverless

Amazon OpenSearch Serverless è una configurazione serverless su richiesta, con scalabilità automatica per Amazon Service. OpenSearch Serverless rimuove le complessità operative legate al provisioning, alla configurazione e all'ottimizzazione dei cluster. OpenSearch Per ulteriori informazioni, consulta Amazon OpenSearch Serverless.

OpenSearch Ingestione di Amazon

Amazon OpenSearch Ingestion è un raccoglitore di dati completamente gestito, basato su Data Prepper, che fornisce dati di log and trace in tempo reale ai domini di Amazon OpenSearch Service e alle raccolte Serverless. OpenSearch Consente di filtrare, arricchire, trasformare, normalizzare e aggregare i dati per l'analisi e la visualizzazione a valle. Per ulteriori informazioni, consulta Amazon OpenSearch Ingestion.

Versioni supportate di OpenSearch Elasticsearch

OpenSearch Il servizio attualmente supporta le seguenti versioni: OpenSearch

- 2.13, 2.11, 2.9, 2.7, 2.5, 2.3, 1.3, 1.2, 1.1, 1.0

OpenSearch Il servizio supporta anche le seguenti versioni precedenti di 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

Per ulteriori informazioni, consultare the section called “Operazioni supportate”, the section called “Funzionalità per versione di motore” e the section called “Plug-in per versione motore”.

Se si avvia un nuovo progetto di OpenSearch assistenza, si consiglia vivamente di scegliere l'ultima versione supportata. OpenSearch Se un dominio esistente usa una versione di Elasticsearch meno recente, è possibile decidere di mantenere il dominio o migrare i dati. Per ulteriori informazioni, consulta the section called “Aggiornamento dei domini”.

Prezzi per Amazon OpenSearch Service

Per il OpenSearch servizio, paghi per ogni ora di utilizzo di un'istanza EC2 e per la dimensione cumulativa di tutti i volumi di storage EBS collegati alle tue istanze. Si applicano anche le tariffe standard per il trasferimento AWS dei dati.

Tuttavia, esistono alcune eccezioni di trasferimento dati notevoli. Se un dominio utilizza più zone di disponibilità, il OpenSearch servizio non fattura il traffico tra le zone di disponibilità. Un significativo trasferimento di dati avviene all'interno di un dominio durante l'allocazione e il ribilanciamento degli shard. OpenSearch Non servono né contatori né bollette per questo traffico. Allo stesso modo, il OpenSearch Servizio non fattura il trasferimento di dati tra UltraWarm/cold nodes e Amazon S3.

Per i dettagli completi sui prezzi, consulta i prezzi OpenSearch di Amazon Service. Per informazioni sui costi addebitati durante le modifiche di configurazione, consulta the section called “Costi per le modifiche di configurazione”.

Guida introduttiva ad Amazon OpenSearch Service

Per iniziare, registrarsi per ottenere un Account AWS se non ne è già disponibile uno. Dopo aver configurato un account, completa il tutorial introduttivo per Amazon OpenSearch Service. Per ulteriori informazioni mentre apprendi come usare il servizio, consulta gli argomenti introduttivi seguenti:

- Creare un dominio
- Dimensionare il dominio in modo appropriato per il carico di lavoro.
- Controllare l'accesso al dominio utilizzando una policy di accesso al dominio o un controllo granulare degli accessi
- Indicizza i dati manualmente o da altri AWS servizi

- Usa OpenSearch le dashboard per cercare i dati e creare visualizzazioni

Per informazioni sulla migrazione a OpenSearch Service da un cluster OpenSearch autogestito, consulta. the section called “Migrazione aOpenSearchServizio”

Servizi correlati

OpenSearch Il servizio viene comunemente utilizzato con i seguenti servizi:

Amazon CloudWatch

OpenSearch I domini di servizio inviano automaticamente le metriche a CloudWatch in modo da poter monitorare lo stato e le prestazioni del dominio. Per ulteriori informazioni, consulta Monitoraggio delle metriche dei OpenSearch cluster con Amazon CloudWatch.

CloudWatch I log possono anche andare nella direzione opposta. È possibile configurare CloudWatch i registri per lo streaming dei dati al OpenSearch Servizio per l'analisi. Per ulteriori informazioni, consulta the section called “Caricamento di dati di streaming da Amazon CloudWatch”.

AWS CloudTrail

Utilizzalo AWS CloudTrail per ottenere una cronologia delle chiamate all'API di configurazione del OpenSearch servizio e degli eventi correlati per il tuo account. Per ulteriori informazioni, consulta Monaggio delle chiamate API Amazon OpenSearch Service con AWS CloudTrail.

Amazon Kinesis

Kinesis è un servizio gestito per l'elaborazione in tempo reale dei dati di streaming su vasta scala. Per ulteriori informazioni, consultare the section called “Caricamento dei dati in streaming in Amazon Kinesis Data Streams” e the section called “Caricamento di dati di streaming da Amazon Data Firehose”.

Amazon S3

Amazon Simple Storage Service (Amazon S3) è un servizio di archiviazione su Internet. Questa guida fornisce il codice di esempio Lambda per l'integrazione con Amazon S3. Per ulteriori informazioni, consultare the section called “Caricamento di dati in streaming da Amazon S3”.

AWS IAM

AWS Identity and Access Management (IAM) è un servizio web che puoi utilizzare per gestire l'accesso ai tuoi domini OpenSearch di servizio. Per ulteriori informazioni, consulta the section called “Identity and Access Management”.

AWS Lambda

AWS Lambda è un servizio di elaborazione che consente di eseguire codice senza effettuare il provisioning o la gestione di server. Questa guida fornisce il codice di esempio Lambda per lo streaming dei dati da DynamoDB, Amazon S3 e Kinesis. Per ulteriori informazioni, consultare the section called “Caricamento di dati di streaming in OpenSearch Service”.

Amazon DynamoDB

Amazon DynamoDB è un servizio di database NoSQL interamente gestito che combina prestazioni elevate e prevedibili con una scalabilità ottimale. Per ulteriori informazioni sullo streaming di dati su OpenSearch Service, consulta. the section called “Caricamento di dati in streaming da una tabella Amazon DynamoDB”

Amazon QuickSight

Puoi visualizzare i dati di OpenSearch Service utilizzando i QuickSight dashboard di Amazon. Per ulteriori informazioni, consulta Using Amazon OpenSearch Service with Amazon QuickSight nella Amazon QuickSight User Guide.

> **Note**
>
> OpenSearch include alcuni codici Elasticsearch con licenza Apache di Elasticsearch B.V. e altro codice sorgente. Elasticsearch B.V. non è la fonte di quell'altro codice sorgente. ELASTICSEARCH è un marchio registrato di Elasticsearch B.V.

Configurazione di Amazon OpenSearch Service

Argomenti

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

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

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

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

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

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

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

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

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

Accedi come utente con accesso amministrativo

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

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

Assegna l'accesso ad altri utenti

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

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

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

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Concessione delle autorizzazioni

Negli ambienti di produzione, ti consigliamo di utilizzare politiche più dettagliate. Per ulteriori informazioni sulla gestione degli accessi, consulta Access management for AWS resources nella IAM User Guide.

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

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

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

Concessione dell'accesso programmatico

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

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

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface • Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in Uso delle credenziali temporanee con AWS risorse nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimen

Quale utente necessita dell'accesso programmatico?	Per	Come
		to agli SDK e agli AWS strumenti. • Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Installa e configura il AWS CLI

Se desideri utilizzare le API OpenSearch di servizio, devi installare la versione più recente di AWS Command Line Interface (AWS CLI). Non è necessario AWS CLI utilizzare il OpenSearch servizio dalla console e puoi iniziare senza la CLI seguendo la procedura riportata di seguito. Guida introduttiva ad AmazonOpenSearchServizio

Per configurare il AWS CLI

1. Per installare la versione più recente di AWS CLI per macOS, Linux o Windows, vedi Installazione o aggiornamento della versione più recente di. AWS CLI
2. Per configurare AWS CLI la configurazione sicura dell'accesso a Servizi AWS, incluso il OpenSearch servizio, vedi Configurazione rapida con `aws configure`.
3. Per verificare la configurazione, immettete il seguente DataBrew comando al prompt dei comandi.

   ```
   aws opensearch help
   ```

   AWS CLI i comandi utilizzano l'impostazione predefinita Regione AWS della configurazione, a meno che non venga impostata con un parametro o un profilo. Per impostare Regione AWS un parametro, è possibile aggiungere il `--region` parametro a ciascun comando.

   Per impostare Regione AWS un profilo, aggiungi prima un profilo denominato nel `~/.aws/config` file o nel `%UserProfile%/.aws/config` file (per Microsoft Windows). Segui la procedura descritta in Profili denominati per AWS CLI. Successivamente, imposta le tue Regione AWS e le altre impostazioni con un comando simile a quello illustrato nell'esempio seguente.

```
[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
```

Aprire la console

La maggior parte degli argomenti relativi alla console di questa sezione inizia dalla console di OpenSearch servizio. Se non hai già effettuato l'accesso al tuo Account AWS, accedi, quindi apri la console di OpenSearch servizio e passa alla sezione successiva per continuare a usare Service. OpenSearch

Guida introduttiva ad AmazonOpenSearchServizio

Questo tutorial ti mostra come usare AmazonOpenSearchServizio per creare e configurare un dominio di test. UnOpenSearchIl dominio di servizio è sinonimo diOpenSearchgrappolo. I domini sono cluster con le impostazioni, i tipi di istanza, il numero di istanze e le risorse di archiviazione specificate.

Questo tutorial ti guida attraverso i passaggi di base per ottenere unOpenSearchDominio di servizio attivo e funzionante rapidamente. Per informazioni più dettagliate, consulta Creazione e gestione dei domini e altri argomenti all'interno di questa guida. Per informazioni sulla migrazione aOpenSearchServizio fornito da un sistema autogestitoOpenSearchcluster, vedithe section called "Migrazione aOpenSearchServizio".

Puoi completare i passaggi di questo tutorial utilizzando ilOpenSearchConsole di servizio,AWS CLI, o ilAWSSDK. Per ulteriori informazioni sull'installazione e la configurazione di AWS CLI, consultare la Guida per l'utente di AWS Command Line Interface.

Fase 1: Crea un AmazonOpenSearchDominio del servizio

> **Important**
>
> Questo è un breve tutorial per configurare untestAmazonOpenSearchDominio del servizio. Non utilizzare questo processo per creare domini di produzione. Per una versione completa della stessa procedura, consulta Creazione e gestione dei domini.

UnOpenSearchIl dominio di servizio è sinonimo diOpenSearchgrappolo. I domini sono cluster con le impostazioni, i tipi di istanza, il numero di istanze e le risorse di archiviazione specificate. Puoi creare unOpenSearchDominio del servizio utilizzando la console,AWS CLI, o ilAWSSDK.

Per creare unOpenSearchDominio del servizio che utilizza la console

1. Passare all'indirizzo https://aws.amazon.com e scegliere Sign In to the Console (Accedi alla console).
2. Sottoanalitica, scegliAmazonOpenSearchServizio.
3. Scegli Crea dominio.

4. Specificare un nome per il dominio. Gli esempi di questo tutorial utilizzano il nome movies.
5. Per il metodo di creazione del dominio, scegliCreazione standard.

> **Note**
>
> Per configurare rapidamente un dominio di produzione con le migliori pratiche, puoi scegliereFacile da creare. Per lo sviluppo e il test di questo tutorial, useremoCreazione standard.

6. Per i modelli, scegliSviluppo/test.
7. Per l'opzione di distribuzione, scegliDominio con standby.
8. Per Versione, scegliere la versione più recente.
9. Per ora, ignora ilNodi dati,Archiviazione dati a caldo e a freddo,Nodi master dedicati,Configurazione delle istantanee, eEndpoint personalizzatosezioni.
10. Per semplicità in questo tutorial, viene utilizzato un dominio ad accesso pubblico. In Rete, scegli Accesso pubblico.
11. Nelle impostazioni di controllo degli accessi dettagliate, mantieni ilAbilita un controllo degli accessi granularecasella di controllo selezionata. SelezionaCrea utente principalee fornisci un nome utente e una password.
12. Per adesso, ignorare le sezioni Autenticazione SAML e Autenticazione Amazon Cognito.
13. Per Policy di accesso, scegli Utilizza solo controllo granulare degli accessi. In questa esercitazione, il controllo granulare degli accessi gestisce l'autenticazione, non la policy di accesso al dominio.
14. Ignora il resto delle impostazioni per il momento e scegli Crea. I nuovi domini richiedono in genere 15-30 minuti per l'inizializzazione, ma possono richiedere più tempo a seconda della configurazione. Dopo l'inizializzazione del dominio, selezionarlo per aprire il riquadro di configurazione. Annotare l'endpoint del dominio sotto Informazioni generali (ad esempio,`https://search-`*`my-domain`*`.us-east-1.es.amazonaws.com`), che potrai utilizzare nel prossimo passaggio.

Prossimo:Caricare i dati su unOpenSearchDominio di servizio per l'indicizzazione

Fase 2: Caricare i dati su AmazonOpenSearchServizio di indicizzazione

> **Important**
>
> Questo è un breve tutorial per caricare una piccola quantità di dati di test su AmazonOpenSearchServizio. Per ulteriori informazioni sul caricamento dei dati in un dominio di produzione, consultare Indicizzazione dei dati.

Puoi caricare i dati su unOpenSearchDominio del servizio che utilizza la riga di comando o la maggior parte dei linguaggi di programmazione.

Per brevità e comodità, le richieste di esempio seguenti utilizzano curl, un comune client HTTP. I client come curl non sono in grado di eseguire la firma della richiesta, necessaria se la policy d'accesso specifica utenti o ruoli IAM. Per completare correttamente questo processo, è necessario utilizzare un controllo di accesso granulare con un nome utente e una password primari come quelli configurati inFase 1.

È possibile installare curl su Windows e utilizzarlo dal prompt dei comandi, ma consigliamo di utilizzare uno strumento come Cygwin o Windows Subsystem for Linux. I sistemi macOS e la maggior parte delle distribuzioni Linux includono già curl.

Opzione 1: Caricamento di un singolo documento

Esegui il comando seguente per aggiungere un singolo documento al dominio movies:

```
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'
```

Nel comando, inserisci il nome utente e la password che hai creato inFase 1.

Per una spiegazione dettagliata di questo comando e di come effettuare richieste firmate aOpenSearchAssistenza, vediIndicizzazione dei dati.

Opzione 2: Caricamento di più documenti

Per caricare un file JSON che contiene più documenti su unOpenSearchDominio del servizio

1. Creare un file locale denominato `bulk_movies.json`. Copiare e incollare il seguente contenuto nel file e aggiungere un carattere newline finale:

```
{ "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. Eseguire il comando seguente nella directory locale in cui è memorizzato il file per caricarlo nel dominio movies:

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

Per ulteriori informazioni sul formato di file bulk, consulta Indicizzazione dei dati

Successivo: Ricerca di documenti

Fase 3: Cerca documenti in AmazonOpenSearchServizio

Per cercare documenti su AmazonOpenSearchDominio del servizio, usa ilOpenSearchAPI di ricerca. In alternativa, puoi usareOpenSearchPannelli di controlloper cercare documenti nel dominio.

Come eseguire la ricerca di documenti dalla riga di comando

Esegui il comando seguente per cercare la parola mars nel dominio movies:

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

Se nella pagina precedente hai utilizzato il blocco di dati, prova a cercare invece rebel.

Noterai una risposta simile alla seguente:

```
{
  "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!"
        }
      }
    ]
  }
}
```

Cerca documenti utilizzandoOpenSearchPannelli di controllo

OpenSearchDashboards è un popolare strumento di visualizzazione open source progettato per funzionare conOpenSearch. Fornisce un'interfaccia utente utile per cercare e monitorare gli indici.

Per cercare documenti da unOpenSearchDominio del servizio tramite dashboard

1. Accedere allaOpenSearchURL delle dashboard per il tuo dominio. Puoi trovare l'URL nella dashboard del dominio nelOpenSearchConsole di servizio. L'URL segue il seguente formato:

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

2. Accedi utilizzando il tuo nome utente e la password principali.
3. Per utilizzare Dashboards, è necessario creare almeno un modello di indice. Dashboards usa questi modelli per identificare gli indici da analizzare. Aprire il riquadro di spostamento a sinistra, scegliere Gestione stack, scegliere Modelli di indice, quindi scegliere Crea modello di indice. Per questo tutorial, digita movies.
4. Scegliere Fase successiva quindi selezionare Crea modello di indice. Dopo aver creato il modello, è possibile visualizzare i vari campi del documento, ad esempio `actor` e `director`.
5. Tornare alla pagina Modelli di indice e assicurarsi che `movies` sia impostato come valore di default. In caso contrario, seleziona il modello e scegli l'icona a forma di stella per renderlo predefinito.
6. Per iniziare a cercare i dati, aprire di nuovo il riquadro di spostamento a sinistra e scegliere Individua.

7. Nella barra di ricerca, inserire mars se è stato caricato un singolo documento oppure rebel se sono stati caricati più documenti, quindi premere Invio. È possibile provare a cercare altri termini, come i nomi di attori o registi.

Successivo: Eliminazione di un dominio

Fase 4: Eliminare un AmazonOpenSearchDominio del servizio

Poiché il dominio movies utilizzato in questo tutorial è solo a scopo di test, è consigliabile eliminarlo una volta terminate le prove in modo da evitare costi aggiuntivi.

Per eliminare unOpenSearchDominio di servizio dalla console

1. Accedi alAmazonOpenSearchServizioconsolle.
2. In Domini, seleziona il dominio movies.
3. Scegli Elimina e conferma l'eliminazione.

Fasi successive

Adesso che è chiaro come creare un dominio e i dati di indice, è possibile provare a completare alcuni degli esercizi seguenti:

- Scopri di più sulle opzioni avanzate per la creazione di un dominio. Per ulteriori informazioni, consultare Creazione e gestione dei domini.
- Scopri come gestire gli indici nel dominio. Per ulteriori informazioni, consulta Gestione degli indici.
- Prova uno dei tutorial per lavorare con AmazonOpenSearchServizio. Per ulteriori informazioni, consulta Tutorial.

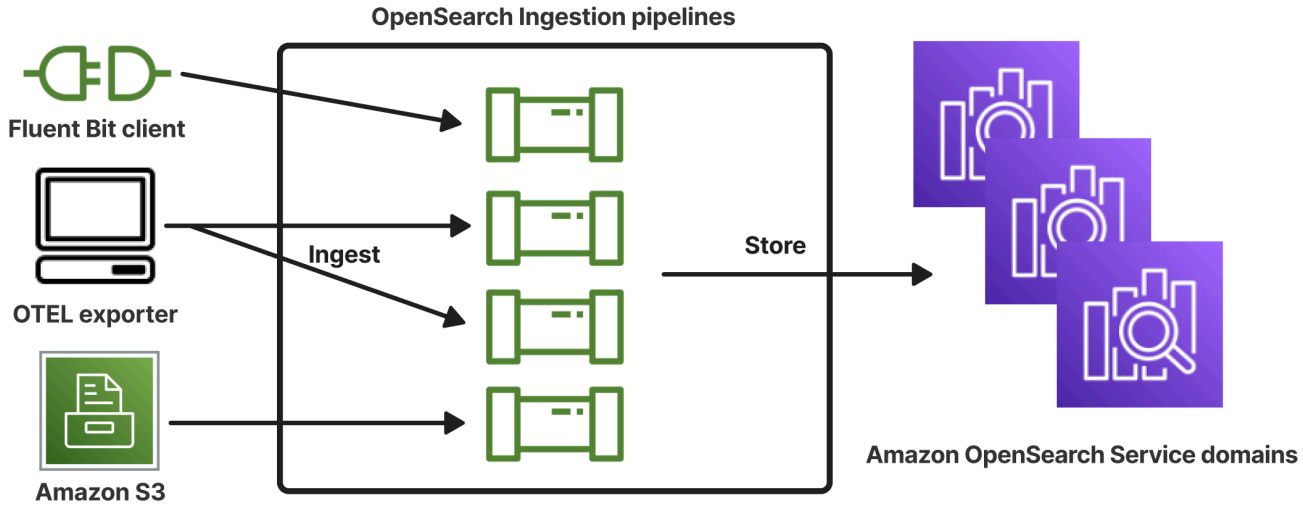
OpenSearch Ingestione di Amazon

Amazon OpenSearch Ingestion è un raccoglitore di dati serverless completamente gestito che fornisce dati di log, metrici e tracciamento in tempo reale ai domini di Amazon OpenSearch Service e alle raccolte Serverless. OpenSearch

Con OpenSearch Ingestion, non è più necessario utilizzare soluzioni di terze parti come Logstash o Jaeger per inserire dati nei domini di servizio e nelle raccolte Serverless. OpenSearch OpenSearch Configurate i vostri produttori di dati per inviare dati a Ingestion. OpenSearch Quindi, invia automaticamente i dati al dominio o alla raccolta specificati. Puoi anche configurare OpenSearch Ingestion per trasformare i tuoi dati prima di consegnarli.

Inoltre, con OpenSearch Ingestion, non è necessario preoccuparsi del provisioning dei server, della gestione e dell'applicazione di patch al software o della scalabilità del cluster di server. Effettuate il provisioning delle pipeline di importazione direttamente all'interno di e Ingestion si occupa della AWS Management Console loro gestione e OpenSearch scalabilità.

OpenSearch Ingestion è un sottoinsieme di Amazon Service. OpenSearch È alimentato da Data Prepper, un raccoglitore di dati open source in grado di filtrare, arricchire, trasformare, normalizzare e aggregare i dati per l'analisi e la visualizzazione a valle.



Argomenti

- Concetti chiave
- Vantaggi dell'ingestione OpenSearch
- Limitazioni
- Versioni di Data Prepper supportate

- Scalabilità delle pipeline
- OpenSearch Prezzi di ingestione
- Supportato Regioni AWS
- OpenSearch Quote di ingestione
- Configurazione di ruoli e utenti in Amazon OpenSearch Ingestion
- Guida introduttiva ad Amazon OpenSearch Ingestion
- Panoramica delle funzionalità della pipeline in Amazon Ingestion OpenSearch
- Creazione di pipeline Amazon OpenSearch Ingestion
- Visualizzazione delle pipeline OpenSearch di Amazon Ingestion
- Aggiornamento delle pipeline di Amazon OpenSearch Ingestion
- Interruzione e avvio delle pipeline di Amazon OpenSearch Ingestion
- Eliminazione delle pipeline di Amazon OpenSearch Ingestion
- Plugin e opzioni supportati per le pipeline di Amazon OpenSearch Ingestion
- Utilizzo delle integrazioni della OpenSearch pipeline di Amazon Ingestion
- Migrazione dei dati tra domini e raccolte utilizzando Amazon Ingestion OpenSearch
- Utilizzo degli AWS SDK per interagire con Amazon Ingestion OpenSearch
- Sicurezza in Amazon OpenSearch Ingestion
- Etichettatura delle pipeline di Amazon OpenSearch Ingestion
- Registrazione e monitoraggio di Amazon OpenSearch Ingestion con Amazon CloudWatch
- Le migliori pratiche per Amazon OpenSearch Ingestion

Concetti chiave

Quando iniziate a usare OpenSearch Ingestion, potete trarre vantaggio dalla comprensione dei seguenti concetti:

Pipeline

> Dal punto di vista OpenSearch dell'ingestione, una pipeline si riferisce a un unico raccoglitore di dati fornito che viene creato all'interno di Service. OpenSearch Puoi considerarlo come l'intero file di configurazione YAML, che include una o più pipeline secondarie. Per i passaggi per creare una pipeline di ingestione, consulta. the section called “Creazione di pipeline”

Sotto-pipeline

Le sotto-pipeline vengono definite all'interno di un file di configurazione YAML. Ogni sub-pipeline è una combinazione di una sorgente, un buffer, zero o più processori e uno o più sink. È possibile definire più sotto-pipeline in un unico file YAML, ognuna con sorgenti, processori e sink unici. Per facilitare il monitoraggio con CloudWatch e altri servizi, ti consigliamo di specificare un nome di pipeline diverso da tutte le relative pipeline secondarie.

Puoi mettere insieme più subpipeline all'interno di un singolo file YAML, in modo che l'origine di una sottopipeline sia un'altra sottopipeline e il relativo sink sia una terza sottopipeline. Per vedere un esempio, consulta the section called “OpenTelemetry Collezionista”.

Origine

Il componente di input di una sottopipeline. Definisce il meccanismo attraverso il quale una pipeline consuma i record. La fonte può consumare gli eventi ricevendoli tramite HTTPS o leggendo da endpoint esterni come Amazon S3. Esistono due tipi di fonti: basate su push e basate su pull. Le fonti basate su push, come i log HTTP e OTel, trasmettono i record agli endpoint di ingestione. Le fonti basate su pull, come Otel trace e S3, estraggono i dati dalla fonte.

Processors

Unità di elaborazione intermedie in grado di filtrare, trasformare e arricchire i record nel formato desiderato prima di pubblicarli nel sink. Il processore è un componente opzionale di una pipeline. Se non si definisce un processore, i record vengono pubblicati nel formato definito nel codice sorgente. È possibile avere più di un processore. Una pipeline esegue i processori nell'ordine in cui vengono definiti dall'utente.

Sink

Il componente di output di una sottopipeline. Definisce una o più destinazioni in cui una sub-pipeline pubblica i record. OpenSearch Ingestion supporta OpenSearch i domini di servizio come sink. Supporta anche le condutture secondarie come sink. Ciò significa che è possibile mettere insieme più sotto-pipeline all'interno di una singola pipeline di OpenSearch ingestione (file YAML). I cluster OpenSearch autogestiti non sono supportati come sink.

Buffer

La parte del processore che funge da strato tra la sorgente e il sink. Non è possibile configurare manualmente un buffer all'interno della pipeline. OpenSearch L'ingestione utilizza una configurazione di buffer predefinita.

Route

La parte di un processore che consente agli autori della pipeline di inviare solo eventi che soddisfano determinate condizioni a diversi sink.

Una definizione di subpipeline valida deve contenere una fonte e un sink. Per ulteriori informazioni su ciascuno di questi elementi della pipeline, consultate il riferimento alla configurazione.

Vantaggi dell'ingestione OpenSearch

OpenSearch L'ingestione presenta i seguenti vantaggi principali:

- Elimina la necessità di gestire manualmente una pipeline autoalimentata.
- Ridimensiona automaticamente le pipeline in base ai limiti di capacità definiti dall'utente.
- Mantiene la pipeline aggiornata con patch di sicurezza e bug.
- Offre la possibilità di collegare le pipeline al cloud privato virtuale (VPC) per un ulteriore livello di sicurezza.
- Consente di interrompere e avviare le pipeline per controllare i costi.
- Fornisce modelli di configurazione delle pipeline per i casi d'uso più diffusi per aiutarvi a iniziare a lavorare più velocemente.
- Consente di interagire a livello di codice con le pipeline tramite i vari AWS SDK e l'API Ingestion. OpenSearch
- Supporta il monitoraggio delle prestazioni in Amazon CloudWatch e la registrazione degli errori nei CloudWatch log.

Limitazioni

OpenSearch Ingestion presenta le seguenti limitazioni:

- Puoi importare dati solo in domini con OpenSearch versione 1.0 o successiva oppure Elasticsearch 6.8 o versione successiva. Se utilizzi la fonte di traccia Otel, ti consigliamo di utilizzare Elasticsearch 7.9 o versione successiva in modo da poter utilizzare il plug-in Dashboards. OpenSearch
- Se una pipeline sta scrivendo su un dominio di OpenSearch servizio all'interno di un VPC, la pipeline deve essere creata nello Regione AWS stesso dominio.

- È possibile configurare solo una singola origine dati all'interno di una definizione di pipeline.
- Non è possibile specificare OpenSearch cluster autogestiti come sink.
- Non è possibile specificare un endpoint personalizzato come sink. Puoi comunque scrivere su un dominio con endpoint personalizzati abilitati, ma devi specificarne l'endpoint standard.
- Non puoi specificare risorse all'interno delle Regioni opt-in come sorgenti o sink.
- Esistono alcuni vincoli sui parametri che è possibile includere in una configurazione di pipeline. Per ulteriori informazioni, consulta the section called “Requisiti e vincoli di configurazione”.

Versioni di Data Prepper supportate

OpenSearch Attualmente Ingestion supporta le seguenti versioni principali di Data Prepper:

- 2.x

Quando create una pipeline, utilizzate l'`version`opzione richiesta per specificare la versione principale di Data Prepper da utilizzare. Ad esempio,. `version: "2"` OpenSearch Ingestion recupera l'ultima versione secondaria supportata di quella versione principale e fornisce la pipeline con quella versione. Per ulteriori informazioni, consulta the section called “Specificare la versione della pipeline”.

Attualmente, alle pipeline OpenSearch di ingestione viene fornita la versione 2.7 di Data Prepper. Per informazioni, consulta le note di rilascio della versione 2.7. Per informazioni sulle funzionalità e le correzioni di bug presenti in ogni versione di Data Prepper, consulta la pagina Releases. Non tutte le versioni secondarie di una particolare versione principale sono supportate da Ingestion. OpenSearch

Quando si aggiorna il file di configurazione YAML di una pipeline, se è disponibile il supporto per una nuova versione secondaria di Data Prepper, OpenSearch Ingestion aggiorna automaticamente la pipeline all'ultima versione secondaria supportata della versione principale specificata nella configurazione della pipeline. Ad esempio, potreste avere `version: "2"` nella configurazione della pipeline e Ingestion inizialmente aveva fornito alla pipeline la versione 2.6.0. OpenSearch Quando viene aggiunto il supporto per la versione 2.7.0 e si apporta una modifica alla configurazione della pipeline, Ingestion aggiorna la pipeline alla versione 2.7.0. OpenSearch Questo processo mantiene la pipeline aggiornata con le ultime correzioni di bug e i miglioramenti delle prestazioni. OpenSearch Ingestion non può aggiornare la versione principale della pipeline a meno che non si modifichi manualmente l'`version`opzione all'interno della configurazione della pipeline. Per ulteriori informazioni, consulta the section called “Aggiornamento delle pipeline”.

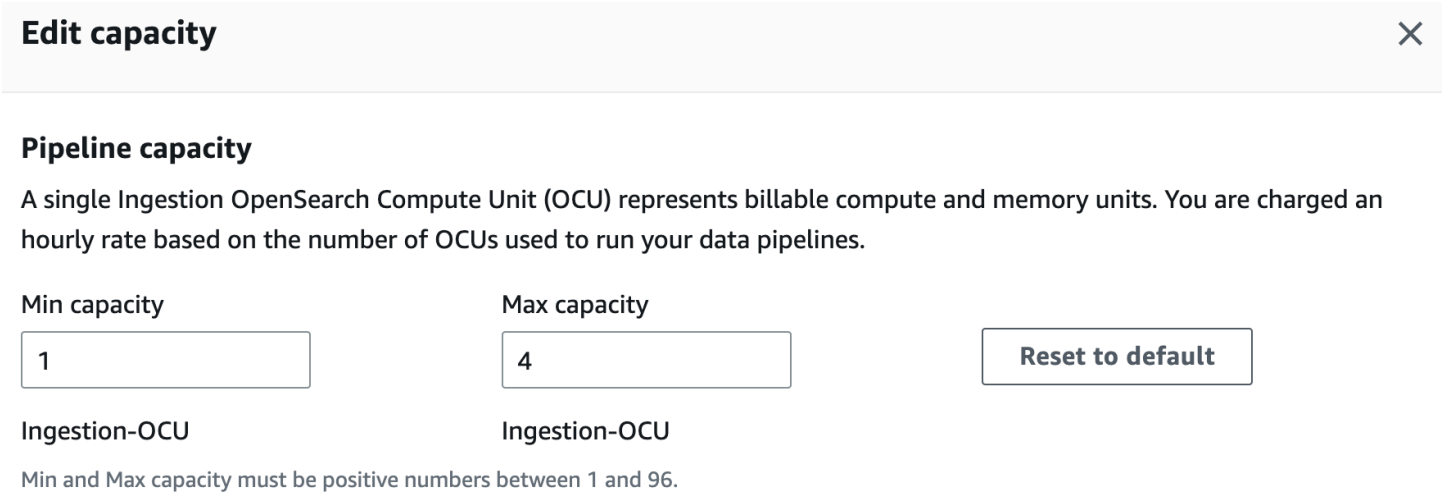
Scalabilità delle pipeline

Non è necessario fornire e gestire autonomamente la capacità delle pipeline. OpenSearch Ingestion ridimensiona automaticamente la capacità della pipeline in base al carico di lavoro stimato, in base alle Ingestion OpenSearch Compute Unit (Ingestion OCU) minime e massime specificate.

Ogni OCU Ingestion è una combinazione di circa 8 GiB di memoria e 2 vCPU. È possibile specificare i valori OCU minimi e massimi per una pipeline e OpenSearch Ingestion ridimensiona automaticamente la capacità della pipeline in base a questi limiti.

Puoi specificare le seguenti valori:

- Capacità minima: la pipeline può ridurre la capacità fino a questo numero di OCU di ingestione. La capacità minima specificata è anche la capacità iniziale di una pipeline.
- Capacità massima: la pipeline può aumentare la capacità fino a questo numero di OCU di ingestione.



Assicurati che la capacità massima di una pipeline sia sufficientemente elevata da gestire i picchi di carico di lavoro e che la capacità minima sia sufficientemente bassa da ridurre al minimo i costi quando la pipeline non è occupata. In base alle impostazioni, OpenSearch Ingestion ridimensiona automaticamente il numero di OCU di Ingestion per consentire alla pipeline di elaborare il carico di lavoro di importazione. In un momento specifico, ti vengono addebitati solo gli OCU di Ingestion utilizzati attivamente dalla tua pipeline.

La capacità allocata alla pipeline di OpenSearch Ingestion aumenta e diminuisce in base ai requisiti di elaborazione della pipeline e al carico generato dall'applicazione client. Quando la capacità è limitata,

OpenSearch Ingestion aumenta allocando più unità di calcolo (GiB di memoria). Quando la pipeline elabora carichi di lavoro più piccoli o non elabora affatto i dati, può essere ridimensionata fino alle OCU di Ingestion minime configurate.

È possibile specificare un minimo di 1 OCU di ingestione, un massimo di 96 OCU di ingestione per pipeline stateless e un massimo di 48 OCU di ingestione per pipeline a stato. Si consiglia un minimo di 2 OCU di ingestione per sorgenti basate su push. Quando il buffering persistente è abilitato, è possibile specificare un minimo di 2 e un massimo di 384 OCU di ingestione.

Data una pipeline di log standard con un'unica fonte, un pattern grok semplice e un sink, ogni unità di elaborazione può supportare fino a 2 MiB al secondo. Per pipeline di log più complesse con più processori, ogni unità di calcolo potrebbe supportare un carico di importazione inferiore. In base alla capacità della pipeline e all'utilizzo delle risorse, inizia il processo di scalabilità di OpenSearch Ingestion.

Per garantire un'elevata disponibilità, gli OCU di Ingestion sono distribuiti tra zone di disponibilità (AZ). Il numero di AZ dipende dalla capacità minima specificata.

Ad esempio, se si specifica un minimo di 2 unità di calcolo, le OCU di ingestione utilizzate in un dato momento vengono distribuite uniformemente su 2 AZ. Se si specifica un minimo di 3 o più unità di calcolo, le OCU di Ingestione vengono distribuite uniformemente su 3 AZ. Si consiglia di effettuare il provisioning di almeno due OCU di ingestione per garantire una disponibilità del 99,9% per le pipeline di importazione.

Non ti vengono addebitati i costi per gli OCU di ingestione quando una pipeline si trova negli stati,, e. `Create failed` `Creating` `Deleting` `Stopped`

Per istruzioni su come configurare e recuperare le impostazioni di capacità per una pipeline, consulta. the section called “Creazione di pipeline”

OpenSearch Prezzi di ingestione

In un momento specifico, paghi solo per il numero di OCU di Ingestion allocati a una pipeline, indipendentemente dal fatto che i dati scorrano attraverso la pipeline. OpenSearch Ingestion soddisfa immediatamente i carichi di lavoro aumentando o diminuendo la capacità della pipeline in base all'utilizzo.

Per i dettagli completi sui prezzi, consulta i prezzi OpenSearch di Amazon Service.

Supportato Regioni AWS

OpenSearch L'ingestione è disponibile in un sottoinsieme di Regioni AWS tale OpenSearch servizio è disponibile in. Per un elenco delle regioni supportate, consulta gli endpoint e le quote di Amazon OpenSearch Service nel. Riferimenti generali di AWS

OpenSearch Quote di ingestione

Per un elenco delle quote predefinite per le risorse di OpenSearch Ingestion, consulta le quote di Amazon OpenSearch Service.

Configurazione di ruoli e utenti in Amazon OpenSearch Ingestion

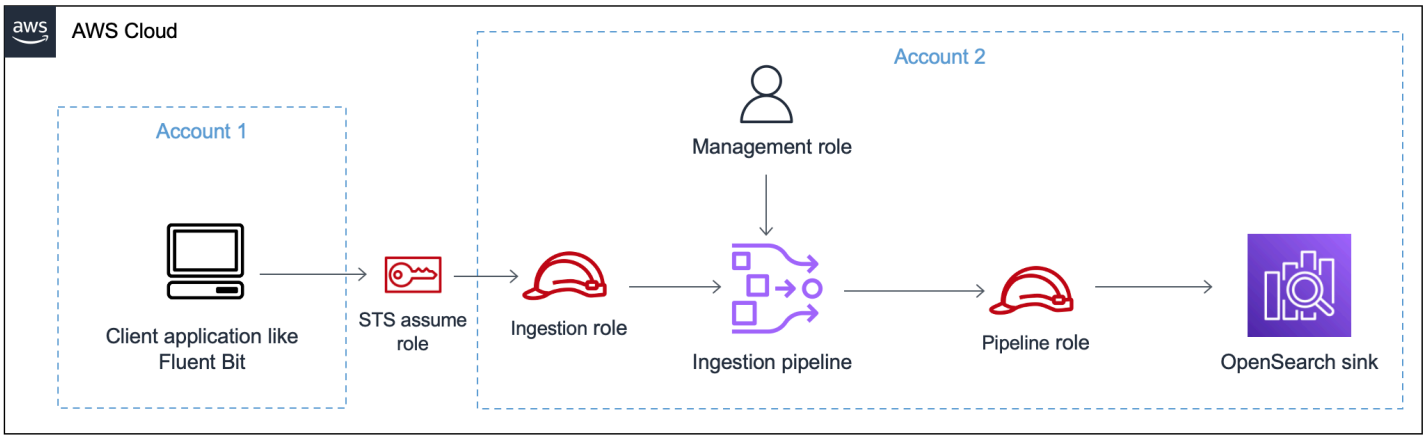
Amazon OpenSearch Ingestion utilizza una varietà di modelli di autorizzazioni e ruoli IAM per consentire alle applicazioni di origine di scrivere nelle pipeline e consentire alle pipeline di scrivere nei sink. Prima di iniziare a importare dati, devi creare uno o più ruoli IAM con autorizzazioni specifiche in base al tuo caso d'uso.

Per configurare una pipeline di successo sono necessari almeno i seguenti ruoli.

Nome	Description
Ruolo di gestione	Qualsiasi responsabile della gestione delle pipeline (in genere un «amministratore della pipeline») necessita dell'accesso alla gestione, che include autorizzazioni come e. `osis:CreatePipeline` `osis:UpdatePipeline` e Queste autorizzazioni consentono a un utente di amministrare le pipeline ma non necessariamente di scrivervi dati.
Ruolo della pipeline	Il ruolo pipeline, specificato all'interno della configurazione YAML della pipeline, fornisce le autorizzazioni necessarie affinché una pipeline possa scrivere nel dominio o nel collection sink e leggere da fonti basate su pull. Per ulteriori informazioni, consulta i seguenti argomenti: • the section called “Concedere alle pipeline l'accesso ai domini” • the section called “Concedere alle pipeline l'accesso alle raccolte”

Nome	Description
Ruolo di ingestione	Il ruolo di importazione contiene l'`osis:Ingest` autorizzazione per la risorsa della pipeline. Questa autorizzazione consente alle fonti basate su push di importare dati in una pipeline.

L'immagine seguente mostra una tipica configurazione di pipeline, in cui un'origine dati come Amazon S3 o Fluent Bit sta scrivendo su una pipeline in un account diverso. In questo caso, il client deve assumere il ruolo di ingestione per accedere alla pipeline. Per ulteriori informazioni, consulta the section called “Inserimento tra più account”.



Per una semplice guida alla configurazione, consulta. the section called “Tutorial: inserisci dati in un dominio”

Argomenti

- the section called “Ruolo di gestione”
- the section called “Ruolo di ingestione”
- the section called “Ruolo Pipeline”
- the section called “Inserimento tra più account”

Ruolo di gestione

Oltre alle `osis:*` autorizzazioni di base necessarie per creare e modificare una pipeline, è necessaria anche l'`iam:PassRole`autorizzazione per la risorsa del ruolo della pipeline. Chiunque Servizio AWS accetti un ruolo deve utilizzare questa autorizzazione. OpenSearch Ingestion assume

il ruolo ogni volta che deve scrivere dati in un sink. Questo aiuta gli amministratori a garantire che solo gli utenti approvati possano configurare OpenSearch Ingestion con un ruolo che concede le autorizzazioni. Per ulteriori informazioni, vedere Concessione a un utente delle autorizzazioni per passare un ruolo a un. Servizio AWS

Se utilizzi AWS Management Console (utilizzando i blueprint e successivamente controllando la pipeline), hai bisogno delle seguenti autorizzazioni per creare e aggiornare una pipeline:

```
{
   "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"
         ]
      }
   ]
}
```

Se utilizzi AWS CLI (non preconvalidando la pipeline o utilizzando i blueprint), hai bisogno delle seguenti autorizzazioni per creare e aggiornare una pipeline:

```
{
   "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"
         ]
      }
   ]
}
```

Ruolo Pipeline

Una pipeline necessita di determinate autorizzazioni per scrivere nel relativo sink. Queste autorizzazioni dipendono dal fatto che il sink sia un dominio di OpenSearch servizio o una OpenSearch raccolta Serverless.

Inoltre, una pipeline potrebbe aver bisogno delle autorizzazioni per estrarre dall'applicazione di origine (se l'origine è un plug-in basato su pull) e delle autorizzazioni per scrivere su una coda di lettere morte S3, se configurata.

Argomenti

- Scrittura su un sink di dominio
- Scrivere su un lavandino di raccolta
- Scrittura in una coda di lettere non scritte

Scrittura su un sink di dominio

Una pipeline di OpenSearch Ingestion necessita dell'autorizzazione per scrivere su un dominio OpenSearch di servizio configurato come sink. Queste autorizzazioni includono la possibilità di descrivere il dominio e inviargli richieste HTTP.

Per fornire alla pipeline le autorizzazioni necessarie per scrivere su un sink, crea innanzitutto un ruolo AWS Identity and Access Management (IAM) con le autorizzazioni richieste. Queste autorizzazioni sono le stesse per le pipeline pubbliche e VPC. Quindi, specifica il ruolo della pipeline nella politica di accesso al dominio in modo che il dominio possa accettare richieste di scrittura dalla pipeline.

Infine, specifica il ruolo ARN come valore dell'opzione sts_role_arn all'interno della configurazione della pipeline:

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

Per istruzioni su come completare ciascuno di questi passaggi, consulta Consentire alle pipeline di accedere ai domini.

Scrivere su un lavandino di raccolta

Una pipeline di OpenSearch Ingestion necessita dell'autorizzazione per scrivere su una raccolta OpenSearch Serverless configurata come sink. Queste autorizzazioni includono la possibilità di descrivere la raccolta e inviarle richieste HTTP.

Innanzitutto, crea un ruolo IAM che disponga dell'`aoss:BatchGetCollection`autorizzazione per tutte le risorse (*). Quindi, includi questo ruolo in una politica di accesso ai dati e concedigli le autorizzazioni per creare indici, aggiornare indici, descrivere indici e scrivere documenti all'interno della raccolta. Infine, specificate il ruolo ARN come valore dell'opzione sts_role_arn all'interno della configurazione della pipeline.

Per istruzioni su come completare ciascuno di questi passaggi, consulta Consentire alle pipeline di accedere alle raccolte.

Scrittura in una coda di lettere non scritte

Se configurate la pipeline per la scrittura su una coda di lettere morte (DLQ), dovete includere l'opzione nella configurazione DLQ. `sts_role_arn` Le autorizzazioni incluse in questo ruolo consentono alla pipeline di accedere al bucket S3 specificato come destinazione per gli eventi DLQ.

È necessario utilizzare lo stesso in tutti i componenti della pipeline`sts_role_arn`. Pertanto, è necessario allegare una politica di autorizzazioni separata al ruolo della pipeline che fornisca l'accesso DLQ. Al ruolo deve essere almeno consentita l'`S3:PutObject`azione sulla risorsa bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WriteToS3DLQ",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-dlq-bucket/*"
    }
  ]
}
```

È quindi possibile specificare il ruolo all'interno della configurazione DLQ della 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/pipeline-role"
```

Ruolo di ingestione

Tutti i plugin di origine attualmente supportati da OpenSearch Ingestion, ad eccezione di S3, utilizzano un'architettura basata su push. Ciò significa che l'applicazione di origine invia i dati alla pipeline, anziché la pipeline che estrae i dati dall'origine.

Pertanto, è necessario concedere alle applicazioni di origine le autorizzazioni necessarie per importare dati in una pipeline di ingestione. OpenSearch Al ruolo che firma la richiesta deve essere almeno concessa l'autorizzazione per l'`osis:Ingest`azione, che gli consente di inviare dati a una pipeline. Le stesse autorizzazioni sono richieste per gli endpoint pubblici e per gli endpoint della pipeline VPC.

La seguente politica di esempio consente al principale associato di inserire dati in un'unica pipeline denominata: `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"
    }
  ]
}
```

Per ulteriori informazioni, consulta the section called “Utilizzo delle integrazioni di pipeline”.

Inserimento tra più account

Potrebbe essere necessario importare dati in una pipeline da un altroAccount AWS, ad esempio un account di applicazione. Per configurare l'ingestione tra account, definite un ruolo di importazione all'interno dello stesso account della pipeline e stabilite una relazione di fiducia tra il ruolo di inserimento e l'account dell'applicazione:

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

```
      "Principal": {
        "AWS": "arn:aws:iam::{external-account-id}:root"
       },
      "Action": "sts:AssumeRole"
  }]
}
```

Quindi, configura l'applicazione in modo che assuma il ruolo di ingestione. L'account dell'applicazione deve concedere al ruolo dell'applicazione AssumeRolele autorizzazioni per il ruolo di ingestione nell'account pipeline.

Per i passaggi dettagliati e gli esempi di policy IAM, consulta. the section called “Fornire l'accesso all'importazione su più account”

Concedere alle pipeline OpenSearch di Amazon Ingestion l'accesso ai domini

Una pipeline Amazon OpenSearch Ingestion necessita dell'autorizzazione per scrivere nel dominio OpenSearch di servizio configurato come sink. Per fornire l'accesso, configuri un ruolo AWS Identity and Access Management (IAM) con una politica di autorizzazioni restrittiva che limita l'accesso al dominio a cui una pipeline invia i dati. Ad esempio, potresti voler limitare una pipeline di ingestione solo al dominio e agli indici necessari per supportarne il caso d'uso.

Prima di specificare il ruolo nella configurazione della pipeline, è necessario configurarlo con una relazione di trust appropriata e quindi concedergli l'accesso al dominio nell'ambito della politica di accesso al dominio.

Argomenti

Fase 1: Creare un ruolo nella pipeline

Il ruolo specificato nel parametro sts_role_arn di una configurazione di pipeline deve avere una politica di autorizzazioni associata che gli consenta di inviare dati al sink di dominio. Deve inoltre

avere una relazione di fiducia che consenta a Ingestion di assumere il ruolo. OpenSearch Per istruzioni su come allegare una policy a un ruolo, consulta Aggiungere i permessi di identità IAM nella Guida per l'utente IAM.

La seguente policy di esempio mostra il privilegio minimo che puoi fornire nel ruolo sts_role_arn di una configurazione di pipeline per la scrittura su un singolo 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}/*"
        }
    ]
}
```

Se prevedi di riutilizzare il ruolo per scrivere su più domini, puoi rendere la politica più ampia sostituendo il nome di dominio con un carattere jolly (). *

Il ruolo deve avere la seguente relazione di fiducia, che consente a OpenSearch Ingestion di assumere il ruolo di pipeline:

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

Inoltre, ti consigliamo di aggiungere i tasti `aws:SourceAccount` e `aws:SourceArn` condition alla policy per proteggerti dal confuso problema del vicedirettore. L'account di origine è il proprietario della pipeline.

Ad esempio, è possibile aggiungere il seguente blocco di condizione alla policy:

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

Fase 2: Includi il ruolo della pipeline nella politica di accesso al dominio

Affinché una pipeline possa scrivere dati su un dominio, il dominio deve disporre di una politica di accesso a livello di dominio che consenta al ruolo della pipeline sts_role_arn di accedervi.

Il seguente esempio di policy di accesso al dominio consente al ruolo pipeline denominato`pipeline-role`, creato nel passaggio precedente, di scrivere dati nel dominio denominato: `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}/*"
    }
  ]
}
```

Passaggio 3: mappare il ruolo della pipeline (solo per i domini che utilizzano un controllo di accesso granulare)

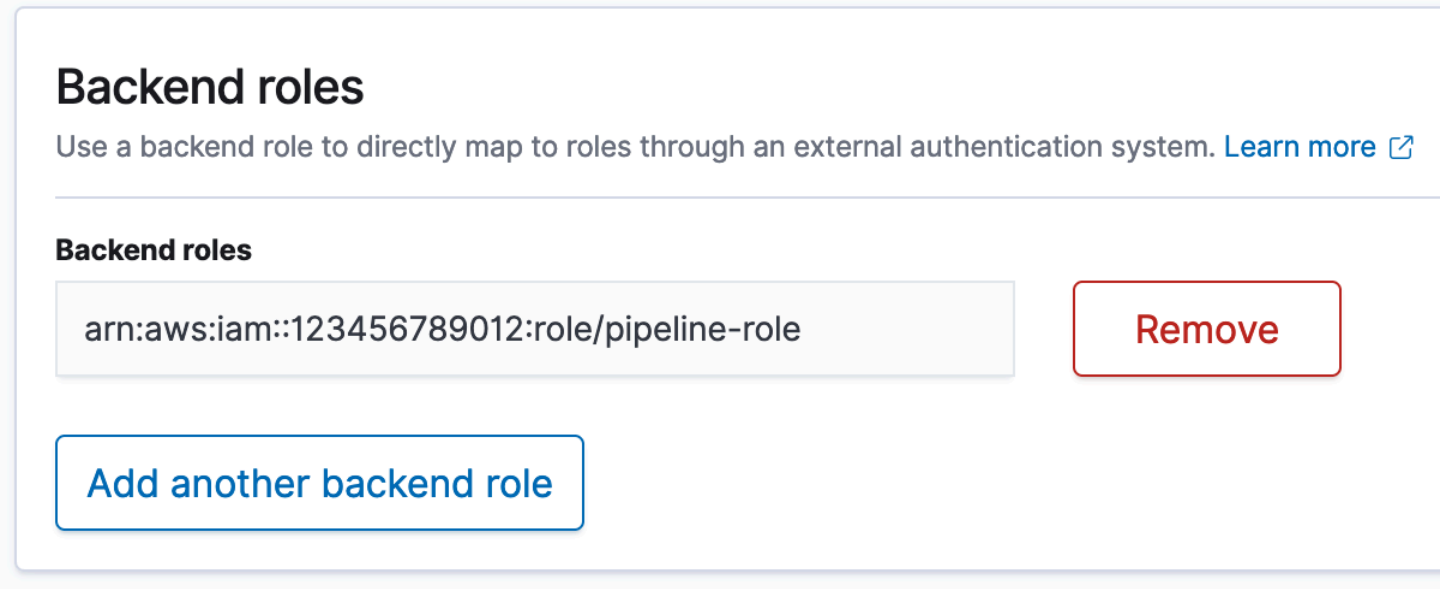
Se il tuo dominio utilizza un controllo granulare degli accessi per l'autenticazione, è necessario eseguire ulteriori passaggi per fornire alla pipeline l'accesso a un dominio. I passaggi variano a seconda della configurazione del dominio:

Scenario 1: ruolo principale e ruolo pipeline diversi: se utilizzi un IAM Amazon Resource Name (ARN) come utente principale ed è diverso dal ruolo pipeline `sts_role_arn` (), devi mappare il ruolo della pipeline al ruolo di backend. OpenSearch `all_access` Ciò aggiunge essenzialmente il ruolo della pipeline come utente principale aggiuntivo. Per ulteriori informazioni, consulta Utenti master aggiuntivi.

Scenario 2: Utente principale nel database utenti interno: se il dominio utilizza un utente principale nel database utenti interno e l'autenticazione di base HTTP per le OpenSearch dashboard, non è possibile passare il nome utente e la password principali direttamente nella configurazione della pipeline. È invece necessario mappare il ruolo della pipeline (`sts_role_arn`) al ruolo di backend. OpenSearch `all_access` Ciò aggiunge essenzialmente il ruolo della pipeline come utente principale aggiuntivo. Per ulteriori informazioni, consulta Utenti master aggiuntivi.

Scenario 3: stesso ruolo principale e ruolo della pipeline (non comune): se utilizzi un ARN IAM come utente principale ed è lo stesso ARN che utilizzi come ruolo pipeline (`sts_role_arn`), non devi intraprendere ulteriori azioni. La pipeline dispone delle autorizzazioni necessarie per scrivere nel dominio. Questo scenario è raro perché la maggior parte degli ambienti utilizza un ruolo di amministratore o un altro ruolo come ruolo principale.

L'immagine seguente mostra come mappare il ruolo della pipeline a un ruolo di backend:



Fase 4: Specificare il ruolo nella configurazione della pipeline

Per creare correttamente una pipeline, è necessario specificare il ruolo della pipeline creato nel passaggio 1 come parametro sts_role_arn nella configurazione della pipeline. La pipeline assume questo ruolo per firmare le richieste al service domain sink. OpenSearch

Nel `sts_role_arn` campo, specifica l'ARN del ruolo della pipeline IAM:

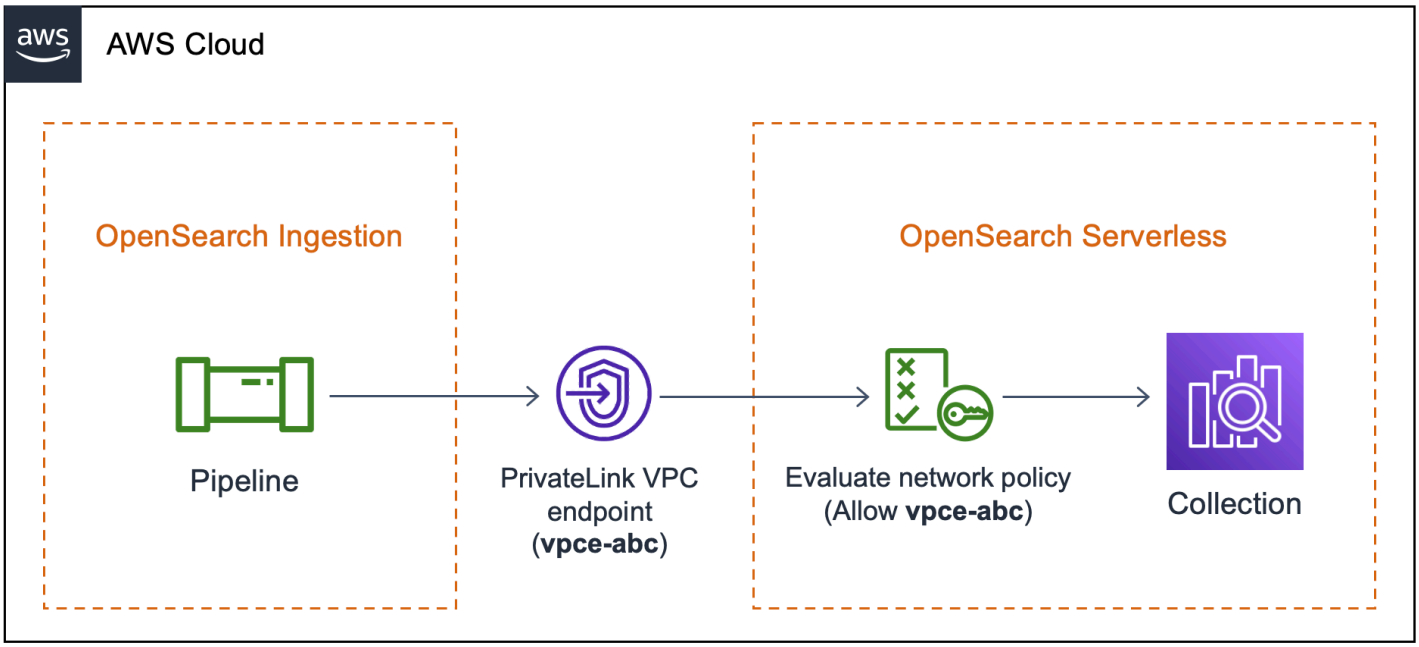
```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG}" ]
  sink:
    - opensearch:
        hosts: [ "https://search-{domain-name}.us-east-1.es.amazonaws.com" ]
        index: "my-index"
        aws:
          region: "{region}"
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
```

Per un riferimento completo dei parametri obbligatori e non supportati, consulta. the section called “Plugin e opzioni supportati”

Concedere alle pipeline OpenSearch di Amazon Ingestion l'accesso alle raccolte

Una pipeline Amazon OpenSearch Ingestion può scrivere su una raccolta pubblica OpenSearch Serverless o su una raccolta VPC. Per fornire l'accesso alla raccolta, configuri un ruolo di pipeline AWS Identity and Access Management (IAM) con una politica di autorizzazioni che garantisca l'accesso alla raccolta. Prima di specificare il ruolo nella configurazione della pipeline, è necessario configurarlo con una relazione di fiducia appropriata e quindi concedergli le autorizzazioni di accesso ai dati tramite una politica di accesso ai dati.

Durante la creazione della pipeline, OpenSearch Ingestion crea una AWS PrivateLink connessione tra la pipeline e la raccolta Serverless. OpenSearch Tutto il traffico proveniente dalla pipeline passa attraverso questo endpoint VPC e viene indirizzato alla raccolta. Per raggiungere la raccolta, all'endpoint deve essere concesso l'accesso alla raccolta tramite una politica di accesso alla rete.



Argomenti

- Limitazioni
- Fornire l'accesso di rete alle pipeline
- Fase 1: Creare un ruolo di pipeline
- Fase 2: creazione di una raccolta
- Fase 3: Creare una pipeline

Limitazioni

Le seguenti limitazioni si applicano alle pipeline che scrivono su raccolte OpenSearch Serverless:

- Il processore del gruppo di traccia Otel attualmente non funziona con i sink di raccolta OpenSearch Serverless.
- Attualmente, OpenSearch Ingestion supporta solo l'`_template`operazione legacy, mentre OpenSearch Serverless supporta l'operazione componibile. `_index_template` Pertanto, se la configurazione della pipeline include l'`index_type`opzione, questa deve essere impostata su. `management_disabled`

Fornire l'accesso di rete alle pipeline

A ogni raccolta creata in OpenSearch Serverless è associata almeno una politica di accesso alla rete. Le politiche di accesso alla rete determinano se la raccolta è accessibile su Internet da reti pubbliche o se è necessario accedervi privatamente. Per ulteriori informazioni sulle politiche di rete, vederethe section called “Accesso alla rete”.

All'interno di una politica di accesso alla rete, puoi specificare solo endpoint OpenSearch VPC gestiti senza server. Per ulteriori informazioni, consulta the section called “Endpoint VPC”. Tuttavia, affinché la pipeline possa scrivere nella raccolta, la policy deve anche concedere l'accesso all'endpoint VPC OpenSearch che Ingestion crea automaticamente tra la pipeline e la raccolta. Pertanto, quando si crea una pipeline con un sink di raccolta OpenSearch Serverless, è necessario fornire il nome della politica di rete associata utilizzando l'opzione. `network_policy_name`

Per esempio:

```
...
sink:
   - opensearch:
       hosts: [ "https://{collection-id}.{region}.aoss.amazonaws.com" ]
       index: "my-index"
        aws:
          serverless: true
          serverless_options:
            network_policy_name: "{network-policy-name}"
```

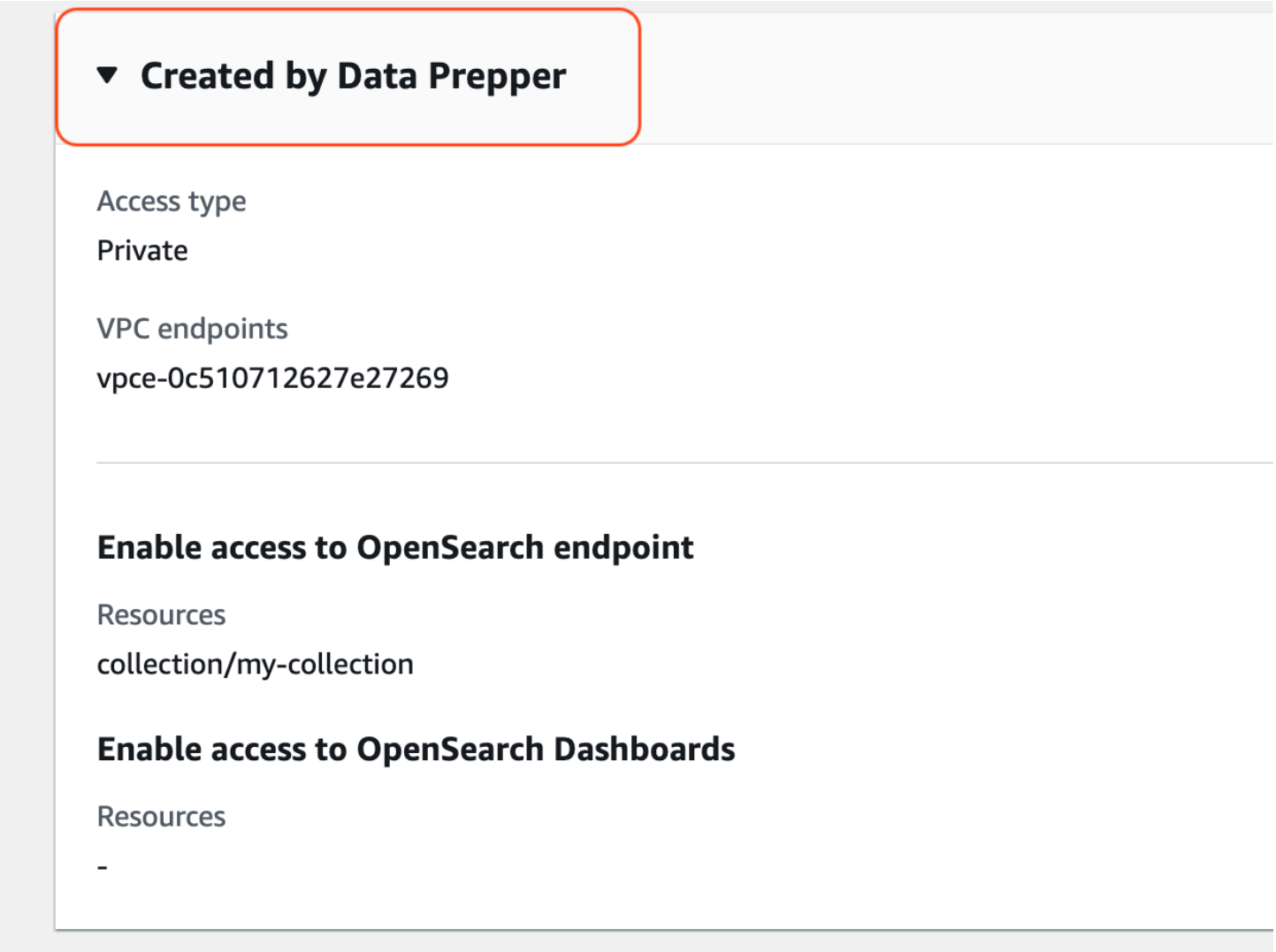
Durante la creazione della pipeline, OpenSearch Ingestion verifica l'esistenza della politica di rete specificata. Se non esiste, OpenSearch Ingestion la crea. Se esiste, OpenSearch Ingestion lo

aggiorna aggiungendovi una nuova regola. La regola concede l'accesso all'endpoint VPC che collega la pipeline e la raccolta.

Per esempio:

```
{
   "Rules":[
      {
         "Resource":[
            "collection/my-collection"
         ],
         "ResourceType":"collection"
      }
   ],
   "SourceVPCEs":[
      "vpce-0c510712627e27269" # The ID of the VPC endpoint that OpenSearch Ingestion
 creates between the pipeline and collection
   ],
   "Description":"Created by Data Prepper"
}
```

Nella console, tutte le regole che OpenSearch Ingestion aggiunge alle policy di rete sono denominate Created by Data Prepper:



> **Note**
>
> In generale, una regola che specifica l'accesso pubblico per una raccolta ha la precedenza su una regola che specifica l'accesso privato. Pertanto, se la policy aveva già configurato l'accesso pubblico, questa nuova regola aggiunta da OpenSearch Ingestion non modifica effettivamente il comportamento della politica. Per ulteriori informazioni, consulta the section called “Priorità delle policy”.

Se si arresta o si elimina la pipeline, OpenSearch Ingestion elimina l'endpoint VPC tra la pipeline e la raccolta. Modifica inoltre la politica di rete per rimuovere l'endpoint VPC dall'elenco degli endpoint consentiti. Se riavvii la pipeline, ricrea l'endpoint VPC e aggiorna nuovamente la politica di rete con l'ID dell'endpoint.

Fase 1: Creare un ruolo di pipeline

Il ruolo specificato nel parametro sts_role_arn di una configurazione di pipeline deve avere una politica di autorizzazioni associata che gli consenta di inviare dati al sink di raccolta. Deve inoltre avere una relazione di fiducia che consenta a Ingestion di assumere il ruolo. OpenSearch Per istruzioni su come allegare una policy a un ruolo, consulta Aggiungere i permessi di identità IAM nella Guida per l'utente IAM.

La seguente policy di esempio mostra il privilegio minimo che puoi fornire nel ruolo sts_role_arn di una configurazione di pipeline per la scrittura nelle raccolte:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "aoss:APIAccessAll",
                "aoss:BatchGetCollection",
                "aoss:CreateSecurityPolicy",
                "aoss:GetSecurityPolicy",
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Il ruolo deve avere la seguente relazione di fiducia, che consente a Ingestion di assumerlo:
OpenSearch

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

```
    ]
}
```

Fase 2: creazione di una raccolta

Crea una raccolta OpenSearch Serverless con le seguenti impostazioni. Per istruzioni su come creare una raccolta, consultathe section called “Creazione di raccolte”.

Politica di accesso ai dati

Crea una politica di accesso ai dati per la raccolta che conceda le autorizzazioni richieste al ruolo della pipeline. Per esempio:

```
[
  {
    "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**
>
> Nell'`Principal`elemento, specifica l'Amazon Resource Name (ARN) del ruolo della pipeline creato nel passaggio precedente.

Politica di accesso alla rete

Crea una politica di accesso alla rete per la raccolta. Puoi inserire dati in una raccolta pubblica o in una raccolta VPC. Ad esempio, la seguente policy fornisce l'accesso a un singolo endpoint OpenSearch VPC gestito senza server:

```
[
   {
      "Description":"Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/{collection-name}"
            ]
         }
      ],
      "AllowFromPublic": false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   }
]
```

Important

È necessario specificare il nome della politica di rete all'interno dell'`network_policy_name`opzione nella configurazione della pipeline. Al momento della creazione della pipeline, OpenSearch Ingestion aggiorna questa policy di rete per consentire l'accesso all'endpoint VPC che crea automaticamente tra la pipeline e la raccolta. Vedi il passaggio 3 per un esempio di configurazione della pipeline. Per ulteriori informazioni, consulta the section called “Fornire l'accesso di rete alle pipeline”.

Fase 3: Creare una pipeline

Infine, crea una pipeline in cui specifichi il ruolo della pipeline e i dettagli della raccolta. La pipeline assume questo ruolo per firmare le richieste al sink di raccolta Serverless. OpenSearch

Completa le seguenti operazioni:

- Per l'`hosts`opzione, specifica l'endpoint della raccolta che hai creato nel passaggio 2.
- Per l'`sts_role_arn`opzione, specifica l'Amazon Resource Name (ARN) del ruolo della pipeline che hai creato nel passaggio 1.
- Imposta l'`serverless`opzione su. `true`
- Imposta l'`network_policy_name`opzione sul nome della politica di rete allegata alla raccolta. OpenSearch Ingestion aggiorna automaticamente questa politica di rete per consentire l'accesso dal VPC che crea tra la pipeline e la raccolta. Per ulteriori informazioni, consulta the section called “Fornire l'accesso di rete alle pipeline”.

```
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}"
```

Per un riferimento completo dei parametri richiesti e non supportati, vedere. the section called “Plugin e opzioni supportati”

Guida introduttiva ad Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion supporta l'inserimento di dati in domini di OpenSearch servizi gestiti e raccolte serverless. OpenSearch I seguenti tutorial illustra i passaggi di base per ottenere una base per ottenere una base per ottenere una base per ottenere una base per ottenere una base di base

per ottenere una base per ottenere una base di base per ottenere una base per ottenere una base di base per ottenere una

> **Note**
>
> La creazione della pipeline avrà esito negativo se non si impostano le autorizzazioni corrette. Consulta the section called “Configurazione di ruoli e utenti” la sezione per una migliore comprensione dei ruoli richiesti prima di creare una pipeline.

Argomenti

- Tutorial: importazione di dati in un dominio utilizzando Amazon Ingestion OpenSearch
- Tutorial: Inserimento di dati in una raccolta con Amazon Ingestion OpenSearch

Tutorial: importazione di dati in un dominio utilizzando Amazon Ingestion OpenSearch

Questo tutorial mostra come usare Amazon OpenSearch Ingestion per configurare una pipeline semplice e inserire dati in un dominio Amazon Service. OpenSearch Una pipeline è una risorsa che OpenSearch Ingestion fornisce e gestisce. È possibile utilizzare una pipeline per filtrare, arricchire, trasformare, normalizzare e aggregare i dati per l'analisi e la visualizzazione a valle in Service. OpenSearch

Questo tutorial illustra i passaggi di base per avviare rapidamente una pipeline. Per informazioni più dettagliate, consulta the section called “Creazione di pipeline”.

In questo tutorial completerai le seguenti fasi:

1. Crea il ruolo della pipeline.
2. Crea un dominio.
3. Crea una pipeline.
4. Inserisci alcuni dati di esempio.

All'interno del tutorial, creerai le seguenti risorse:

- Una pipeline denominata `ingestion-pipeline`
- Un dominio denominato su `ingestion-domain` cui la pipeline scriverà

- Un ruolo IAM denominato `PipelineRole` che la pipeline assumerà per scrivere nel dominio

Autorizzazioni richieste

Per completare questo tutorial, devi disporre delle autorizzazioni IAM corrette. Il tuo utente o ruolo deve avere una policy basata sull'identità allegata con le seguenti autorizzazioni minime. Queste autorizzazioni consentono di creare un ruolo pipeline (`iam:Create`), creare o modificare un dominio (`es:*`) e utilizzare pipelines (). `osis:*`

Inoltre, è richiesta l'`iam:PassRole`autorizzazione sulla risorsa del ruolo pipeline. Questa autorizzazione consente di passare il ruolo della pipeline a OpenSearch Ingestion in modo che possa scrivere dati nel 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"
         ]
      }
   ]
}
```

Fase 1: Creare il ruolo della pipeline

Innanzitutto, crea un ruolo che la pipeline assumerà per accedere al OpenSearch service domain sink. Includerai questo ruolo nella configurazione della pipeline più avanti in questo tutorial.

Per creare il ruolo della pipeline

1. Apri la AWS Identity and Access Management console all'indirizzo https://console.aws.amazon.com/iamv2/.
2. Scegli Politiche, quindi scegli Crea politica.
3. In questo tutorial, inserirai i dati in un dominio chiamato`ingestion-domain`, che creerai nel passaggio successivo. Seleziona JSON e incolla la seguente politica nell'editor. Sostituiscilo `{your-account-id}` con l'ID del tuo account e, se necessario, modifica la regione.

```
{
    "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/*"
        }
    ]
}
```

Se desideri scrivere dati su un dominio esistente, sostituiscili `ingestion-domain` con il nome del tuo dominio.

> **Note**
>
> Per semplicità in questo tutorial, utilizziamo una politica di accesso abbastanza ampia. Negli ambienti di produzione, tuttavia, ti consigliamo di applicare una politica di accesso più restrittiva al tuo ruolo di pipeline. Per un esempio di policy che fornisce le autorizzazioni minime richieste, vedi. the section called “Concedere alle pipeline l'accesso ai domini”

4. Scegliete Avanti, scegliete Avanti e assegnate un nome alla vostra policy pipeline-policy.

5. Scegli Crea policy.
6. Quindi, crea un ruolo e allega la policy ad esso. Selezionare Roles (Ruoli), quindi selezionare Create role (Crea ruolo).
7. Scegli una politica di fiducia personalizzata e incolla la seguente politica nell'editor:

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

8. Seleziona Successivo. Quindi cerca e seleziona pipeline-policy (che hai appena creato).
9. Scegli Avanti e assegna un nome al ruolo. PipelineRole
10. Scegli Crea ruolo.

Ricorda l'Amazon Resource Name (ARN) del ruolo (ad esempio,`arn:aws:iam::{your-account-id}:role/PipelineRole`). Ne avrai bisogno quando creerai la tua pipeline.

Passaggio 2: crea un dominio

Quindi, crea un dominio denominato in `ingestion-domain` cui inserire i dati.

Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home e crea un dominio che soddisfi i seguenti requisiti:

- È in esecuzione OpenSearch 1.0 o versione successiva oppure Elasticsearch 7.4 o versione successiva
- Utilizza l'accesso pubblico
- Non utilizza un controllo degli accessi a grana fine

> **Note**
>
> Questi requisiti hanno lo scopo di garantire la semplicità di questo tutorial. Negli ambienti di produzione, puoi configurare un dominio con accesso VPC e/o utilizzare un controllo degli accessi granulare. Per utilizzare un controllo granulare degli accessi, consulta Mappare il ruolo della pipeline.

Il dominio deve avere una politica di accesso che conceda l'autorizzazione`PipelineRole`, creata nel passaggio precedente. La pipeline assumerà questo ruolo (denominato sts_role_arn nella configurazione della pipeline) per inviare i dati al service domain sink. OpenSearch

Assicurati che il dominio abbia la seguente politica di accesso a livello di dominio, che concede l'accesso al dominio. `PipelineRole` Sostituisci la regione e l'ID dell'account con i tuoi:

```
{
  "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/*"
    }
  ]
}
```

Per ulteriori informazioni sulla creazione di politiche di accesso a livello di dominio, consulta Politiche di accesso basate sulle risorse.

Se hai già creato un dominio, modifica la sua politica di accesso esistente per fornire le autorizzazioni di cui sopra. `PipelineRole`

> **Note**
>
> Ricorda l'endpoint del dominio (ad esempio,`https://search-ingestion-domain.us-east-1.es.amazonaws.com`). Lo utilizzerai nel passaggio successivo per configurare la tua pipeline.

Fase 3: Creare una pipeline

Ora che disponi di un dominio e di un ruolo con i diritti di accesso appropriati, puoi creare una pipeline.

Per creare una pipeline

1. Nella console di Amazon OpenSearch Service, scegli Pipelines dal riquadro di navigazione a sinistra.
2. Scegliere Create pipeline (Crea pipeline).
3. Assegna un nome alla pipeline di ingestione e mantieni le impostazioni di capacità come predefinite.
4. In questo tutorial, creerai una semplice sottopipeline chiamata che utilizza il plugin sorgente Http. `log-pipeline` Questo plugin accetta i dati di registro in un formato di matrice JSON. Specificherai un singolo dominio di OpenSearch servizio come sink e inserirai tutti i dati nell'`application_logs`indice.

   In Configurazione Pipeline, incolla la seguente configurazione YAML nell'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**
>
> L'`path`opzione specifica il percorso URI per l'ingestione. Questa opzione è necessaria per le sorgenti basate su pull. Per ulteriori informazioni, consulta the section called “Specificare il percorso di ingestione”.

5. Sostituisci l'`hosts`URL con l'endpoint del dominio che hai creato (o modificato) nella sezione precedente. Sostituisci il `sts_role_arn` parametro con l'ARN di. `PipelineRole`
6. Scegli Convalida pipeline e assicurati che la convalida abbia esito positivo.
7. Per semplificare questo tutorial, configura l'accesso pubblico alla pipeline. In Rete, scegli Accesso pubblico.

   Per informazioni sulla configurazione dell'accesso al VPC, vedere. the section called “Configurazione dell'accesso VPC per le pipeline”
8. Mantieni abilitata la pubblicazione dei log in caso di problemi durante il completamento di questo tutorial. Per ulteriori informazioni, consulta the section called “Monaggio aggio aggio aggio aggio aggio aggio aggio aggio”.

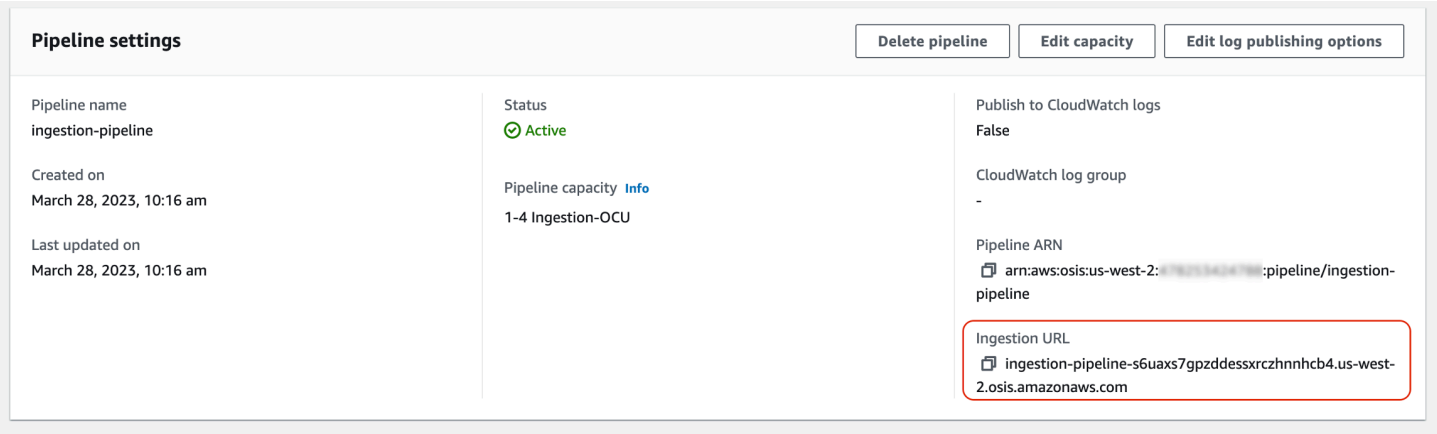
   Specificate il seguente nome del gruppo di log: `/aws/vendedlogs/OpenSearchIngestion/ingestion-pipeline/audit-logs`
9. Seleziona Successivo. Controlla la configurazione della pipeline e scegli Crea pipeline. La pipeline impiega 5-10 minuti per diventare attiva.

Fase 4: Inserimento di alcuni dati di esempio

Quando lo stato della pipeline è impostato`Active`, puoi iniziare a importare dati al suo interno. È necessario firmare tutte le richieste HTTP alla pipeline utilizzando Signature Version 4. Utilizza uno strumento HTTP come Postman o awscurl per inviare alcuni dati alla pipeline. Come per l'indicizzazione dei dati direttamente su un dominio, l'importazione dei dati in una pipeline richiede sempre un ruolo IAM o una chiave di accesso IAM e una chiave segreta.

> **Note**
>
> Il principale che firma la richiesta deve disporre dell'autorizzazione IAM. `osis:Ingest`

Innanzitutto, ottieni l'URL di importazione dalla pagina delle impostazioni di Pipeline:



Quindi, inserisci alcuni dati di esempio. La seguente richiesta utilizza awscurl per inviare un singolo file di registro all'indice: `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
```

Dovresti vedere una `200 OK` risposta. Se ricevi un errore di autenticazione, potrebbe essere perché stai importando dati da un account diverso da quello in cui si trova la pipeline. Per informazioni, consulta the section called “Risoluzione dei problemi relativi alle autorizzazioni”.

Ora, interroga l'`application_logs`indice per assicurarti che la voce di registro sia stata inserita correttamente:

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

Esempio di risposta:

```
{
```

```
   "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"
            }
         }
      ]
   }
}
```


Risoluzione dei problemi relativi alle autorizzazioni

Se hai seguito i passaggi del tutorial e continui a riscontrare errori di autenticazione quando tenti di importare dati, è possibile che il ruolo della scrittura in una pipeline sia Account AWS diverso da quello della pipeline stessa. In questo caso, devi creare e assumere un ruolo che ti consenta specificamente di importare dati. Per istruzioni, consulta the section called “Fornire l'accesso all'importazione su più account”.

Risorse correlate

Questo tutorial ha presentato un semplice caso d'uso di ingestione di un singolo documento tramite HTTP. Negli scenari di produzione, configurerai le tue applicazioni client (come Fluent Bit, Kubernetes o OpenTelemetry Collector) per inviare dati a una o più pipeline. Le tue pipeline saranno probabilmente più complesse del semplice esempio di questo tutorial.

Per iniziare a configurare i client e ad acquisire dati, consulta le seguenti risorse:

- Creazione e gestione delle pipeline
- Configurazione dei client per l'invio di dati a Ingestion OpenSearch
- Documentazione Data Prepper

Tutorial: Inserimento di dati in una raccolta con Amazon Ingestion OpenSearch

Questo tutorial mostra come usare Amazon OpenSearch Ingestion per configurare una pipeline semplice e inserire dati in una raccolta Amazon Serverless. OpenSearch Una pipeline è una risorsa che Ingestion fornisce e gestisce. OpenSearch È possibile utilizzare una pipeline per filtrare, arricchire, trasformare, normalizzare e aggregare i dati per l'analisi e la visualizzazione a valle in Service. OpenSearch

Per un tutorial che dimostra come inserire dati in un dominio di servizio fornito, consulta. OpenSearch the section called “Tutorial: inserisci dati in un dominio”

In questo tutorial completerai le seguenti fasi:

1. Crea il ruolo della pipeline.
2. Creare una raccolta.
3. Crea una pipeline.
4. Inserisci alcuni dati di esempio.

All'interno del tutorial, creerai le seguenti risorse:

- Una pipeline denominata `ingestion-pipeline-serverless`
- Una raccolta denominata in `ingestion-collection` cui la pipeline scriverà

- Un ruolo IAM denominato `PipelineRole` che la pipeline assumerà per scrivere nella raccolta

Autorizzazioni richieste

Per completare questo tutorial, devi disporre delle autorizzazioni IAM corrette. Il tuo utente o ruolo deve avere una policy basata sull'identità allegata con le seguenti autorizzazioni minime. Queste autorizzazioni consentono di creare un ruolo pipeline (`iam:Create*`), creare o modificare una raccolta () e lavorare con `aoss:*` pipelines (). `osis:*`

Inoltre, è richiesta l'`iam:PassRole`autorizzazione sulla risorsa del ruolo pipeline. Questa autorizzazione consente di passare il ruolo della pipeline a OpenSearch Ingestion in modo che possa scrivere dati nella raccolta.

```
{
   "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"
         ]
      }
   ]
}
```

Fase 1: Creare il ruolo della pipeline

Innanzitutto, crea un ruolo che la pipeline assumerà per accedere al sink di raccolta OpenSearch Serverless. Includerai questo ruolo nella configurazione della pipeline più avanti in questo tutorial.

Per creare il ruolo della pipeline

1. Apri la AWS Identity and Access Management console all'indirizzo https://console.aws.amazon.com/iamv2/.
2. Scegli Politiche, quindi scegli Crea politica.
3. Seleziona JSON e incolla la seguente politica nell'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. Scegli Avanti, scegli Avanti e dai un nome alla tua politica collection-pipeline-policy.
5. Scegli Crea policy.
6. Quindi, crea un ruolo e allega la politica ad esso. Selezionare Roles (Ruoli), quindi selezionare Create role (Crea ruolo).
7. Scegli una politica di fiducia personalizzata e incolla la seguente politica nell'editor:

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

8. Seleziona Avanti. Quindi cerca e seleziona collection-pipeline-policy(che hai appena creato).
9. Scegli Avanti e assegna un nome al ruolo PipelineRole.
10. Scegli Crea ruolo.

Ricorda l'Amazon Resource Name (ARN) del ruolo (ad esempio,`arn:aws:iam::`*`{your-account-id}`*`:role/PipelineRole`). Ne avrai bisogno quando creerai la tua pipeline.

Fase 2: creazione di una raccolta

Quindi, crea una raccolta in cui inserire i dati. Daremo un nome alla raccolta`ingestion-collection`.

1. Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegli Raccolte dalla barra di navigazione a sinistra e scegli Crea raccolta.
3. Assegna un nome alla raccolta ingestion-collection.
4. In Impostazioni di accesso alla rete, modifica il tipo di accesso in Pubblico.
5. Mantenere tutte le altre impostazioni come valori predefiniti e scegliere Successivo.
6. Per il metodo di definizione, scegli JSON e incolla la seguente politica nell'editor. Questa politica fa due cose:

   - Consente al ruolo della pipeline di scrivere nella raccolta.

- Consente di leggere i contenuti della raccolta. Successivamente, dopo aver inserito alcuni dati di esempio nella pipeline, interrogherete la raccolta per assicurarvi che i dati siano stati inseriti e scritti correttamente nell'indice.

```
[
  {
    "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. Sostituisci gli elementi. `Principal` Il primo principale dovrebbe specificare il ruolo della pipeline che hai creato. Il secondo dovrebbe specificare un utente o un ruolo da utilizzare per interrogare la raccolta in un secondo momento.
8. Seleziona Avanti. Assegna un nome alla politica di accesso pipeline-domain-accesse scegli nuovamente Avanti.
9. Rivedi la configurazione della raccolta e scegli Submit (Invia).

Quando la raccolta è attiva, annota l' OpenSearch endpoint in Endpoint (ad esempio,`https://{collection-id}.us-east-1.aoss.amazonaws.com`). Ne avrai bisogno quando creerai la tua pipeline.

Fase 3: Creare una pipeline

Ora che disponi di una raccolta e di un ruolo con i diritti di accesso appropriati, puoi creare una pipeline.

Per creare una pipeline

1. Nella console di Amazon OpenSearch Service, scegli Pipelines dal riquadro di navigazione a sinistra.
2. Scegliere Create pipeline (Crea pipeline).
3. Assegna un nome alla pipeline serverless-ingestion e mantieni le impostazioni di capacità come predefinite.
4. In questo tutorial, creeremo una semplice sottopipeline chiamata che utilizza il plugin sorgente HTTP. `log-pipeline` Il plugin accetta i dati di registro in un formato di matrice JSON. Specificheremo una singola raccolta OpenSearch Serverless come sink e inseriremo tutti i dati nell'indice. `my_logs`

   In Configurazione Pipeline, incolla la seguente configurazione YAML nell'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. Sostituisci l'`hosts`URL con l'endpoint della raccolta che hai creato nella sezione precedente. Sostituisci il `sts_role_arn` parametro con l'ARN di. `PipelineRole` Facoltativamente, modificare il. `region`

6. Scegli Convalida pipeline e assicurati che la convalida abbia esito positivo.
7. Per semplicità, in questo tutorial, configureremo l'accesso pubblico alla pipeline. In Rete, scegli Accesso pubblico.

   Per informazioni sulla configurazione dell'accesso al VPC, vedere. the section called “Configurazione dell'accesso VPC per le pipeline”
8. Mantieni abilitata la pubblicazione dei log in caso di problemi durante il completamento di questo tutorial. Per ulteriori informazioni, consulta the section called “Monaggio aggio aggio aggio aggio aggio aggio aggio”.

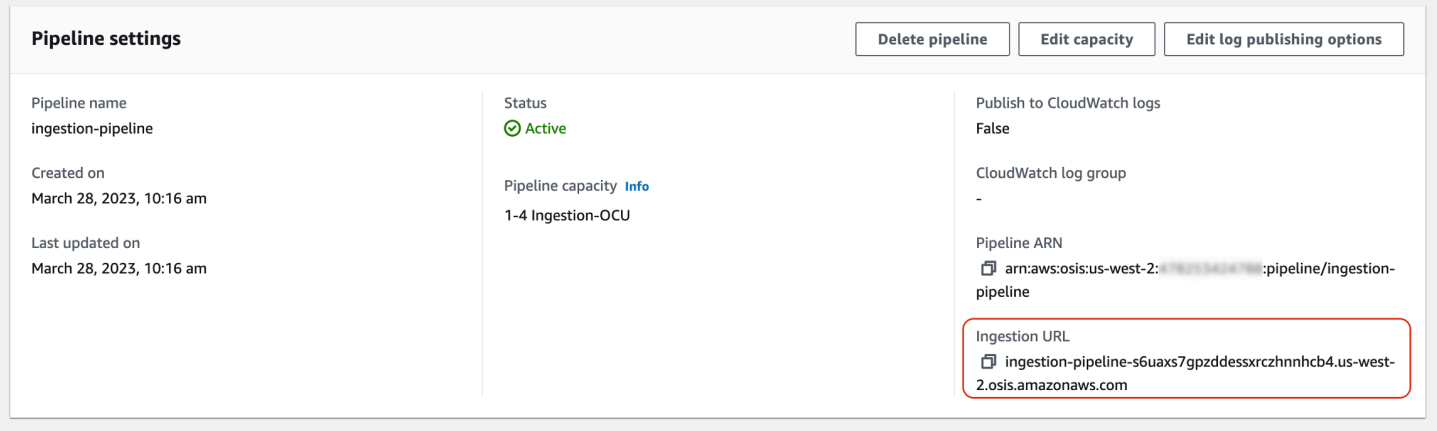
   Specificate il seguente nome del gruppo di log: `/aws/vendedlogs/OpenSearchIngestion/serverless-ingestion/audit-logs`
9. Seleziona Avanti. Controlla la configurazione della pipeline e scegli Crea pipeline. La pipeline impiega 5-10 minuti per diventare attiva.

Fase 4: Inserimento di alcuni dati di esempio

Quando lo stato della pipeline è impostato`Active`, puoi iniziare a importare i dati al suo interno. È necessario firmare tutte le richieste HTTP alla pipeline utilizzando Signature Version 4. Utilizza uno strumento HTTP come Postman o awscurl per inviare alcuni dati alla pipeline. Come per l'indicizzazione dei dati direttamente in una raccolta, l'importazione dei dati in una pipeline richiede sempre un ruolo IAM o una chiave di accesso IAM e una chiave segreta.

> **Note**
>
> Il principale che firma la richiesta deve disporre dell'autorizzazione IAM. `osis:Ingest`

Innanzitutto, ottieni l'URL di importazione dalla pagina delle impostazioni di Pipeline:



Quindi, inserisci alcuni dati di esempio. La seguente richiesta di esempio utilizza awscurl per inviare un singolo file di registro all'indice: `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
```

Dovresti vedere una `200 OK` risposta.

Ora, interroga l'`my_logs`indice per assicurarti che la voce di registro sia stata inserita correttamente:

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

Esempio di risposta:

```
{
   "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"
            }
         }
      ]
   }
}
```


Risorse correlate

Questo tutorial ha presentato un semplice caso d'uso di assimilazione di un singolo documento tramite HTTP. Negli scenari di produzione, configurerai le tue applicazioni client (come Fluent Bit, Kubernetes o OpenTelemetry Collector) per inviare dati a una o più pipeline. Le tue pipeline saranno probabilmente più complesse del semplice esempio di questo tutorial.

Per iniziare a configurare i client e ad acquisire dati, consulta le seguenti risorse:

- Creazione e gestione delle pipeline
- Configurazione dei client per l'invio di dati a Ingestion OpenSearch
- Documentazione Data Prepper

Panoramica delle funzionalità della pipeline in Amazon Ingestion OpenSearch

Amazon OpenSearch Ingestion fornisce pipeline, che consistono in una fonte, un buffer, zero o più processori e uno o più sink. Le pipeline di ingestione sono alimentate da Data Prepper come motore di dati. Per una panoramica dei vari componenti di una pipeline, vedere. the section called “Concetti chiave”

Le seguenti sezioni forniscono una panoramica di alcune delle funzionalità più comunemente utilizzate in Amazon OpenSearch Ingestion.

> **Note**
>
> Questo non è un elenco esaustivo delle funzionalità disponibili per le pipeline. Per una documentazione completa di tutte le funzionalità della pipeline disponibili, consulta la documentazione di Data Prepper. Tieni presente che OpenSearch Ingestion impone alcuni vincoli ai plugin e alle opzioni che puoi utilizzare. Per ulteriori informazioni, consulta the section called “Plugin e opzioni supportati”.

Argomenti

Buffering persistente

Un buffer persistente archivia i dati in un buffer basato su disco su più zone di disponibilità per aggiungere durabilità ai dati. È possibile utilizzare il buffering persistente per importare dati da tutte le fonti basate su push supportate senza la necessità di configurare un buffer autonomo. Questi includono HTTP e OpenTelemetry sorgenti per log, tracce e metriche.

Per abilitare il buffering persistente, scegli Abilita buffer persistente durante la creazione o l'aggiornamento di una pipeline. Per ulteriori informazioni, consulta. the section called “Creazione di pipeline” OpenSearch L'ingestione determina automaticamente la capacità di buffering richiesta in base alle Ingestion OpenSearch Compute Unit (Ingestion OCU) specificate per la pipeline.

Per impostazione predefinita, le pipeline utilizzano an per crittografare i dati del buffer. Chiave di proprietà di AWS Queste pipeline non necessitano di autorizzazioni aggiuntive per il ruolo della pipeline. In alternativa, puoi specificare una chiave gestita dal cliente e aggiungere le seguenti autorizzazioni IAM al ruolo della pipeline:

```
{
    "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"
        }
    ]
}
```

Per ulteriori informazioni, consulta Customer managed keys nella Guida per sviluppatori AWS Key Management Service .

> **Note**
>
> Se disabiliti il buffering persistente, la pipeline verrà aggiornata per essere eseguita interamente con il buffering in memoria.

Ottimizzazione della dimensione massima del payload della richiesta

Se abiliti il buffering persistente per una pipeline, la dimensione massima del payload della richiesta è predefinita a 1 MB. Il valore predefinito offre le migliori prestazioni. Tuttavia, puoi aumentare questo valore se i tuoi clienti inviano richieste superiori a 1 MB. Per ottimizzare la dimensione

massima del payload, impostate l'`max_request_length`opzione all'interno della configurazione di origine. Proprio come il buffering persistente, questa opzione è supportata solo per HTTP e per OpenTelemetry le fonti per log, tracce e metriche.

Gli unici valori validi per l'`max_request_length`opzione sono 1 MB, 1,5 MB, 2 MB, 2,5 MB, 3 MB, 3,5 MB e 4 MB. Se si specifica un valore diverso, viene visualizzato un errore.

L'esempio seguente mostra come configurare la dimensione massima del payload all'interno di una configurazione di pipeline:

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

Se non abilitate il buffering persistente per una pipeline, il valore predefinito dell'`max_request_length`opzione è 10 MB per tutte le fonti e non può essere modificato.

Divisione

È possibile configurare una pipeline di OpenSearch ingestione per suddividere gli eventi in entrata in una sottopipeline, in modo da eseguire diversi tipi di elaborazione sullo stesso evento in entrata.

La pipeline di esempio seguente divide gli eventi in entrata in due sotto-pipeline. Ogni sottopipeline utilizza il proprio processore per arricchire e manipolare i dati, quindi invia i dati a indici diversi. 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"
```

Concatenamento

È possibile concatenare più sotto-pipeline per eseguire l'elaborazione e l'arricchimento dei dati in blocchi. In altre parole, è possibile arricchire un evento in entrata con determinate funzionalità di elaborazione in una sottopipeline, quindi inviarlo a un'altra sottopipeline per un ulteriore arricchimento con un processore diverso e infine inviarlo al relativo sink. OpenSearch

Nell'esempio seguente, la `log_pipeline` sub-pipeline arricchisce un evento di registro in entrata con un set di processori, quindi invia l'evento a un indice denominato. OpenSearch `enriched_logs` La pipeline invia lo stesso evento alla `log_advanced_pipeline` pipeline secondaria, che lo elabora e lo invia a un indice diverso denominato. OpenSearch `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"
```

Code DLQ

Le code DLQ (Dead-letter Queues) sono destinazioni per eventi che una pipeline non riesce a scrivere in un sink. In OpenSearch Ingestion, è necessario specificare un bucket Amazon S3 con autorizzazioni di scrittura appropriate da utilizzare come DLQ. Puoi aggiungere una configurazione DLQ a ogni sink all'interno di una pipeline. Quando una pipeline incontra errori di scrittura, crea oggetti DLQ nel bucket S3 configurato. Gli oggetti DLQ esistono all'interno di un file JSON come una serie di eventi falliti.

Una pipeline scrive eventi nel DLQ quando viene soddisfatta una delle seguenti condizioni:

- I `max_retries` rubinetti per il OpenSearch lavandino sono esauriti. OpenSearch L'ingestione richiede un minimo di 16 per questa opzione.
- Gli eventi vengono rifiutati dal sink a causa di una condizione di errore.

Configurazione

Per configurare una coda di lettere non scritte per una pipeline secondaria, specifica l'`dlq`opzione all'interno della configurazione sink: `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"
```

I file scritti su questo S3 DLQ avranno il seguente schema di denominazione:

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

Per ulteriori informazioni, consulta Dead-Letter Queues (DLQ).

Per istruzioni su come configurare il ruolo, vedere. `sts_role_arn` the section called “Scrittura in una coda di lettere non scritte”

Esempio

Considerate il seguente file DLQ di esempio:

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

Ecco un esempio di dati che non sono stati scritti nel sink e che vengono inviati al bucket DLQ S3 per ulteriori analisi:

```
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"
```

Gestione degli indici

Amazon OpenSearch Ingestion offre molte funzionalità di gestione degli indici, tra cui le seguenti.

Creazione di indici

È possibile specificare un nome di indice in un sink di pipeline e OpenSearch Ingestion crea l'indice quando effettua il provisioning della pipeline. Se esiste già un indice, la pipeline lo utilizza per indicizzare gli eventi in entrata. Se si arresta e si riavvia una pipeline o se si aggiorna la configurazione YAML, la pipeline tenta di creare nuovi indici se non esistono già. Una pipeline non può mai eliminare un indice.

I sinks di esempio seguenti creano due indici quando viene eseguito il provisioning della pipeline:

```
sink:
  - opensearch:
```

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

Generazione di nomi e modelli di indici

È possibile generare nomi di indice dinamici utilizzando variabili dai campi degli eventi in arrivo. Nella configurazione sink, usa il formato `string${}` per segnalare l'interpolazione delle stringhe e usa un puntatore JSON per estrarre i campi dagli eventi. Le opzioni per sono o. `index_type` `custom` `management_disabled` Poiché l'`index_type`impostazione predefinita è per i OpenSearch domini e `custom` `management_disabled` per le raccolte OpenSearch Serverless, può essere lasciata non impostata.

Ad esempio, la seguente pipeline seleziona il `metadataType` campo dagli eventi in entrata per generare i nomi degli indici.

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

La seguente configurazione continua a generare un nuovo indice ogni giorno o ogni ora.

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

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

Il nome dell'indice può anche essere una stringa semplice con un modello data-ora come suffisso, ad esempio. `my-index-%{yyyy.MM.dd}` Quando il sink invia dati a OpenSearch, sostituisce il modello data-ora con l'ora UTC e crea un nuovo indice per ogni giorno, ad esempio. `my-index-2022.01.25` Per ulteriori informazioni, consultate la classe. DateTimeFormatter

Questo nome di indice può anche essere una stringa formattata (con o senza un suffisso del modello data-ora), ad esempio. `my-${index}-name` Quando il sink invia dati a OpenSearch, sostituisce la `"${index}"` parte con il valore dell'evento in fase di elaborazione. Se il formato è`"${index1/index2/index3}"`, sostituisce il campo `index1/index2/index3` con il relativo valore nell'evento.

Generazione degli ID dei documenti

Una pipeline può generare un ID di documento durante l'indicizzazione dei documenti su. OpenSearch Può dedurre questi ID di documento dai campi all'interno degli eventi in arrivo.

Questo esempio utilizza il `uuid` campo di un evento in entrata per generare un ID di documento.

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

Nell'esempio seguente, il processore Add entries unisce i campi `uuid` e `other_field` l'evento in entrata per generare un ID del documento.

L'`create`azione garantisce che i documenti con ID identici non vengano sovrascritti. La pipeline elimina i documenti duplicati senza alcun tentativo o evento DLQ. Si tratta di un'aspettativa ragionevole per gli autori della pipeline che utilizzano questa azione, poiché l'obiettivo è evitare l'aggiornamento dei documenti esistenti.

```
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"
```

Potresti voler impostare l'ID del documento di un evento su un campo di un oggetto secondario. Nell'esempio seguente, il plugin OpenSearch sink utilizza l'oggetto secondario `info/id` per generare un ID del documento.

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

Dato il seguente evento, la pipeline genererà un documento con il `_id` campo impostato su: `json001`

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

Generazione di ID di routing

È possibile utilizzare l'`routing_field`opzione all'interno del plug-in OpenSearch sink per impostare il valore di una proprietà di routing del documento (`_routing`) su un valore proveniente da un evento in arrivo.

Il routing supporta la sintassi del puntatore JSON, quindi sono disponibili anche campi annidati, non solo campi di primo livello.

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

Dato il seguente evento, il plugin genera un documento con il campo impostato su: `_routing` `abcd`

```
{
   "id":"123",
   "metadata":{
```

```
      "id":"abcd",
      "fieldA":"valueA"
   },
   "fieldB":"valueB"
}
```

Per istruzioni su come creare modelli di indice che le pipeline possono utilizzare durante la creazione dell'indice, vedete Modelli di indice.

End-to-end) Riconoscimento

OpenSearch Ingestion garantisce la durata e l'affidabilità dei dati tracciandone la trasmissione dalla fonte ai pozzi nelle condutture stateless mediante riconoscimento. end-to-end Attualmente, solo il plug-in sorgente S3 supporta il riconoscimento. end-to-end

Con il end-to-end riconoscimento, il plug-in pipeline source crea un set di riconoscimenti per monitorare un batch di eventi. Riceve un riconoscimento positivo quando tali eventi vengono inviati con successo ai rispettivi sink o un riconoscimento negativo quando nessuno degli eventi non può essere inviato ai rispettivi sink.

In caso di guasto o arresto anomalo di un componente della pipeline, o se una fonte non riceve una conferma, la fonte scade e intraprende le azioni necessarie, come riprovare o registrare l'errore. Se nella pipeline sono configurati più sink o più subpipeline, i riconoscimenti a livello di evento vengono inviati solo dopo che l'evento è stato inviato a tutti i sink di tutte le pipeline secondarie. Se un sink ha un DLQ configurato, i riconoscimenti tengono traccia anche degli eventi scritti nel DLQ. end-to-end

Per abilitare la end-to-end conferma, includi l'opzione nella `acknowledgments` configurazione di origine:

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

Contropressione alla fonte

Una pipeline può subire una contropressione quando è impegnata nell'elaborazione dei dati o se i suoi sink sono temporaneamente inattivi o rallentano l'acquisizione dei dati. OpenSearch Ingestion ha diversi modi di gestire la contropressione a seconda del plug-in di origine utilizzato da una pipeline.

Origine HTTP

Le pipeline che utilizzano il plug-in di origine HTTP gestiscono la contropressione in modo diverso a seconda del componente della pipeline che è congestionato:

- Buffer: quando i buffer sono pieni, la pipeline inizia a restituire lo stato HTTP `REQUEST_TIMEOUT` con il codice di errore 408 all'endpoint di origine. Quando i buffer vengono liberati, la pipeline riavvia l'elaborazione degli eventi HTTP.
- Thread di origine: quando tutti i thread di origine HTTP sono impegnati nell'esecuzione di richieste e la dimensione della coda delle richieste non elaborate ha superato il numero massimo consentito di richieste, la pipeline inizia a restituire lo stato HTTP `TOO_MANY_REQUESTS` con il codice di errore 429 all'endpoint di origine. Quando la coda delle richieste scende al di sotto della dimensione massima consentita, la pipeline riavvia l'elaborazione delle richieste.

Fonte Otel

Quando i buffer sono pieni per le pipeline che utilizzano OpenTelemetry sorgenti (otEL logs, otEL metrics e OTel trace), la pipeline inizia a restituire lo stato HTTP `REQUEST_TIMEOUT` con il codice di errore 408 all'endpoint di origine. Quando i buffer vengono liberati, la pipeline riprende a elaborare gli eventi.

Fonte S3

Quando i buffer sono pieni per le pipeline con una sorgente S3, le pipeline interrompono l'elaborazione delle notifiche SQS. Man mano che i buffer vengono liberati, le pipeline riprendono a elaborare le notifiche.

Se un sink è inattivo o non è in grado di inserire dati e la end-to-end conferma è abilitata per la fonte, la pipeline interrompe l'elaborazione delle notifiche SQS finché non riceve un riconoscimento riuscito da tutti i sink.

Creazione di pipeline Amazon OpenSearch Ingestion

Una pipeline è il meccanismo utilizzato da Amazon OpenSearch Ingestion per spostare i dati dalla fonte (da cui provengono i dati) al relativo sink (dove vanno i dati). In OpenSearch Ingestion, il sink sarà sempre un singolo dominio Amazon OpenSearch Service, mentre la fonte dei dati potrebbe essere costituita da client come Amazon S3, Fluent Bit o Collector. OpenTelemetry

Per ulteriori informazioni, consulta Pipelines nella documentazione. OpenSearch

Argomenti

Prerequisiti e ruoli richiesti

Per creare una pipeline di OpenSearch ingestione, è necessario disporre delle seguenti risorse:

- Un ruolo IAM che OpenSearch Ingestion assumerà per scrivere nel sink. Includerai questo ruolo ARN nella configurazione della pipeline.
- Un dominio OpenSearch di servizio o una raccolta OpenSearch Serverless che funge da sink. Se stai scrivendo su un dominio, deve essere in esecuzione OpenSearch 1.0 o versione successiva oppure Elasticsearch 7.4 o versione successiva. Il sink deve disporre di una politica di accesso che conceda le autorizzazioni appropriate al ruolo della pipeline IAM.

Per istruzioni su come creare queste risorse, consulta i seguenti argomenti:

- the section called “Concedere alle pipeline l'accesso ai domini”
- the section called “Concedere alle pipeline l'accesso alle raccolte”

> **Note**
>
> Se stai scrivendo su un dominio che utilizza un controllo granulare degli accessi, devi completare alcuni passaggi aggiuntivi. Per informazioni, consulta the section called “Passaggio 3: mappare il ruolo della pipeline (solo per i domini che utilizzano un controllo di accesso granulare)”.

Autorizzazioni richieste

OpenSearch Ingestion utilizza le seguenti autorizzazioni IAM per creare pipeline:

- `osis:CreatePipeline`— Creare una pipeline.
- `osis:ValidatePipeline`— Verificare se la configurazione di una tubazione è valida.
- `iam:PassRole`— Passa il ruolo della pipeline a OpenSearch Ingestion in modo che possa scrivere dati nel dominio. Questa autorizzazione deve essere sulla risorsa del ruolo della pipeline (l'ARN specificato per l'opzione nella configurazione `sts_role_arn` della pipeline) o * semplicemente se prevedi di utilizzare ruoli diversi in ciascuna pipeline.

Ad esempio, la seguente politica concede l'autorizzazione a creare una pipeline:

```
{
   "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 include anche un'autorizzazione chiamata`osis:Ingest`, necessaria per inviare richieste firmate alla pipeline utilizzando Signature Version 4. Per ulteriori informazioni, consulta the section called “Creazione di un ruolo di importazione”.

> **Note**
>
> Inoltre, il primo utente che crea una pipeline in un account deve disporre delle autorizzazioni per l'azione. `iam:CreateServiceLinkedRole` Per ulteriori informazioni, consulta pipeline role resource.

Per ulteriori informazioni su ciascuna autorizzazione, vedere Azioni, risorse e chiavi di condizione per l' OpenSearch ingestione nel Service Authorization Reference.

Specificare la versione della pipeline

Quando si configura una pipeline, è necessario specificare la versione principale di Data Prepper che verrà eseguita dalla pipeline. Per specificare la versione, includi l'`version`opzione nella configurazione della pipeline:

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

Quando scegliete Crea, OpenSearch Ingestion determina l'ultima versione secondaria disponibile della versione principale specificata e fornisce la pipeline con quella versione. Ad esempio, se si specifica e l'ultima versione supportata di Data Prepper è la 2.1.1`version: "2"`, OpenSearch Ingestion esegue il provisioning della pipeline con la versione 2.1.1. Non mostriamo pubblicamente la versione secondaria in esecuzione nella tua pipeline.

Per aggiornare la pipeline quando è disponibile una nuova versione principale di Data Prepper, modifica la configurazione della pipeline e specifica la nuova versione. Non puoi effettuare il downgrade di una pipeline a una versione precedente.

> **Note**
>
> OpenSearch Ingestion non supporta immediatamente le nuove versioni di Data Prepper non appena vengono rilasciate. Si verificherà un certo ritardo tra il momento in cui una nuova versione sarà disponibile pubblicamente e il momento in cui sarà supportata in Ingestion. OpenSearch Inoltre, OpenSearch Ingestion potrebbe esplicitamente non supportare del tutto

determinate versioni principali o secondarie. Per un elenco completo, consulta the section called “Versioni di Data Prepper supportate”.

Ogni volta che apporti una modifica alla pipeline che avvia una distribuzione blu/verde, OpenSearch Ingestion può aggiornarla all'ultima versione secondaria della versione principale attualmente configurata nel file YAML della pipeline. the section called “Implementazioni blu/verdi per gli aggiornamenti della pipeline”Per ulteriori informazioni, consulta. OpenSearch L'ingestione non può modificare la versione principale della pipeline a meno che non aggiorni esplicitamente l'`version`opzione all'interno della configurazione della pipeline.

Specificare il percorso di ingestione

Per le fonti basate su pull come Otel trace e OTel metrics, OpenSearch Ingestion richiede l'opzione aggiuntiva nella configurazione del codice sorgente. `path` Il percorso è una stringa come`/log/ingest`, che rappresenta il percorso URI per l'ingestione. Questo percorso definisce l'URI utilizzato per inviare dati alla pipeline.

Ad esempio, supponiamo di specificare la seguente sottopipeline di ingresso per una pipeline di ingestione denominata: `logs`

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

Quando si inseriscono dati nella pipeline, è necessario specificare il seguente endpoint nella configurazione del client:. `https://logs-abcdefgh.us-west-2.osis.amazonaws.com/my/test_path`

Il percorso deve iniziare con una barra (/) e può contenere i caratteri speciali '-', '_', ' . 'e'/', oltre al `${pipelineName}` segnaposto. Se si utilizza `${pipelineName}` (ad esempio`path: "/${pipelineName}/test_path"`), la variabile viene sostituita con il nome della pipeline secondaria associata. In questo esempio, lo sarebbe. `https://logs.us-west-2.osis.amazonaws.com/entry-pipeline/test_path`

Creazione di pipeline

Questa sezione descrive come creare pipeline di OpenSearch ingestione utilizzando la console di OpenSearch servizio e il. AWS CLI

Console

Per creare una pipeline

1. Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegli Pipelines nel riquadro di navigazione a sinistra e scegli Crea pipeline.
3. Immetti un nome per la pipeline
4. (Facoltativo) Scegliete Abilita buffer persistente. Un buffer persistente archivia i dati in un buffer basato su disco su più AZ. Per ulteriori informazioni, consulta Buffering persistente. Se abiliti il buffer persistente, seleziona la AWS Key Management Service chiave per crittografare i dati del buffer.
5. Configura la capacità minima e massima della pipeline nelle Ingestion Compute OpenSearch Units (OCU). Per ulteriori informazioni, consulta the section called “Scalabilità delle pipeline”.
6. In Configurazione Pipeline, fornite la configurazione della pipeline in formato YAML. Un singolo file di configurazione della pipeline può contenere 1-10 sotto-pipeline. Ogni sub-pipeline è una combinazione di un'unica fonte, zero o più processori e un singolo sink. Per OpenSearch Ingestion, il sink deve sempre essere un dominio di servizio. OpenSearch Per un elenco delle opzioni supportate, vedere. the section called “Plugin e opzioni supportati”

   > **Note**
   >
   > È necessario includere le `sigv4` opzioni `sts_role_arn` e in ogni pipeline secondaria. La pipeline assume il ruolo definito in `sts_role_arn` per firmare le richieste al dominio. Per ulteriori informazioni, consulta the section called “Concedere alle pipeline l'accesso ai domini”.

   Il seguente file di configurazione di esempio utilizza il codice sorgente HTTP e i plugin Grok per elaborare dati di registro non strutturati e inviarli a un dominio di servizio. OpenSearch La pipeline secondaria è denominata. `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**
>
> Se si specificano più sink all'interno di una definizione di pipeline YAML, devono appartenere tutti allo stesso dominio di servizio. OpenSearch Una pipeline OpenSearch di ingestione non può scrivere su più domini diversi.

Puoi creare la tua configurazione di pipeline oppure scegliere Carica file e importare una configurazione esistente per una pipeline Data Prepper autogestita. In alternativa, puoi utilizzare un blueprint di configurazione.

7. Dopo aver configurato la pipeline, scegli Convalida pipeline per confermare che la configurazione è corretta. Se la convalida fallisce, correggi gli errori ed esegui nuovamente la convalida.
8. In Configurazione di rete, scegli Accesso VPC o Accesso pubblico. Se si sceglie Public access (Accesso pubblico), andare al passaggio successivo. Se scegli l'accesso VPC, configura le seguenti impostazioni:

Impostazione	Descrizione
Gestione degli endpoint	Scegliete se volete creare voi stessi gli endpoint VPC o lasciateli creare da OpenSearch Ingestion per voi. Per impostazione predefini ta, la gestione degli endpoint utilizza gli endpoint gestiti da Ingestion. OpenSearch
VPC	Scegli l'ID per il cloud privato virtuale (VPC) da utilizzare. Il VPC e la pipeline devono trovarsi nello stesso ambiente. Regione AWS
Sottoreti	Scegli una o più sottoreti. OpenSearch Il servizio inserirà un endpoint VPC e interfacce di rete elastiche nelle sottoreti.
Gruppi di sicurezza	Scegli uno o più gruppi di sicurezza VPC che consentano all'applicazione richiesta di raggiungere la pipeline di OpenSearch ingestione sulle porte (80 o 443) e sui protocolli (HTTP o HTTPS) esposti dalla pipeline.
Opzioni di collegamento VPC	Se la tua fonte è un endpoint autogestito, collega la pipeline a un VPC. Scegli una delle opzioni CIDR predefinite fornite o utilizza un CIDR personalizzato.

Per ulteriori informazioni, consulta the section called “Configurazione dell'accesso VPC per le pipeline”.

9. (Facoltativo) In Tag, aggiungi uno o più tag (coppie chiave-valore) alla tua pipeline. Per ulteriori informazioni, consulta the section called “Etichettatura delle tubazioni”.
10. (Facoltativo) In Opzioni di pubblicazione dei log, attiva la pubblicazione dei log della pipeline su Amazon CloudWatch Logs. Ti consigliamo di abilitare la pubblicazione dei log in modo da poter risolvere più facilmente i problemi relativi alla pipeline. Per ulteriori informazioni, consulta la pagina the section called “Monaggio aggio aggio aggio aggio aggio aggio aggio aggio”.
11. Seleziona Next (Successivo).
12. Controlla la configurazione della pipeline e scegli Crea.

OpenSearch Ingestion esegue un processo asincrono per creare la pipeline. Una volta raggiunto lo stato della pipeline, puoi iniziare a importare i dati`Active`.

AWS CLI

Il comando create-pipeline accetta la configurazione della pipeline come stringa o all'interno di un file.yaml. Se fornite la configurazione come stringa, ogni nuova riga deve essere scappata con. `\n` Ad esempio, `"log-pipeline:\n source:\n http:\n processor:\n - grok:\n ...`

Il seguente comando di esempio crea una pipeline con la seguente configurazione:

- Minimo 4 OCU di ingestione, massimo 10 OCU di ingestione
- Fornito all'interno di un cloud privato virtuale (VPC)
- Pubblicazione dei log abilitata

```
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 esegue un processo asincrono per creare la pipeline. Una volta raggiunto lo stato della pipeline, puoi iniziare a importare i dati`Active`. Per controllare lo stato della pipeline, utilizzate il comando. GetPipeline

OpenSearch API di ingestione

Per creare una pipeline OpenSearch di ingestione utilizzando l'API Ingestion, chiama l' OpenSearch operazione. CreatePipeline

Dopo aver creato correttamente la pipeline, puoi configurare il client e iniziare a importare dati nel tuo dominio di servizio. OpenSearch Per ulteriori informazioni, consulta the section called “Utilizzo delle integrazioni di pipeline”.

Monitoraggio dello stato della creazione della pipeline

È possibile tenere traccia dello stato di una pipeline man mano che OpenSearch Ingestion la rifornisce e la prepara per l'importazione dei dati.

Console

Dopo aver creato inizialmente una pipeline, questa passa attraverso più fasi man mano OpenSearch che Ingestion la prepara per l'inserimento dei dati. Per visualizzare le varie fasi della creazione della pipeline, scegliete il nome della pipeline per visualizzarne la pagina delle impostazioni della pipeline. In Stato, scegliete Visualizza dettagli.

Una pipeline passa attraverso le seguenti fasi prima di essere disponibile per l'acquisizione dei dati:

- Convalida: convalida della configurazione della pipeline. Una volta completata questa fase, tutte le convalide hanno avuto esito positivo.
- Crea ambiente: preparazione e approvvigionamento delle risorse. Al termine di questa fase, è stato creato il nuovo ambiente di pipeline.
- Distribuisci pipeline: distribuzione della pipeline. Una volta completata questa fase, la pipeline è stata implementata con successo.
- Verifica dello stato della pipeline: verifica dello stato della pipeline. Una volta completata questa fase, tutti i controlli sanitari sono stati superati.
- Abilita il traffico: consente alla pipeline di importare dati. Una volta completata questa fase, puoi iniziare a importare i dati nella pipeline.

CLI

Utilizzate il get-pipeline-change-progresscomando per controllare lo stato di una pipeline. La seguente AWS CLI richiesta verifica lo stato di una pipeline denominata: `my-pipeline`

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

Risposta:

```
{
   "ChangeProgressStatuses": {
      "ChangeProgressStages": [
         {
            "Description": "Validating pipeline configuration",
            "LastUpdated": 1.671055851E9,
            "Name": "VALIDATION",
            "Status": "PENDING"
```

```
            }
        ],
        "StartTime": 1.671055851E9,
        "Status": "PROCESSING",
        "TotalNumberOfStages": 5
    }
}
```

OpenSearch API di ingestione

Per tenere traccia dello stato della creazione della pipeline utilizzando l'API OpenSearch Ingestion, chiama l'operazione. GetPipelineChangeProgress

Utilizzo dei blueprint per creare una pipeline

Invece di creare una definizione di pipeline partendo da zero, è possibile utilizzare i blueprint di configurazione, che sono modelli YAML preconfigurati per scenari di ingestione comuni come Trace Analytics o i log di Apache. I blueprint di configurazione consentono di effettuare facilmente il provisioning delle pipeline senza dover creare una configurazione da zero.

Console

Per utilizzare un blueprint di pipeline

1. Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegli Pipelines nel riquadro di navigazione a sinistra e scegli Crea pipeline.
3. Seleziona un progetto. La configurazione della pipeline viene compilata con una pipeline secondaria per il caso d'uso selezionato.
4. Esamina il testo commentato che ti guida nella configurazione del blueprint.

> **Important**
>
> Il blueprint della pipeline non è valido così com'è. È necessario apportare alcune modifiche, ad esempio fornire l'ARN Regione AWS e il ruolo da utilizzare per l'autenticazione, altrimenti la convalida della pipeline avrà esito negativo.

CLI

Per ottenere un elenco di tutti i blueprint disponibili utilizzando il AWS CLI, invia una richiesta. list-pipeline-blueprints

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

La richiesta restituisce un elenco di tutti i blueprint disponibili.

Per ottenere informazioni più dettagliate su un progetto specifico, usa il get-pipeline-blueprintcomando:

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

Questa richiesta restituisce il contenuto del blueprint della pipeline di log di 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 di ingestione

Per ottenere informazioni sui progetti di pipeline utilizzando l'API OpenSearch Ingestion, utilizza le operazioni and. ListPipelineBlueprintsGetPipelineBlueprint

Visualizzazione delle pipeline OpenSearch di Amazon Ingestion

Puoi visualizzare i dettagli di una pipeline Amazon OpenSearch Ingestion utilizzando l'APIAWS Management Console, la o l'OpenSearchIngestion API. AWS CLI

Console

Per visualizzare una pipeline

1. Accedi alla console dei OpenSearch servizi Amazon all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegliete Pipelines nel riquadro di navigazione a sinistra.
3. (Facoltativo) Per visualizzare le tubazioni con uno stato particolare, scegliete Qualsiasi stato e selezionate uno stato in base al quale filtrare.

   Una pipeline può avere i seguenti stati:

   - `Creating`— La pipeline è in fase di creazione.
   - `Active`— La pipeline è attiva e pronta per l'acquisizione di dati.
   - `Updating`— La pipeline è in fase di aggiornamento.
   - `Deleting`— La pipeline è in fase di eliminazione.
   - `Create failed`— Impossibile creare la pipeline.
   - `Update failed`— La pipeline non può essere aggiornata.
   - `Starting`— Il gasdotto sta iniziando.
   - `Start failed`— La pipeline non può essere avviata.
   - `Stopping`— Il gasdotto è in fase di arresto.

- `Stopped`— La pipeline viene interrotta e può essere riavviata in qualsiasi momento.

Non ti vengono fatturate le OCU di importazione quando una pipeline è negli stati`Create failed`,, `Creating` e. `Deleting` `Stopped`

CLI

Per visualizzare le pipeline utilizzando ilAWS CLI, invia una richiesta list-pipelines:

```
aws osis list-pipelines
```

La richiesta restituisce un elenco di tutte le pipeline esistenti:

```
{
    "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."
            }
        }
    ]
```

```
}
```

Per ottenere informazioni su una singola pipeline, usa il comando get-pipeline:

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

La richiesta restituisce le informazioni di configurazione per la pipeline specificata:

```
{
    "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"
        ]
    }
}
```

OpenSearchAPI di ingestione

Per visualizzare le pipeline OpenSearch di ingestione utilizzando l'API di OpenSearch ingestione, chiama le operazioni and. ListPipelinesGetPipeline

Aggiornamento delle pipeline di Amazon OpenSearch Ingestion

Puoi aggiornare le pipeline OpenSearch di Amazon Ingestion utilizzando l' AWS Management Console, la o l' OpenSearch API AWS CLI Ingestion. OpenSearch Ingestion avvia una distribuzione

blu/verde quando aggiorni la configurazione YAML di una pipeline. Per ulteriori informazioni, consulta the section called “Implementazioni blu/verdi per gli aggiornamenti della pipeline”.

Argomenti

Considerazioni

Quando aggiorni una pipeline, considera quanto segue:

- Puoi modificare i limiti di capacità di una pipeline, le opzioni di pubblicazione dei log e la configurazione YAML. Non puoi modificarne il nome o le impostazioni di rete.
- Se la pipeline scrive su un sink di dominio VPC, non puoi tornare indietro e modificare il sink in un dominio VPC diverso dopo la creazione della pipeline. È necessario eliminare e ricreare la pipeline con il nuovo sink. Puoi comunque passare il sink da un dominio VPC a un dominio pubblico, da un dominio pubblico a un dominio VPC o da un dominio pubblico a un altro dominio pubblico.
- È possibile passare il sink della pipeline in qualsiasi momento da un dominio di OpenSearch servizio pubblico a una raccolta Serverless. OpenSearch
- Quando aggiorni la configurazione YAML di una pipeline, OpenSearch Ingestion avvia una distribuzione blu/verde. Per ulteriori informazioni, consulta the section called “Implementazioni blu/verdi per gli aggiornamenti della pipeline”.
- Quando si aggiorna la configurazione YAML di una pipeline, OpenSearch Ingestion aggiorna automaticamente la pipeline all'ultima versione secondaria supportata della versione principale di Data Prepper specificata nella configurazione della pipeline. Questo processo mantiene la pipeline aggiornata con le ultime correzioni di bug e i miglioramenti delle prestazioni.
- Puoi comunque aggiornare la tua pipeline quando viene interrotta.

Autorizzazioni richieste

OpenSearch Ingestion utilizza le seguenti autorizzazioni IAM per l'aggiornamento delle pipeline:

- `osis:UpdatePipeline`— Aggiornare una pipeline.

- `osis:ValidatePipeline`— Verificare se la configurazione di una tubazione è valida.
- `iam:PassRole`— Passa il ruolo della pipeline a OpenSearch Ingestion in modo che possa scrivere dati nel dominio. Questa autorizzazione è richiesta solo se stai aggiornando la configurazione YAML della pipeline, non se stai modificando altre impostazioni come la pubblicazione dei log o i limiti di capacità.

Ad esempio, la seguente politica concede l'autorizzazione all'aggiornamento di una pipeline:

```
{
   "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"
         ]
      }
   ]
}
```

Aggiornamento delle pipeline

Puoi aggiornare le pipeline OpenSearch di Amazon Ingestion utilizzando l' AWS Management Console, la o l' OpenSearch API AWS CLI Ingestion.

Console

Per aggiornare una pipeline

1. Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegli Pipelines nel riquadro di navigazione a sinistra.
3. Scegli una pipeline per aprirne le impostazioni. Puoi modificare i limiti di capacità di una pipeline, le opzioni di pubblicazione dei log e la configurazione YAML. Non puoi modificarne il nome o le impostazioni di rete.
4. Una volta completate le modifiche, scegli Save (Salva).

CLI

Per aggiornare una pipeline utilizzando AWS CLI, invia una richiesta di update-pipeline. La seguente richiesta di esempio carica un nuovo file di configurazione e aggiorna i valori di capacità minima e massima:

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

OpenSearch API di ingestione

Per aggiornare una pipeline OpenSearch di ingestione utilizzando l'API Ingestion, chiamate l' OpenSearch operazione. UpdatePipeline

Implementazioni blu/verdi per gli aggiornamenti della pipeline

OpenSearch L'ingestione avvia un processo di distribuzione blu/verde quando si aggiorna la configurazione YAML di una pipeline.

Il blu/verde si riferisce alla pratica di creare un nuovo ambiente per gli aggiornamenti della pipeline e di indirizzare il traffico verso il nuovo ambiente dopo il completamento di tali aggiornamenti. In questo modo si riducono al minimo i tempi di inattività e si mantiene l'ambiente originale nel caso in cui ci siano problemi nella distribuzione al nuovo ambiente. Le implementazioni blu/verdi di per sé non

hanno alcun impatto sulle prestazioni, ma le prestazioni potrebbero cambiare se la configurazione della pipeline cambia in modo tale da alterare le prestazioni.

OpenSearch L'ingestione blocca l'auto-scaling durante le implementazioni blu/green. Continuerai a essere addebitato solo per il traffico verso la vecchia pipeline fino a quando non viene reindirizzato alla nuova pipeline. Una volta che il traffico è stato reindirizzato, ti verrà addebitato solo il costo della nuova pipeline. Non ti vengono mai addebitati costi per due pipeline contemporaneamente.

Quando aggiorni il file di configurazione YAML di una pipeline, OpenSearch Ingestion può aggiornare automaticamente la pipeline all'ultima versione secondaria supportata della versione principale di Data Prepper specificata nella configurazione della pipeline. Ad esempio, è possibile che `version: "2"` nella configurazione della pipeline Ingestion abbia inizialmente fornito alla pipeline la versione 2.1.0. OpenSearch Quando viene aggiunto il supporto per la versione 2.1.1 e si apporta una modifica alla configurazione della pipeline, Ingestion aggiorna la pipeline alla versione 2.1.1. OpenSearch

Questo processo mantiene la pipeline aggiornata con le ultime correzioni di bug e i miglioramenti delle prestazioni. OpenSearch Ingestion non può aggiornare la versione principale della pipeline a meno che non si modifichi manualmente l'`version`opzione all'interno della configurazione della pipeline.

Interruzione e avvio delle pipeline di Amazon OpenSearch Ingestion

Avviare e arrestare le pipeline Amazon OpenSearch Ingestion aiuta a gestire i costi degli ambienti di test e sviluppo. Puoi arrestare temporaneamente una pipeline invece di impostarla e rimozione ogni volta che utilizzi la pipeline.

Argomenti

Panoramica dell'avvio e dell'arresto di una pipeline di OpenSearch ingestione

È possibile interrompere una pipeline nei periodi in cui non è necessario inserire dati al suo interno. Puoi avviare nuovamente la pipeline ogni volta che devi utilizzarla. L'avvio e l'arresto semplificano i

processi di impostazione e rimozione delle pipeline utilizzate per lo sviluppo, i test o attività simili che non richiedono una disponibilità continua.

Quando la pipeline è arrestata, non viene addebitato alcun costo per le ore dell'Ingestion OCU. Puoi comunque aggiornare le pipeline interrotte e queste ricevono aggiornamenti automatici delle versioni secondarie e patch di sicurezza.

Non utilizzare l'avvio e l'arresto se la pipeline deve rimanere in esecuzione ma ha più capacità di quanta ne occorre. Se la tua pipeline è troppo costosa o poco trafficata, valuta la possibilità di ridurne i limiti di capacità massima. Per ulteriori informazioni, consulta the section called “Scalabilità delle pipeline”.

Arresto di una pipeline di OpenSearch ingestione

Per utilizzare una pipeline di OpenSearch ingestione o eseguire l'amministrazione, è necessario iniziare sempre con una pipeline attiva, quindi interrompere la pipeline e quindi riavviare la pipeline. Quando la pipeline è arrestata, non è previsto alcun costo per le ore dell'Ingestion OCU.

Console

Arresto di una pipeline

1. Accedi alla console del OpenSearch servizio Amazon all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel riquadro di navigazione, scegli pipeline e quindi seleziona una pipeline. Si può eseguire l'operazione di arresto da questa pagina o andare alla pagina dei dettagli della pipeline da arrestare.
3. Per Azioni, scegli Stop pipeline.

   Se una pipeline non può essere fermata e avviata, l'azione Arresta pipeline non è disponibile.

AWS CLI

Per arrestare una pipeline tramiteAWS CLI, chiamare il comando stop-pipeline con i parametri seguenti:

- `--pipeline-name`— il nome della pipeline.

Example

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

OpenSearchAPI di ingestione

Per arrestare una pipeline tramite l'API OpenSearch di inserimento, chiamare l'StopPipelineoperazione con il parametro seguente:

- `PipelineName`— il nome della pipeline.

Avvio di una pipeline OpenSearch di ingestione

Puoi sempre avviare una pipeline OpenSearch di importazione partendo da una pipeline che è già nello stato di arresto. La pipeline mantiene le sue impostazioni di impostazione, come i limiti di capacità, le impostazioni di rete e le opzioni di pubblicazione dei log.

Il riavvio di una pipeline richiede in genere alcuni minuti.

Console

Per avviare una pipeline

1. Accedi alla console del OpenSearch servizio Amazon all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel riquadro di navigazione, scegli pipeline e quindi seleziona una pipeline. Si può eseguire l'operazione di avvio da questa pagina o andare alla pagina dei dettagli della pipeline da avviare.
3. Per Azioni, scegli Avvia pipeline.

AWS CLI

Per avviare una pipeline tramiteAWS CLI, chiamare il comando start-pipeline con i parametri seguenti:

- `--pipeline-name`— il nome della pipeline.

Example

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

OpenSearchAPI di ingestione

Per avviare una pipeline OpenSearch di ingestione utilizzando l'API di OpenSearch ingestione, chiama l'StartPipelineoperazione con il seguente parametro:

- `PipelineName`— il nome della pipeline.

Eliminazione delle pipeline di Amazon OpenSearch Ingestion

Puoi eliminare una pipeline di Amazon OpenSearch Ingestion utilizzando l'APIAWS Management Console, la o l'AWS CLIOpenSearchIngestion API. Non è possibile eliminare una pipeline con lo stato di `Creating` o`Updating`.

Console

Per eliminare una pipeline

1. Scegli la console del OpenSearch servizio Amazon che si intendono eliminare. https://console.aws.amazon.com/aos/home
2. Scegliete Pipelines nel riquadro di navigazione a sinistra.
3. Selezionare la pipeline che si intendono eliminare e scegli Elimina.
4. Per confermare l'eliminazione, scegliere Delete (Elimina).

CLI

Per eliminare una pipeline utilizzandoAWS CLI, invia una richiesta di eliminazione della pipeline:

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

OpenSearchAPI di ingestione

Per eliminare una pipeline OpenSearch di ingestione utilizzando l'API di OpenSearch ingestione, chiama l'DeletePipelineoperazione con il seguente parametro:

- `PipelineName`— il nome della pipeline.

Plugin e opzioni supportati per le pipeline di Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion supporta un sottoinsieme di sorgenti, processori e sink rispetto all'open source Data Prepper. Inoltre, OpenSearch Ingestion impone alcuni vincoli alle opzioni disponibili per ogni plug-in supportato. Le sezioni seguenti descrivono i plugin e le opzioni associate supportati da Ingestion. OpenSearch

> **Note**
>
> OpenSearch Ingestion non supporta alcun plugin buffer perché configura automaticamente un buffer predefinito. Si riceve un errore di convalida se si include un buffer nella configurazione della pipeline.

Argomenti

Plugin supportati

OpenSearch Ingestion supporta i seguenti plugin Data Prepper:

Fonti:

- Amazon DocumentDB
- DynamoDB
- OpenSearch

- HTTP
- Kafka

- Registri degli hotel
- Metriche dell'Otel
- Traccia dell'hotel
- S3

Processori:

- Aggregazione
- Rilevatore di anomalie
- CSV
- Data
- Decomprimi
- Sezionare
- Elimina gli eventi
- IP geografico
- Grok
- Valore chiave
- Mappa da elencare
- Evento di mutazione (serie di processori)
- Stringa mutata (serie di processori)
- Offuscare
- Metriche Otel
- Gruppo Otel Trace
- Otel trace
- Icona di analisi
- Analizza JSON
- Analizza XML
- Seleziona le voci
- Mappa dei servizi
- Trace peer forwarder

- Troncare
- Agente utente

Lavelli:

- OpenSearch(supporta OpenSearch Service, OpenSearch Serverless ed Elasticsearch 6.8 o versioni successive)
- S3

Codec Sink:

- Avro
- NDJSON
- JSON
- Parquet

Processori stateless e processori stateful

I processori stateless eseguono operazioni come trasformazioni e filtri, mentre i processori stateful eseguono operazioni come le aggregazioni, che ricordano il risultato dell'esecuzione precedente. OpenSearch Ingestion supporta i processori stateful Aggregate e Service-map. Tutti gli altri processori supportati sono stateless.

Per le pipeline che contengono solo processori stateless, il limite di capacità massima è di 96 OCU di ingestione. Se una pipeline contiene processori con stato, il limite di capacità massima è 48 OCU di Ingestion. Tuttavia, se una pipeline ha il buffering persistente abilitato, può avere un massimo di 384 OCU di ingestione con solo processori stateless o 192 OCU di ingestione se contiene processori con stato. Per ulteriori informazioni, consulta the section called “Scalabilità delle pipeline”.

Il riconoscimento E è supportato solo per i processori stateless. nd-to-end Per ulteriori informazioni, consulta the section called “End-to-end) Riconoscimento”.

Requisiti e vincoli di configurazione

Se non diversamente specificato di seguito, tutte le opzioni descritte nel riferimento alla configurazione di Data Prepper per i plugin supportati sopra elencati sono consentite nelle pipeline

di Ingestion. OpenSearch Le sezioni seguenti spiegano i vincoli che Ingestion impone a determinate opzioni del plug-in. OpenSearch

> **Note**
>
> OpenSearch Ingestion non supporta alcun plugin buffer perché configura automaticamente un buffer predefinito. Si riceve un errore di convalida se si include un buffer nella configurazione della pipeline.

Molte opzioni sono configurate e gestite internamente da OpenSearch Ingestion, come e. `authentication` `acm_certificate_arn` Altre opzioni, come `thread_count` e`request_timeout`, hanno un impatto sulle prestazioni se modificate manualmente. Pertanto, questi valori sono impostati internamente per garantire prestazioni ottimali delle pipeline.

Infine, alcune opzioni non possono essere passate a OpenSearch Ingestion, ad esempio `ism_policy_file` and`sink_template`, perché sono file locali se eseguite in Data Prepper open source. Questi valori non sono supportati.

Argomenti

- Opzioni generali della pipeline
- Processore Grok
- Origine HTTP
- OpenSearch lavandino
- Fonte delle metriche OTel, sorgente di traccia OTel e origine dei registri OTel
- Processore del gruppo di traccia Otel
- Processore di traccia Otel
- Processore Service-map
- Fonte S3

Opzioni generali della pipeline

Le seguenti opzioni generali di pipeline sono impostate da OpenSearch Ingestion e non sono supportate nelle configurazioni della pipeline:

- `workers`

- `delay`

Processore Grok

Le seguenti opzioni del processore Grok non sono supportate:

- `patterns_directories`
- `patterns_files_glob`

Origine HTTP

Il plugin sorgente HTTP ha i seguenti requisiti e vincoli:

- L'*`path`*opzione è obbligatoria. Il percorso è una stringa come`/log/ingest`, che rappresenta il percorso URI per l'inserimento dei log. Questo percorso definisce l'URI utilizzato per inviare dati alla pipeline. Ad esempio, `https://log-pipeline.us-west-2.osis.amazonaws.com/log/ingest`. Il percorso deve iniziare con una barra (/) e può contenere i caratteri speciali '-', '_', '. 'e'/', oltre al `${pipelineName}` segnaposto.
- Le seguenti opzioni di origine HTTP sono impostate da OpenSearch Ingestion e non sono supportate nelle configurazioni della pipeline:
  - `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 lavandino

Il plugin OpenSearchsink presenta i seguenti requisiti e limitazioni.

- L'`aws`opzione è obbligatoria e deve contenere le seguenti opzioni:
  - `sts_role_arn`
  - `region`
  - `hosts`
  - `serverless`(se il sink è una raccolta OpenSearch Serverless)
- L'`sts_role_arn`opzione deve puntare allo stesso ruolo per ogni sink all'interno di un file di definizione YAML.
- L'`hosts`opzione deve specificare un endpoint del dominio OpenSearch di servizio o un endpoint di raccolta OpenSearch Serverless. Tutti gli host all'interno di un file di definizione YAML devono puntare allo stesso endpoint. Non è possibile specificare un endpoint personalizzato per un dominio; deve essere l'endpoint standard.
- Se l'`hosts`opzione è un endpoint di raccolta senza server, è necessario impostarla su. `serverless` `true` Inoltre, se il file di definizione YAML contiene l'`index_type`opzione, questa deve essere impostata su, altrimenti la convalida `management_disabled` fallisce.
- Le seguenti opzioni non sono supportate:
  - `username`
  - `password`
  - `cert`
  - `proxy`
  - `dlq_file`- Se desideri scaricare gli eventi non riusciti su una coda di lettere morte (DLQ), devi utilizzare l'`dlq`opzione e specificare un bucket S3.
  - `ism_policy_file`
  - `socket_timeout`
  - `template_file`
  - `insecure`
  - `bulk_size`

Fonte delle metriche OTel, sorgente di traccia OTel e origine dei registri OTel

I plugin Otel metrics source, OTel trace source e OTel logs source hanno i seguenti requisiti e limitazioni:

- L'*path*opzione è obbligatoria. Il percorso è una stringa come`/log/ingest`, che rappresenta il percorso URI per l'inserimento dei log. Questo percorso definisce l'URI utilizzato per inviare dati alla pipeline. Ad esempio, `https://log-pipeline.us-west-2.osis.amazonaws.com/log/ingest`. Il percorso deve iniziare con una barra (/) e può contenere i caratteri speciali '-', '_', ' . 'e'/', oltre al `${pipelineName}` segnaposto.
- Le seguenti opzioni sono impostate da OpenSearch Ingestion e non sono supportate nelle configurazioni della pipeline:
  - `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`

Processore del gruppo di traccia Otel

Il processore del gruppo di traccia Otel presenta i seguenti requisiti e limitazioni:

- L'`aws`opzione è obbligatoria e deve contenere le seguenti opzioni:
  - `sts_role_arn`
  - `region`
  - `hosts`
- L'`sts_role_arn`opzione specifica lo stesso ruolo del ruolo della pipeline specificato nella configurazione del OpenSearch sink.
- Le `insecure` opzioni `username`,`password`,`cert`, e non sono supportate.
- L'`aws_sigv4`opzione è obbligatoria e deve essere impostata su true.
- L'`serverless`opzione all'interno del plugin OpenSearch sink non è supportata. Il processore Otel trace group attualmente non funziona con le raccolte OpenSearch Serverless.
- Il numero di `otel_trace_group` processori all'interno del corpo di configurazione della pipeline non può superare 8.

Processore di traccia Otel

Il processore di traccia Otel presenta i seguenti requisiti e limitazioni:

- Il valore dell'`trace_flush_interval`opzione non può superare i 300 secondi.

Processore Service-map

Il processore Service-map presenta i seguenti requisiti e limitazioni:

- Il valore dell'`window_duration`opzione non può superare i 300 secondi.

Fonte S3

Il plugin sorgente S3 presenta i seguenti requisiti e limitazioni:

- L'`aws`opzione è obbligatoria e deve contenere `region` `sts_role_arn` opzioni.
- Il valore dell'`records_to_accumulate`opzione non può superare 200.
- Il valore dell'`maximum_messages`opzione non può superare 10.
- Se specificata, l'`disable_bucket_ownership_validation`opzione deve essere impostata su false.

- Se specificata, l'`input_serialization`opzione deve essere impostata su`parquet`.

Utilizzo delle integrazioni della OpenSearch pipeline di Amazon Ingestion

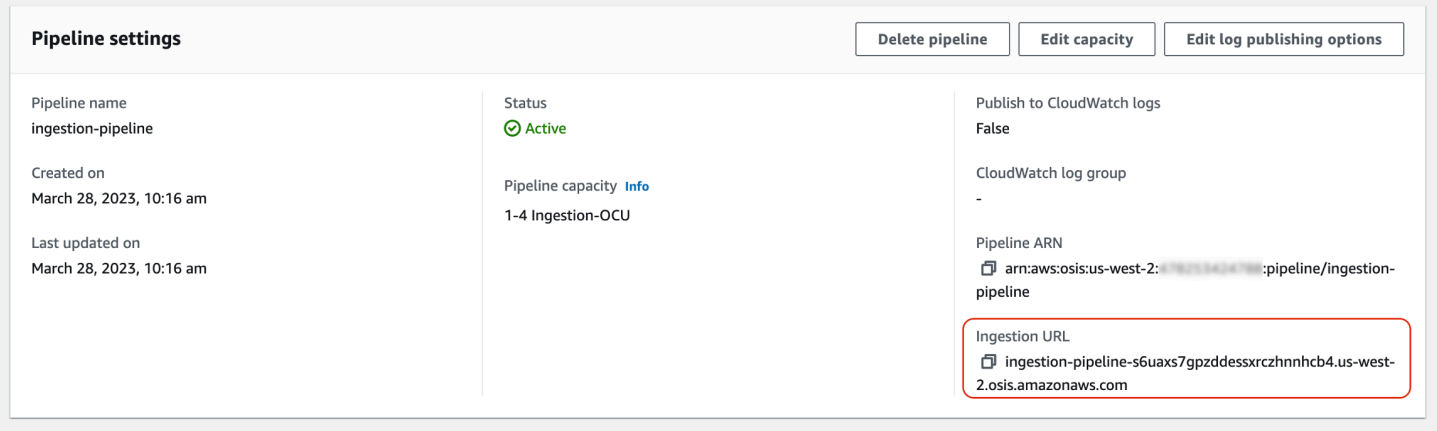
Per inserire correttamente i dati in una pipeline di Amazon OpenSearch Ingestion, devi configurare l'applicazione client (la fonte) per inviare dati all'endpoint della pipeline. La tua fonte potrebbe essere client come Fluent Bit logs, Collector o un semplice bucket S3. OpenTelemetry La configurazione esatta è diversa per ogni client.

Le differenze importanti durante la configurazione dell'origine (rispetto all'invio di dati direttamente a un dominio di OpenSearch servizio o a una raccolta OpenSearch Serverless) sono il nome del AWS servizio (`osis`) e l'endpoint host, che deve essere l'endpoint della pipeline.

Argomenti

Costruzione dell'endpoint di ingestione

Per importare i dati in una pipeline, inviateli all'endpoint di ingestione. Per individuare l'URL di importazione, accedete alla pagina delle impostazioni della pipeline e copiate l'URL di ingestione:



Per creare l'endpoint di ingestione completo per sorgenti basate su pull come Otel trace e Otel Metrics, aggiungete il percorso di ingestione dalla configurazione della pipeline all'URL di ingestione.

Ad esempio, supponiamo che la configurazione della pipeline abbia il seguente percorso di ingestione:

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

L'endpoint di ingestione completo, specificato nella configurazione del client, assumerà il seguente formato:. `https://ingestion-pipeline-abcdefg.us-west-2.osis.amazonaws.com/my/test_path`

Per ulteriori informazioni, consulta the section called “Specificare il percorso di ingestione”.

Creazione di un ruolo di importazione

Tutte le richieste di OpenSearch Ingestion devono essere firmate con Signature Version 4. Al ruolo che firma la richiesta deve essere almeno concessa l'autorizzazione per l'`osis:Ingest`azione, che gli consente di inviare dati a una pipeline di OpenSearch Ingestion.

Ad esempio, la seguente policy AWS Identity and Access Management (IAM) consente al ruolo corrispondente di inviare dati a una singola pipeline:

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

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

> **Note**
>
> Per utilizzare il ruolo per tutte le pipeline, sostituite l'ARN `Resource` nell'elemento con un carattere jolly (*).

Fornire l'accesso all'importazione su più account

> **Note**
>
> Puoi fornire l'accesso all'ingestione tra account solo per le pipeline pubbliche, non per le pipeline VPC.

Potrebbe essere necessario importare dati in una pipeline da un altro Account AWS, ad esempio un account che ospita l'applicazione di origine. Se il principale che sta scrivendo su una pipeline si trova in un account diverso rispetto alla pipeline stessa, devi configurarlo in modo che si fidi di un altro ruolo IAM per l'inserimento dei dati nella pipeline.

Per configurare le autorizzazioni di importazione tra più account

1. Crea il ruolo di ingestione con `osis:Ingest` autorizzazione (descritto nella sezione precedente) all'interno della stessa pipeline. Account AWS Per istruzioni, consulta Creazione di ruoli IAM.
2. Allega una politica di fiducia al ruolo di inserimento che consenta a un responsabile di un altro account di assumerlo:

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

```
        "AWS": "arn:aws:iam::{external-account-id}:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

3. Nell'altro account, configura l'applicazione client (ad esempio, Fluent Bit) per assumere il ruolo di importazione. Affinché ciò funzioni, l'account dell'applicazione deve concedere le autorizzazioni all'utente o al ruolo dell'applicazione per assumere il ruolo di ingestione.

   L'esempio seguente di politica basata sull'identità consente al principale allegato di assumere dall'account della pipeline: `ingestion-role`

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

L'applicazione client può quindi utilizzare l'AssumeRoleoperazione per assumere `ingestion-role` e importare dati nella pipeline associata.

Utilizzo di una pipeline OpenSearch di ingestione con Amazon DynamoDB

Puoi utilizzare una pipeline di OpenSearch ingestion con DynamoDB per trasmettere gli eventi delle tabelle DynamoDB (come creazione, aggiornamento ed eliminazione) ai domini e alle raccolte di Amazon Service. OpenSearch La pipeline OpenSearch Ingestion incorpora l'infrastruttura Change Data Capture (CDC) per fornire un modo su larga scala e a bassa latenza per lo streaming continuo di dati da una tabella DynamoDB.

Esistono due modi per utilizzare DynamoDB come origine per elaborare i dati: con e senza un'istantanea iniziale completa.

Un'istantanea iniziale completa è un backup di una tabella che DynamoDB esegue con la funzionalità di ripristino (point-in-time PITR). DynamoDB carica questa istantanea su Amazon S3. Da lì, una

pipeline di OpenSearch Ingestion lo invia a un indice in un dominio o lo partiziona in più indici di un dominio. Per mantenere i dati in DynamoDB OpenSearch e coerenti, la pipeline sincronizza tutti gli eventi di creazione, aggiornamento ed eliminazione nella tabella DynamoDB con i documenti salvati nell'indice o negli indici. OpenSearch

Quando si utilizza uno snapshot iniziale completo, la pipeline di OpenSearch Ingestion prima lo inserisce e poi inizia a leggere i dati da DynamoDB Streams. Alla fine recupera e mantiene la coerenza dei dati quasi in tempo reale tra DynamoDB e. OpenSearch Quando scegli questa opzione, devi abilitare sia PITR che uno stream DynamoDB sulla tua tabella.

Puoi anche utilizzare l'integrazione di OpenSearch Ingestion con DynamoDB per lo streaming di eventi senza un'istantanea. Scegli questa opzione se disponi già di un'istantanea completa di un altro meccanismo o se desideri semplicemente trasmettere gli eventi correnti da una tabella DynamoDB con DynamoDB Streams. Quando scegli questa opzione, devi solo abilitare un flusso DynamoDB sulla tua tabella.

Per ulteriori informazioni su questa integrazione, consulta l'integrazione zero-ETL di DynamoDB con OpenSearch Amazon Service nella Developer Guide.Amazon DynamoDB

Argomenti

Prerequisiti

Per configurare la pipeline, è necessario disporre di una tabella DynamoDB con DynamoDB Streams abilitato. Il tuo stream deve utilizzare il tipo di visualizzazione dello stream. `NEW_IMAGE` Tuttavia, le pipeline di OpenSearch Ingestion possono anche trasmettere eventi `NEW_AND_OLD_IMAGES` se questo tipo di visualizzazione dello stream si adatta al tuo caso d'uso.

Se utilizzi le istantanee, devi anche abilitare il point-in-time ripristino sulla tua tabella. Per ulteriori informazioni, consulta Creating a table, Enabling point-in-time recovery e Enabling a stream nella Amazon DynamoDB Developer Guide.

Fase 1: Configurare il ruolo della pipeline

Dopo aver impostato la tabella DynamoDB, imposta il ruolo pipeline che desideri utilizzare nella configurazione della pipeline e aggiungi le seguenti autorizzazioni DynamoDB nel ruolo:

```
{
    "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/{exportPath}/*"
            ]
        }
    ]
}
```

Puoi anche utilizzare una chiave gestita dal AWS KMS cliente per crittografare i file di dati di esportazione. Per decrittografare gli oggetti esportati, specificate `s3_sse_kms_key_id` l'ID della chiave nella configurazione di esportazione della pipeline con il seguente formato:. `arn:aws:kms:us-west-2:{account-id}:key/my-key-id` La seguente politica include le autorizzazioni richieste per l'utilizzo di una chiave gestita dal cliente:

```
{
    "Sid": "allowUseOfCustomManagedKey",
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": arn:aws:kms:us-west-2:{account-id}:key/my-key-id
}
```

Fase 2: Creare la pipeline

È quindi possibile configurare una pipeline OpenSearch di ingestione come la seguente, che specifica DynamoDB come origine. Questa pipeline di esempio inserisce i dati `table-a` con lo snapshot PITR, seguiti dagli eventi di DynamoDB Streams. Una posizione iniziale di `LATEST` indica che la pipeline deve leggere i dati più recenti da 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: "${getMetadata(\"table_name\")}"
      index_type: custom
      normalize_index: true
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
```

È possibile utilizzare un blueprint DynamoDB preconfigurato per creare questa pipeline. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

Coerenza dei dati

OpenSearch Ingestion supporta il riconoscimento per garantire la durabilità dei dati. end-to-end Quando una pipeline legge istantanee o flussi, crea dinamicamente partizioni per l'elaborazione parallela. La pipeline contrassegna una partizione come completa quando riceve un riconoscimento dopo aver acquisito tutti i record nel dominio o nella raccolta. OpenSearch

Se desideri importare in una raccolta di ricerca OpenSearch Serverless, puoi generare un ID di documento nella pipeline. Se desideri importare in una raccolta di serie temporali OpenSearch Serverless, tieni presente che la pipeline non genera un ID di documento.

Una pipeline OpenSearch di Ingestion mappa anche le azioni degli eventi in entrata nelle corrispondenti azioni di indicizzazione di massa per facilitare l'acquisizione dei documenti. Ciò mantiene i dati coerenti, in modo che ogni modifica dei dati in DynamoDB venga riconciliata con le corrispondenti modifiche del documento. OpenSearch

Mappatura dei tipi di dati

OpenSearch Il servizio mappa dinamicamente i tipi di dati in ogni documento in entrata al tipo di dati corrispondente in DynamoDB. La tabella seguente mostra come OpenSearch Service mappa automaticamente vari tipi di dati.

Tipo di dati	OpenSearch	DynamoDB
Numero	OpenSearch mappa automaticamente i dati numerici. Se il numero è un numero intero, lo OpenSearch mappa come valore lungo. Se il numero è frazionario, lo OpenSearch mappa come valore float. OpenSearch mappa dinamicamente vari attributi in base al primo documento inviato. Se si dispone di una combinazi one di tipi di dati per lo stesso attributo in DynamoDB, ad esempio un numero intero e un numero frazionario, la mappatura potrebbe non riuscire. Ad esempio, se il primo documento ha un attributo che è un numero intero e un documento successivo ha lo stesso attributo come numero frazionario, OpenSearch non riesce a importare il secondo documento. In questi casi, è necessario fornire un modello di mappatura esplicito, come il seguente: `{ "template": { "mappings": { "properties": { "MixedNumberAttribute": { "type": "float" }`	DynamoDB supporta i numeri.

Tipo di dati	OpenSearch	DynamoDB

	<pre>}
	}
	}
	}</pre>
	Se hai bisogno di una doppia precision e, usa la mappatura dei campi di tipo stringa. Non esiste un tipo numerico equivalente che supporti 38 cifre di precisione in. OpenSearch	

Set di numeri	OpenSearch mappa automaticamente un set di numeri in una matrice di valori lunghi o valori float. Come per i numeri scalari, ciò dipende dal fatto che il primo numero ingerito sia un numero intero o un numero frazionario. È possibile fornire mappature per i set di numeri nello stesso modo in cui si mappano le stringhe scalari.	DynamoDB supporta tipi che rappresentano insiemi di numeri.

Tipo di dati	OpenSearch	DynamoDB
Stringa	OpenSearch mappa automaticamente i valori delle stringhe come testo. In alcune situazioni, come i valori enumerati, è possibile eseguire il mapping al tipo di parola chiave. L'esempio seguente mostra come mappare un attributo DynamoDB `PartType` denominato a una parola chiave. OpenSearch `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	DynamoDB supporta le stringhe.
Set di stringhe	OpenSearch mappa automaticamente un set di stringhe in un array di stringhe. È possibile fornire mappature per i set di stringhe nello stesso modo in cui si mappano le stringhe scalari.	DynamoDB supporta tipi che rappresentano set di stringhe.

Tipo di dati	OpenSearch	DynamoDB
Binario	OpenSearch mappa automaticamente i dati binari come testo. È possibile fornire una mappatura in cui scriverli come campi binari. OpenSearch L'esempio seguente mostra come mappare un attributo DynamoDB `ImageData` denominato su un campo binario. OpenSearch `{ "template": { "mappings": { "properties": { "ImageData": { "type": "binary" } } } } }`	DynamoDB supporta gli attributi di tipo binario.
Set binario	OpenSearch mappa automaticamente un set binario in una matrice di dati binari come testo. È possibile fornire mappature per i set di numeri nello stesso modo in cui si esegue la mappatura di un sistema binario scalare.	DynamoDB supporta tipi che rappresentano insiemi di valori binari.
Booleano	OpenSearch mappa un tipo booleano DynamoDB in un tipo booleano. OpenSearch	DynamoDB supporta gli attributi di tipo booleano.

Tipo di dati	OpenSearch	DynamoDB
Null	OpenSearch può importare documenti con il tipo null DynamoDB. Salva il valore come valore nullo nel documento. Non esiste alcuna mappatura per questo tipo e questo campo non è indicizzato o ricercabile. Se lo stesso nome di attributo viene utilizzato per un tipo nullo e successiv amente passa a un tipo diverso, ad esempio string, OpenSearch crea una mappatura dinamica per il primo valore non nullo. I valori successivi possono ancora essere valori nulli di DynamoDB.	DynamoDB supporta attributi di tipo null.

Tipo di dati	OpenSearch	DynamoDB
Eseguire la mappatura	OpenSearch mappa gli attributi della mappa di DynamoDB ai campi annidati. Le stesse mappature si applicano all'interno di un campo nidificato. L'esempio seguente mappa una stringa in un campo nidificato a un tipo di parola chiave in: OpenSearch `{ "template": { "mappings": { "properties": { "AdditionalDescriptions": { "properties": { "PartType": { "type": "keyword" } } } } } } }`	DynamoDB supporta gli attributi dei tipi di mappa.

Tipo di dati	OpenSearch	DynamoDB
Elenco	OpenSearch fornisce risultati diversi per gli elenchi DynamoDB, a seconda del contenuto dell'elenco. Quando un elenco contiene tutti i tipi scalari dello stesso tipo (ad esempio, un elenco di tutte le stringhe), OpenSearch inserisce l'elenco come un array di quel tipo. Funziona per i tipi stringa, numerica, booleana e null. Le restrizioni per ciascuno di questi tipi sono le stesse delle restrizioni per uno scalare di quel tipo. È inoltre possibile fornire mappature per elenchi di mappe utilizzando la stessa mappatura utilizzata per una mappa. Non puoi fornire un elenco di tipi misti.	DynamoDB supporta gli attributi del tipo di elenco.

Tipo di dati	OpenSearch	DynamoDB
Imposta	OpenSearch fornisce risultati diversi per i set DynamoDB a seconda del contenuto del set. Quando un set contiene tutti i tipi scalari dello stesso tipo (ad esempio, un insieme di tutte le stringhe), OpenSearch inserisce il set come un array di quel tipo. Funziona per i tipi stringa, numerica, booleana e null. Le restrizioni per ciascuno di questi tipi sono le stesse delle restrizioni per uno scalare di quel tipo. È inoltre possibile fornire mappature per set di mappe utilizzando la stessa mappatura utilizzata per una mappa. Non puoi fornire un set di tipi misti.	DynamoDB supporta tipi che rappresentano set.

Ti consigliamo di configurare la dead-letter queue (DLQ) nella pipeline di Ingestion. OpenSearch Se hai configurato la coda, OpenSearch Service invia tutti i documenti non riusciti che non possono essere importati a causa di errori di mappatura dinamica sulla coda.

Nel caso in cui le mappature automatiche falliscano, puoi utilizzare `template_type` e `template_content` nella configurazione della pipeline per definire regole di mappatura esplicite. In alternativa, puoi creare modelli di mappatura direttamente nel tuo dominio di ricerca o nella tua raccolta prima di avviare la pipeline.

Limitazioni

Considerate le seguenti limitazioni quando impostate una pipeline di OpenSearch ingestione per DynamoDB:

- L'integrazione OpenSearch di Ingestion con DynamoDB attualmente non supporta l'ingestione tra regioni. La tabella DynamoDB OpenSearch e la pipeline di ingestione devono trovarsi nella stessa posizione. Regione AWS
- La tabella DynamoDB OpenSearch e la pipeline di ingestione devono trovarsi nella stessa posizione. Account AWS
- Una pipeline OpenSearch di ingestione supporta solo una tabella DynamoDB come origine.
- DynamoDB Streams archivia i dati in un registro solo per un massimo di 24 ore. Se l'inserimento da un'istantanea iniziale di una tabella di grandi dimensioni richiede 24 ore o più, si verificherà una perdita iniziale di dati. Per mitigare questa perdita di dati, stimate la dimensione della tabella e configurate le unità di calcolo appropriate delle pipeline di Ingestion. OpenSearch

Utilizzo di una pipeline OpenSearch di ingestione con Amazon DocumentDB

Puoi utilizzare una pipeline OpenSearch di importazione con Amazon DocumentDB per trasmettere le modifiche ai documenti (ad esempio creazione, aggiornamento ed eliminazione) a domini e raccolte di Amazon OpenSearch Service. La pipeline OpenSearch Ingestion può sfruttare i meccanismi di change data capture (CDC), se disponibili sul tuo cluster Amazon DocumentDB, o il polling delle API per fornire un modo su larga scala e a bassa latenza per lo streaming continuo di dati da un cluster Amazon DocumentDB.

Esistono due modi per utilizzare Amazon DocumentDB come origine per elaborare i dati: con e senza uno snapshot iniziale completo.

Uno snapshot iniziale completo è una query collettiva di un'intera raccolta Amazon DocumentDB. Amazon DocumentDB carica questa istantanea su Amazon S3. Da lì, una pipeline di OpenSearch Ingestion lo invia a un indice in un dominio o lo partiziona in più indici in un dominio. Per mantenere OpenSearch coerenti i dati in Amazon DocumentDB, la pipeline sincronizza tutti gli eventi di creazione, aggiornamento ed eliminazione nella raccolta Amazon DocumentDB con i documenti salvati nell'indice o negli indici. OpenSearch

Quando si utilizza uno snapshot iniziale completo, la pipeline di OpenSearch Ingestion prima lo inserisce e poi inizia a leggere i dati dai flussi di modifiche di Amazon DocumentDB. Alla fine recupera e mantiene la coerenza dei dati quasi in tempo reale tra Amazon OpenSearch DocumentDB e.

Puoi anche utilizzare l'integrazione di OpenSearch Ingestion con Amazon DocumentDB per lo streaming di eventi senza uno snapshot. Scegli questa opzione se disponi già di uno snapshot completo di un altro meccanismo o se desideri semplicemente trasmettere in streaming gli eventi correnti da una raccolta Amazon DocumentDB con flussi di modifiche.

Con entrambe queste opzioni, devi abilitare un flusso di modifiche sulla tua raccolta Amazon DocumentDB se abiliti uno stream nella configurazione in pipeline. Se utilizzi solo il caricamento completo o l'esportazione, non è necessario abilitare un flusso di modifiche.

Prerequisiti

Prima di creare la pipeline OpenSearch di Ingestion, effettuate le seguenti operazioni:

1. Crea un cluster Amazon DocumentDB con l'autorizzazione a leggere i dati seguendo i passaggi descritti in Creare un cluster Amazon DocumentDB nella Amazon DocumentDB Developer Guide. Se utilizzi l'infrastruttura CDC, assicurati di configurare il cluster Amazon DocumentDB per pubblicare flussi di modifiche.
2. Configura l'autenticazione sul tuo cluster Amazon DocumentDB con. AWS Secrets Manager Abilita la rotazione dei segreti seguendo i passaggi descritti in Rotazione automatica delle password per Amazon DocumentDB. Per ulteriori informazioni, consulta Accesso al database con controllo e sicurezza degli accessi basati sui ruoli in Amazon DocumentDB.
3. Se utilizzi un flusso di modifiche per sottoscrivere le modifiche ai dati sulla tua raccolta Amazon DocumentDB, evita la perdita di dati estendendo il periodo di conservazione fino a 7 giorni utilizzando il parametro. `change_stream_log_retention_duration` Gli eventi Change Streams vengono archiviati per impostazione predefinita per 3 ore dopo la registrazione dell'evento, tempo non sufficiente per raccolte di grandi dimensioni. Per modificare il periodo di conservazione del Change Stream, consulta Modifica della durata di conservazione del log del Change Stream.
4. Crea un dominio OpenSearch di servizio o una raccolta OpenSearch Serverless. Per ulteriori informazioni, consulta Creazione di domini OpenSearch di servizio e Creazione di raccolte.
5. Allega una politica basata sulle risorse al tuo dominio o una politica di accesso ai dati alla tua raccolta. Queste politiche di accesso consentono a OpenSearch Ingestion di scrivere dati dal tuo cluster Amazon DocumentDB al tuo dominio o alla tua raccolta.

   Il seguente esempio di policy di accesso al dominio consente al ruolo pipeline, creato nel passaggio successivo, di scrivere dati su un dominio. Assicurati di aggiornarlo `resource` con il tuo ARN.

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

Per creare un ruolo IAM con le autorizzazioni corrette per accedere ai dati di scrittura nella raccolta o nel dominio, consulta Autorizzazioni richieste per i domini e Autorizzazioni richieste per le raccolte.

Fase 1: Configurare il ruolo della pipeline

Dopo aver impostato i prerequisiti della pipeline di Amazon DocumentDB, configura il ruolo pipeline che desideri utilizzare nella configurazione della pipeline e aggiungi le seguenti autorizzazioni Amazon DocumentDB nel ruolo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowS3ListObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::{s3_bucket}"
```

```
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": "{s3_prefix}/*"
                }
            }
        },
        {
            "Sid": "allowReadAndWriteToS3ForExportStream",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::{s3_bucket}/{s3_prefix}/*"
            ]
        },
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:{region}:{account-id}:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

Devi fornire le autorizzazioni Amazon EC2 di cui sopra sul ruolo IAM che usi per creare la pipeline di OpenSearch ingestione, poiché la pipeline utilizza queste autorizzazioni per creare ed eliminare un'interfaccia di rete nel tuo VPC. La pipeline può accedere al cluster Amazon DocumentDB solo tramite questa interfaccia di rete.

Fase 2: Creare la pipeline

È quindi possibile configurare una pipeline OpenSearch di ingestion come la seguente, che specifica Amazon DocumentDB come origine. Tieni presente che per compilare il nome dell'indice, la `getMetadata` funzione utilizza come chiave di metadati. *`documentdb_collection`* Se si desidera utilizzare un nome di indice diverso senza il `getMetadata` metodo, è possibile utilizzare la configurazione. `index: "`*`my_index_name`*`"`

```
version: "2"
documentdb-pipeline:
  source:
    documentdb:
      acknowledgments: true
      host: "https://docdb-cluster-id.us-east-1.docdb.amazonaws.com"
      port: 27017
      authentication:
        username: ${aws_secrets:secret:username}
        password: ${aws_secrets:secret:password}
      aws:
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      s3_bucket: "bucket-name"
      s3_region: "bucket-region"
      s3_prefix: "path" #optional path for storing the temporary data
      collections:
        - collection: "dbname.collection"
          export: true
          stream: true
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      index: "${getMetadata(\"documentdb_collection\")}"
      index_type: custom
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
extension:
  aws:
    secrets:
      secret:
        secret_id: "my-docdb-secret"
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        refresh_interval: PT1H
```

Puoi utilizzare un blueprint Amazon DocumentDB preconfigurato per creare questa pipeline. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

Se utilizzi il AWS Management Console per creare la tua pipeline, devi anche collegare la pipeline al tuo VPC per utilizzare Amazon DocumentDB come sorgente. Per farlo, trova la sezione

Configurazione di rete, seleziona la casella di controllo Collega a VPC e scegli il tuo CIDR da una delle opzioni predefinite fornite oppure selezionane una personalizzata.

Per fornire un CIDR personalizzato, seleziona Altro dal menu a discesa. Per evitare una collisione negli indirizzi IP tra OpenSearch Ingestion e Amazon DocumentDB, assicurati che il CIDR VPC di Amazon DocumentDB sia diverso dal CIDR per Ingestion. OpenSearch

Per ulteriori informazioni, consulta Configurazione dell'accesso VPC per una pipeline.

Coerenza dei dati

La pipeline garantisce la coerenza dei dati effettuando continuamente polling o ricevendo modifiche dal cluster Amazon DocumentDB e aggiornando i documenti corrispondenti nell'indice. OpenSearch

OpenSearch Ingestion supporta il end-to-end riconoscimento per garantire la durabilità dei dati. Quando una pipeline legge istantanee o flussi, crea dinamicamente partizioni per l'elaborazione parallela. La pipeline contrassegna una partizione come completa quando riceve un riconoscimento dopo aver acquisito tutti i record nel dominio o nella raccolta. OpenSearch

Se desideri importare in una raccolta di ricerca OpenSearch Serverless, puoi generare un ID di documento nella pipeline. Se desideri importare in una raccolta di serie temporali OpenSearch Serverless, tieni presente che la pipeline non genera un ID di documento, quindi devi `document_id: "${getMetadata(\"primary_key\")}"` ometterlo nella configurazione del pipeline sink.

Una pipeline OpenSearch di Ingestion mappa anche le azioni degli eventi in entrata nelle corrispondenti azioni di indicizzazione di massa per facilitare l'acquisizione dei documenti. Ciò mantiene i dati coerenti, in modo che ogni modifica dei dati in Amazon DocumentDB venga riconciliata con le corrispondenti modifiche al documento. OpenSearch

Mappatura dei tipi di dati

OpenSearch Il servizio mappa dinamicamente i tipi di dati in ogni documento in entrata al tipo di dati corrispondente in Amazon DocumentDB. La tabella seguente mostra come OpenSearch Service mappa automaticamente vari tipi di dati.

Tipo di dati	OpenSearch	Amazon DocumentDB
Numero intero	OpenSearch mappa automaticamente i valori interi di Amazon DocumentDB su numeri interi. OpenSearch OpenSearch mappa dinamicamente il campo in base al primo documento inviato. Se disponi di una combinazione di tipi di dati per lo stesso attributo in Amazon DocumentDB, la mappatura automatica potrebbe non riuscire. Ad esempio, se il primo documento ha un attributo lungo e un documento successivo ha lo stesso attributo come numero intero, OpenSearch non riesce a importare il secondo documento. In questi casi, è necessario fornire un modello di mappatura esplicito che scelga il tipo di numero più flessibile, come il seguente: `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	Amazon DocumentDB supporta numeri interi.

Tipo di dati	OpenSearch	Amazon DocumentDB
Long	OpenSearch mappa automaticamente i valori long di Amazon DocumentDB su OpenSearch long. OpenSearch mappa dinamicamente il campo in base al primo documento inviato. Se disponi di una combinazione di tipi di dati per lo stesso attributo in Amazon DocumentDB, la mappatura automatica potrebbe non riuscire. Ad esempio, se il primo documento ha un attributo lungo e un documento successivo ha lo stesso attributo come numero intero, OpenSearch non riesce a importare il secondo documento. In questi casi, è necessario fornire un modello di mappatura esplicito che scelga il tipo di numero più flessibile, come il seguente: `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	Amazon DocumentDB supporta i file long.

Tipo di dati	OpenSearch	Amazon DocumentDB
Stringa	OpenSearch mappa automaticamente i valori delle stringhe come testo. In alcune situazioni, come i valori enumerati, è possibile eseguire il mapping al tipo di parola chiave. L'esempio seguente mostra come mappare un attributo Amazon DocumentDB denominato `PartType` a una OpenSearch parola chiave. `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	Amazon DocumentDB supporta le stringhe.

Tipo di dati	OpenSearch	Amazon DocumentDB
Doppio	OpenSearch mappa automaticamente i valori doppi di Amazon DocumentDB a OpenSearch valori doppi. OpenSearch mappa dinamicamente il campo in base al primo documento inviato. Se disponi di una combinazione di tipi di dati per lo stesso attributo in Amazon DocumentDB, la mappatura automatica potrebbe non riuscire. Ad esempio, se il primo documento ha un attributo lungo e un documento successivo ha lo stesso attributo come numero intero, OpenSearch non riesce a importare il secondo documento. In questi casi, è necessario fornire un modello di mappatura esplicito che scelga il tipo di numero più flessibile, come il seguente: `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	Amazon DocumentDB supporta il doppio.

Tipo di dati	OpenSearch	Amazon DocumentDB
Data	Per impostazione predefinita, la data viene mappata a un numero intero in. OpenSearch È possibile definire un modello di mappatura personalizzato per mappare una data a una OpenSearch data. `{ "template": { "mappings": { "properties": { "myDateField": { "type": "date", "format": "epoch_second" } } } } }`	Amazon DocumentDB supporta le date.

Tipo di dati	OpenSearch	Amazon DocumentDB
Timestamp	Per impostazione predefinita, il timestamp corrisponde a un numero intero in. OpenSearch È possibile definire un modello di mappatura personalizzato per associare una data a una data. OpenSearch `{ "template": { "mappings": { "properties": { "myTimestampField": { "type": "date", "format": "epoch_second" } } } } }`	Amazon DocumentDB supporta i timestamp.
Booleano	OpenSearch mappa un tipo booleano Amazon DocumentDB in un tipo booleano. OpenSearch	Amazon DocumentDB supporta gli attributi di tipo booleano.

Tipo di dati	OpenSearch	Amazon DocumentDB
Decimale	OpenSearch mappa gli attributi delle mappe di Amazon DocumentDB ai campi annidati. Le stesse mappature si applicano all'interno di un campo nidificato. L'esempio seguente mappa una stringa in un campo nidificato a un tipo di parola chiave in: OpenSearch `{ "template": { "mappings": { "properties": { "myDecimalField": { "type": "double" } } } } }` Con questa mappatura personalizzata, puoi interrogare e aggregare il campo con una precisione a doppio livello. Il valore originale mantiene la massima precisione nella `_source` proprietà del documento. OpenSearch Senza questa mappatura, OpenSearch utilizza il testo per impostazione predefinita.	Amazon DocumentDB supporta i decimali.
Espressione regolare	Il tipo regex crea campi annidati. Questi includono *<myFieldName>* `.pattern` e. *<myFieldName>* `.options`	Amazon DocumentDB supporta le espressioni regolari.

Tipo di dati	OpenSearch	Amazon DocumentDB
Dati binari	OpenSearch mappa automaticamente i dati binari di Amazon DocumentDB su OpenSearch testo. Puoi fornire una mappatura in cui scriverli come campi binari. OpenSearch L'esempio seguente mostra come mappare un campo Amazon DocumentDB denominato `imageData` a un campo OpenSearch binario. `{ "template": { "mappings": { "properties": { "imageData": { "type": "binary" } } } } }`	Amazon DocumentDB supporta campi di dati binari.
ObjectId	I campi con un tipo di ObjectID vengono mappati ai campi di OpenSearch testo. Il valore sarà la rappresentazione in formato stringa di ObjectID.	Amazon DocumentDB supporta gli ObjectID.

Tipo di dati	OpenSearch	Amazon DocumentDB
Null	OpenSearch può importare documenti con il tipo null di Amazon DocumentDB. Salva il valore come valore nullo nel documento. Non esiste alcuna mappatura per questo tipo e questo campo non è indicizzato o ricercabile. Se lo stesso nome di attributo viene utilizzato per un tipo nullo e successivamente passa a un tipo diverso, ad esempio string, OpenSearch crea una mappatura dinamica per il primo valore non nullo. I valori successivi possono comunque essere valori null di Amazon DocumentDB.	Amazon DocumentDB supporta campi di tipo null.
Undefined	OpenSearch può importare documenti con il tipo non definito di Amazon DocumentDB. Salva il valore come valore nullo nel documento. Non esiste alcuna mappatura per questo tipo e questo campo non è indicizzato o ricercabile. Se lo stesso nome di campo viene utilizzato per un tipo non definito e successivamente passa a un tipo diverso, ad esempio string, OpenSearch crea una mappatura dinamica per il primo valore non definito. I valori successivi possono ancora essere valori non definiti di Amazon DocumentDB.	Amazon DocumentDB supporta campi di tipo non definito.

Tipo di dati	OpenSearch	Amazon DocumentDB
MinKey	OpenSearch può importare documenti con il tipo Amazon DocumentDB MinKey. Salva il valore come valore nullo nel documento. Non esiste alcuna mappatura per questo tipo e questo campo non è indicizzato o ricercabile. Se lo stesso nome di campo viene utilizzato per un tipo MinKey e successivamente passa a un tipo diverso, ad esempio string, OpenSearch crea una mappatura dinamica per il primo valore non MinKey. I valori successivi possono ancora essere valori MinKey di Amazon DocumentDB.	Amazon DocumentDB supporta i campi di tipo MinKey.
MaxKey	OpenSearch può importare documenti con il tipo Amazon DocumentDB MaxKey. Salva il valore come valore nullo nel documento. Non esiste alcuna mappatura per questo tipo e questo campo non è indicizzato o ricercabile. Se lo stesso nome di campo viene utilizzato per un tipo di MaxKey e successivamente passa a un tipo diverso, ad esempio string, OpenSearch crea una mappatura dinamica per il primo valore non MaxKey. I valori successivi possono ancora essere valori MaxKey di Amazon DocumentDB.	Amazon DocumentDB supporta i campi di tipo MaxKey.

Ti consigliamo di configurare la dead-letter queue (DLQ) nella pipeline di Ingestion. OpenSearch Se hai configurato la coda, OpenSearch Service invia tutti i documenti non riusciti che non possono essere importati a causa di errori di mappatura dinamica sulla coda.

Nel caso in cui le mappature automatiche falliscano, puoi utilizzare `template_type` e `template_content` nella configurazione della pipeline per definire regole di mappatura esplicite. In alternativa, puoi creare modelli di mappatura direttamente nel tuo dominio di ricerca o nella tua raccolta prima di avviare la pipeline.

Limitazioni

Considera le seguenti limitazioni quando configuri una pipeline di OpenSearch ingestione per Amazon DocumentDB:

- L'integrazione OpenSearch di Ingestion con Amazon DocumentDB attualmente non supporta l'ingestione tra regioni. Il cluster Amazon DocumentDB e la pipeline OpenSearch di Ingestion devono trovarsi nello stesso ambiente. Regione AWS
- L'integrazione OpenSearch di Ingestion con Amazon DocumentDB attualmente non supporta l'ingestione tra account. Il cluster Amazon DocumentDB e la pipeline OpenSearch di Ingestion devono trovarsi nello stesso ambiente. Account AWS
- Una pipeline OpenSearch di ingestion supporta solo un cluster Amazon DocumentDB come origine.
- L'integrazione OpenSearch di Ingestion con Amazon DocumentDB supporta specificamente i cluster basati su istanze di Amazon DocumentDB. Non supporta i cluster elastici di Amazon DocumentDB.
- L'integrazione OpenSearch di Ingestion supporta solo AWS Secrets Manager come meccanismo di autenticazione per il tuo cluster Amazon DocumentDB.
- Non puoi aggiornare la configurazione della pipeline esistente per importare dati da un database o una raccolta diversi. È invece necessario creare una nuova pipeline.

Utilizzo di una pipeline OpenSearch di ingestione con il cloud Confluent Kafka

Puoi utilizzare Confluent Kafka come fonte in OpenSearch Ingestion per lo streaming di dati da un cluster Confluent Kafka a un dominio Amazon Service o a una raccolta Amazon Serverless.

OpenSearch OpenSearch OpenSearch Ingestion supporta l'elaborazione di dati in streaming da Kafka autogestito in spazi di rete pubblici e privati.

Connettività al Kafka Cloud pubblico Confluent

Puoi utilizzare le pipeline di OpenSearch Ingestion per lo streaming di dati da un cluster Confluent Kafka con configurazione pubblica (il nome DNS del server bootstrap deve essere risolto pubblicamente). A tale scopo, avrai bisogno di una pipeline di OpenSearch ingestione, un cluster Kafka confluente come origine e un OpenSearch dominio Amazon Service o una raccolta Amazon Serverless come destinazione. OpenSearch

Per migrare i dati, devi disporre di quanto segue:

- Un cluster Confluent Kafka che funge da fonte. Il cluster deve contenere i dati che desideri migrare.
- Un dominio Amazon OpenSearch Service o una raccolta Amazon OpenSearch Serverless che funge da destinazione.
- Il cluster Kafka dovrebbe avere l'autenticazione abilitata con le credenziali di. AWS Secrets Manager

Requisiti

Per abilitare l'autenticazione AWS Secrets Manager basata sul tuo cluster di origine autogestito OpenSearch o Elasticsearch, devi

- Configura l'autenticazione sul tuo cluster Confluent Kafka seguendo i passaggi in AWS Secrets Manager Rotate secrets. AWS Secrets Manager
- Crea un ruolo di pipeline in IAM con le autorizzazioni per scrivere su un dominio Amazon OpenSearch Service o su una raccolta Amazon OpenSearch Serverless. È inoltre necessario specificare l'autorizzazione da cui leggere le credenziali. AWS Secrets Manager Per farlo:
  - Allega una politica basata sulle risorse al tuo dominio Amazon OpenSearch Service o una politica di accesso ai dati alla tua raccolta. Queste politiche di accesso consentono a OpenSearch Ingestion di scrivere dati dal tuo cluster di origine autogestito OpenSearch o Elasticsearch sul tuo OpenSearch dominio Amazon Service o sulla tua raccolta Amazon Serverless. OpenSearch
- Crea una pipeline di OpenSearch Ingestion facendo riferimento al blueprint.

  Dopo aver completato questi passaggi, la pipeline inizierà automaticamente a elaborare i dati dal cluster di origine e a inserirli nel dominio Amazon OpenSearch Service o nella destinazione di

raccolta Amazon OpenSearch Serverless. Puoi utilizzare vari processori nella pipeline OpenSearch Ingestion per eseguire qualsiasi trasformazione sui dati ingeriti.

Ruoli e autorizzazioni IAM

Il seguente esempio di policy di accesso al dominio consente al ruolo pipeline, creato nel passaggio successivo, di scrivere dati su un dominio Amazon OpenSearch Service. Assicurati di aggiornare la risorsa con il tuo ARN.

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

Per gestire l'interfaccia di rete sono necessarie le seguenti autorizzazioni:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
```

```
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [ "ec2:CreateTags" ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals": { "aws:RequestTag/OSISManaged": "true" }
            }
        }
    ]
}
```

Le seguenti sono le autorizzazioni necessarie per leggere i segreti del AWS Secrets Manager servizio:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": ["secretsmanager:GetSecretValue"],
            "Resource": ["arn:aws:secretsmanager:<region>:<account-id>:secret:<secret-
name>"]
```

```
        }
    ]
}
```

Per scrivere su un dominio Amazon OpenSearch Service sono necessarie le seguenti autorizzazioni:

```
{
  "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}/*"
    }
  ]
}
```

Creare una pipeline

Dopo aver associato la policy al ruolo della pipeline, utilizza il blueprint della pipeline di migrazione dei dati Confluent Kafka per creare la pipeline. Questo progetto include una configurazione predefinita per la migrazione dei dati tra Kafka e la destinazione.

- Puoi specificare più domini Amazon OpenSearch Service come destinazioni per i tuoi dati. Questa funzionalità consente il routing o la replica condizionale dei dati in entrata in più domini Amazon Service. OpenSearch
- Puoi migrare i dati da un cluster Confluent Kafka di origine a una raccolta VPC Amazon Serverless. OpenSearch Assicurati di fornire una politica di accesso alla rete all'interno della configurazione della pipeline.
- È possibile utilizzare il registro degli schemi confluenti per definire uno schema confluente.

Il seguente esempio di pipeline inserisce dati da un cluster Confluent Kafka in un dominio Amazon Service: OpenSearch

```
version: "2"
kafka-pipeline:
  source:
    kafka:
```

```
      # Encryption is always required
      encryption:
        type: "ssl"
      topics:
        - name: "topic_4"
          group_id: "demoGroup"
      bootstrap_servers:
        # TODO: for public confluent kafka use public booststrap server dns
        - "<<bootstrap-server>>.us-west-2.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: "${{aws_secrets:confluent-kafka-secret:username}}"
            password: "${{aws_secrets:confluent-kafka-secret:password}}"
      # Schema is optional
      schema:
        type: confluent
        registry_url: https://<<registry-url>>.us-west-2.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
sink:
    - opensearch:
        hosts: [ "https://<<opensearchdomain>>.us-west-2.es.amazonaws.com" ]
        index: "enterprise-confluent-demo"
        aws:
          sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
          region: "<<aws-region>>"
 extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "enterprise-kafka-credentials"
        region: "<<aws-region>>"
        sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
      schema-secret:
        secret_id: "self-managed-kafka-schema"
        region: "<<aws-region>>"
        sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
```

Connettività a Confluent Kafka Cloud in VPC

Puoi utilizzare le pipeline di OpenSearch Ingestion per lo streaming di dati da un cluster Confluent Kafka con configurazione pubblica. A tale scopo, configura una pipeline di OpenSearch ingestione con Confluent Kafka come origine e un OpenSearch dominio Amazon Service o una raccolta Amazon Serverless come destinazione. OpenSearch La pipeline elabora tutti i dati in streaming dal cluster kafka e li inserisce nel cluster di destinazione.

Configurazione della rete Confluent Kafka

OpenSearch Ingestion supporta i cluster Confluent Kafka configurati in tutte le modalità di rete supportate in Confluent. Le seguenti modalità di configurazione di rete sono supportate come origine in Ingestion. OpenSearch

- AWS Peering VPC
- AWS PrivateLink per cluster dedicati
- AWS PrivateLink per cluster aziendali
- AWS Transit Gateway

Puoi utilizzare Kafka gestito da Confluent come fonte per l'acquisizione di dati da un cloud Confluent. A tal fine, configuri una pipeline in cui configuri Kafka come origine e un dominio Amazon OpenSearch Service o una raccolta Amazon OpenSearch Serverless come sink. Ciò facilita la migrazione dei dati da Kafka alla destinazione designata. La migrazione supporta anche l'utilizzo di un registro confluente o di nessun registro.

Per eseguire la migrazione dei dati, sono necessarie le seguenti risorse:

- Un cluster Confluent Kafka che funge da origine, contenente i dati che intendi migrare.
- Una destinazione di destinazione, ad esempio un dominio Amazon OpenSearch Service o una raccolta Amazon OpenSearch Serverless come sink.
- Un ID VPC di Amazon VPC che ha accesso a Confluent VPC.
- Il cluster Kafka dovrebbe avere l'autenticazione abilitata con le credenziali di. AWS Secrets Manager

Requisiti

Per configurare l'ingestione sul cluster Kafka, è necessario quanto segue:

- È necessario abilitare l'autenticazione AWS Secrets Manager basata sul cluster Kafka.
  - Configura l'autenticazione sul tuo cluster Kafka con. AWS Secrets Manager Abilita la rotazione dei segreti seguendo la procedura descritta in Ruota AWS Secrets Manager i segreti.
- Dovrai fornire il CIDR VPC da utilizzare dal OpenSearch servizio Ingestion.
  - Se utilizzi la console di AWS gestione per creare la tua pipeline, devi anche collegare la pipeline Amazon OpenSearch Ingestion al tuo VPC per utilizzare Confluent Kafka come sorgente. Per fare ciò, trova la sezione Configurazione di rete, seleziona la casella di controllo Collega a VPC e scegli il tuo CIDR o inserisci manualmente qualsiasi /24 CIDR da utilizzare per Ingestion. OpenSearch Il CIDR scelto per essere utilizzato da OpenSearch Ingestion dovrebbe essere diverso dal CIDR VPC su cui è in esecuzione Kafka gestito da Confluent. Ulteriori informazioni su Confluent Kafka CIDR da evitare qui. Di seguito sono riportate le opzioni CIDR predefinite che possono essere utilizzate da OpenSearch Ingestion Service per creare connettività di rete.
    - 10.99.20.0/24
    - 192,168,36,0/24
    - 172,21,56,0/24
- Dovrai creare un ruolo di pipeline in IAM con autorizzazioni per il dominio Amazon OpenSearch Service o la raccolta Amazon OpenSearch Serverless e il permesso di leggere i segreti. AWS Secrets Manager
  - Allega una policy basata sulle risorse al tuo OpenSearch dominio Amazon Service o una policy di accesso ai dati OpenSearch Amazon Serverless alla tua raccolta. Queste politiche di accesso consentono a OpenSearch Ingestion di scrivere dati da Kafka al OpenSearch dominio Amazon Service o alla raccolta Amazon Serverless. OpenSearch
- Per Confluent Kafka con connettività, configura AWS PrivateLink

  Opzioni DHCP VPC. I nomi host DNS e la risoluzione DNS devono essere abilitati.
  - nome di dominio: aws.private.confluent.cloud

    domain-name-servers: Amazon ha fornito DNS

Ruoli e autorizzazioni IAM

Il seguente esempio di policy di accesso al dominio consente al ruolo pipeline di scrivere dati su un dominio Amazon OpenSearch Service.

> **Note**
>
> Dovrai aggiornarlo `resource` con il tuo ARN.

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

L'esempio seguente fornisce le autorizzazioni necessarie per gestire l'interfaccia di rete:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
```

```
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [ "ec2:CreateTags" ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals": { "aws:RequestTag/OSISManaged": "true" }
            }
        }
    ]
```

L'esempio seguente fornisce le autorizzazioni necessarie per leggere segreti da: AWS Secrets Manager

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": ["secretsmanager:GetSecretValue"],
            "Resource": ["arn:aws:secretsmanager:<region>:<account-id>:secret:<secret-
name>"]
        }
    ]
}
```

L'esempio seguente fornisce le autorizzazioni necessarie per scrivere su un dominio Amazon OpenSearch Service:

```
{
  "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}/*"
    }
  ]
}
```

Creazione di una pipeline

Dopo aver associato la policy al ruolo di pipeline, puoi utilizzare il blueprint della pipeline di migrazione dei dati di Confluent Kafka per creare la tua pipeline. Questo progetto include una configurazione predefinita per la migrazione dei dati tra Kafka e la destinazione.

- Puoi specificare più domini Amazon OpenSearch Service come destinazioni per i tuoi dati. Questa funzionalità consente il routing o la replica condizionale dei dati in entrata su più Amazon Service. OpenSearch
- Puoi migrare i dati da un cluster Confluent Kafka di origine a una raccolta VPC Amazon Serverless. OpenSearch Assicurati di fornire una politica di accesso alla rete all'interno della configurazione della pipeline.
- È possibile utilizzare il registro degli schemi Confluent per definire lo schema Confluent.

Esempio di configurazione della pipeline

```
version: "2"
kafka-pipeline:
  source:
    kafka:
      # Encryption is always required
      encryption:
        type: "ssl"
      topics:
```

```
        - name: "topic_4"
          group_id: "demoGroup"
      bootstrap_servers:
        # TODO: for public confluent kafka use public booststrap server dns
        - "<<bootstrap-server>>.us-west-2.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: "${{aws_secrets:confluent-kafka-secret:username}}"
            password: "${{aws_secrets:confluent-kafka-secret:password}}"
      # Schema is optional
      schema:
        type: confluent
        registry_url: https://<<registry-url>>.us-west-2.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
    - opensearch:
        hosts: [ "https://<<opensearchdomain>>.us-west-2.es.amazonaws.com" ]
        index: "enterprise-confluent-demo"
        aws:
          sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
          region: "<<aws-region>>"
extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "enterprise-kafka-credentials"
        region: "<<aws-region>>"
        sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
      schema-secret:
        secret_id: "self-managed-kafka-schema"
        region: "<<aws-region>>"
        sts_role_arn: "arn:aws:iam::1234567890:role/os-os-test-role"
```

Utilizzo di una pipeline di OpenSearch ingestione con Amazon Managed Streaming for Apache Kafka

Puoi utilizzare il plug-in Kafka per inserire dati da Amazon Managed Streaming for Apache Kafka (Amazon MSK) nella tua pipeline di Ingestion. OpenSearch Con Amazon MSK, puoi creare ed eseguire applicazioni che utilizzano Apache Kafka per elaborare dati in streaming. OpenSearch

Ingestion utilizza AWS PrivateLink per connettersi ad Amazon MSK. Puoi importare dati da cluster Amazon MSK e Amazon MSK Serverless. L'unica differenza tra i due processi sono i passaggi preliminari da eseguire prima di configurare la pipeline.

Argomenti

Prerequisiti di Amazon MSK

Prima di creare la pipeline di OpenSearch Ingestion, esegui i seguenti passaggi:

1. Crea un cluster con provisioning Amazon MSK seguendo i passaggi descritti nella sezione Creazione di un cluster nella Amazon Managed Streaming for Apache Kafka Developer Guide. Per il tipo di broker, scegli qualsiasi opzione tranne i `t3` tipi, poiché questi non sono supportati da Ingestion. OpenSearch
2. Dopo che il cluster ha uno stato Attivo, segui i passaggi in Attivare la connettività multi-VPC.
3. Segui i passaggi in Allegare una politica del cluster al cluster MSK per allegare una delle seguenti politiche, a seconda che il cluster e la pipeline coincidano. Account AWS Questa policy consente a OpenSearch Ingestion di creare una AWS PrivateLink connessione al tuo cluster Amazon MSK e leggere dati da argomenti di Kafka. Assicurati di aggiornarlo `resource` con il tuo ARN.

   Le seguenti politiche si applicano quando il cluster e la pipeline coincidono: Account AWS

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

```
      "Action": [
        "kafka:CreateVpcConnection",
        "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:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    }
  ]
}
```

Se il tuo cluster Amazon MSK si trova in una pipeline Account AWS diversa dalla tua, allega invece la seguente policy. Tieni presente che l'accesso tra account è possibile solo con i cluster Amazon MSK forniti e non con i cluster Amazon MSK Serverless. L'ARN per il AWS `principal` dovrebbe essere l'ARN per lo stesso ruolo di pipeline fornito alla configurazione YAML della pipeline:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "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: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. Crea un argomento di Kafka seguendo la procedura descritta in Creare un argomento. Assicurati che *BootstrapServerString* sia uno degli URL di bootstrap dell'endpoint privato (Single-VPC). Il valore per `--replication-factor` dovrebbe essere 2 o3, in base al numero di zone del tuo cluster Amazon MSK. Il valore di `--partitions` deve essere almeno`10`.
5. Produci e consuma dati seguendo i passaggi descritti in Produrre e consumare dati. Ancora una volta, assicurati che *BootstrapServerString* sia uno degli URL di bootstrap dell'endpoint privato (Single-VPC).

Prerequisiti per Amazon MSK Serverless

Prima di creare la pipeline di OpenSearch Ingestion, esegui i seguenti passaggi:

1. Crea un cluster Serverless Amazon MSK seguendo i passaggi descritti in Creare un cluster Serverless MSK nella Amazon Managed Streaming for Apache Kafka Developer Guide.
2. Dopo che il cluster ha lo stato Attivo, segui i passaggi in Allegare una politica del cluster al cluster MSK per allegare la seguente politica. Assicurati di aggiornarlo `resource` con il tuo ARN.

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

Questa policy consente a OpenSearch Ingestion di creare una AWS PrivateLink connessione al tuo cluster Amazon MSK Serverless e leggere dati da argomenti di Kafka. Questa politica si

applica quando il cluster e la pipeline coincidono Account AWS, il che deve essere vero in quanto Amazon MSK Serverless non supporta l'accesso tra account.

3. Crea un argomento su Kafka seguendo la procedura descritta in Creare un argomento. Assicurati che *BootstrapServerString* sia uno degli URL di bootstrap IAM Simple Authentication and Security Layer (SASL). Il valore per `--replication-factor` dovrebbe essere 2 o3, in base al numero di zone del tuo cluster Amazon MSK Serverless. Il valore di `--partitions` deve essere almeno. `10`
4. Produci e consuma dati seguendo i passaggi descritti in Produrre e consumare dati. Ancora una volta, assicurati che *BootstrapServerString* sia uno degli URL di bootstrap IAM Simple Authentication and Security Layer (SASL).

Fase 1: Configurare il ruolo della pipeline

Dopo aver configurato il cluster Amazon MSK con provisioning o serverless, aggiungi le seguenti autorizzazioni Kafka nel ruolo pipeline che desideri utilizzare nella configurazione della pipeline:

```
{
    "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/*"
            ]
        }
    ]
}
```

Fase 2: Creare la pipeline

È quindi possibile configurare una pipeline OpenSearch di ingestione come la seguente, che specifica Kafka come origine:

```
version: "2"
log-pipeline:
  source:
    kafka:
      acknowledgements: true
      topics:
      - name: "topic-name"
        group_id: "group-id"
      aws:
        msk:
          arn: "arn:aws:kafka:{region}:{account-id}:cluster/cluster-name/cluster-id"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  processor:
  - grok:
      match:
        message:
        - "%{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
```

Puoi utilizzare un blueprint Amazon MSK preconfigurato per creare questa pipeline. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

Fase 3: (Facoltativo) Usa il registro degli schemi AWS Glue

Quando usi OpenSearch Ingestion con Amazon MSK, puoi utilizzare il formato di dati AVRO per gli schemi ospitati nel registro degli schemi. AWS Glue Con lo AWS Glue Schema Registry, puoi scoprire, controllare ed evolvere centralmente gli schemi dei flussi di dati.

Per utilizzare questa opzione, abilita lo schema `type` nella configurazione della pipeline:

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

Devi inoltre fornire i permessi AWS Glue di accesso in lettura nel tuo ruolo di pipeline. È possibile utilizzare la politica AWS gestita denominata. AWSGlueSchemaRegistryReadonlyAccess Inoltre, il registro deve trovarsi nella stessa Account AWS area geografica della pipeline di OpenSearch Ingestion.

Fase 4: (Facoltativo) Configurazione delle unità di calcolo consigliate (OCU) per la pipeline Amazon MSK

Ogni unità di elaborazione ha un consumatore per argomento. I broker bilanciano le partizioni tra questi consumatori per un determinato argomento. Tuttavia, quando il numero di partizioni è maggiore del numero di consumatori, Amazon MSK ospita più partizioni per ogni consumatore. OpenSearch Ingestion dispone della scalabilità automatica integrata per aumentare o ridurre in base all'utilizzo della CPU o al numero di record in sospeso nella pipeline.

Per prestazioni ottimali, distribuisci le partizioni su più unità di calcolo per l'elaborazione parallela. Se gli argomenti hanno un numero elevato di partizioni (ad esempio, più di 96, che è il numero massimo di OCU per pipeline), si consiglia di configurare una pipeline con 1—96 OCU. Questo perché verrà ridimensionato automaticamente in base alle esigenze. Se un argomento ha un numero

basso di partizioni (ad esempio, meno di 96), mantieni l'unità di calcolo massima uguale al numero di partizioni.

Quando una pipeline ha più di un argomento, scegli l'argomento con il maggior numero di partizioni come riferimento per configurare il numero massimo di unità di calcolo. Aggiungendo un'altra pipeline con un nuovo set di OCU allo stesso argomento e allo stesso gruppo di consumatori, puoi scalare il throughput in modo quasi lineare.

Utilizzo di una pipeline OpenSearch di ingestione con Amazon S3

Con OpenSearch Ingestion, puoi usare Amazon S3 come origine o come destinazione. Quando usi Amazon S3 come fonte, invii dati a una pipeline di OpenSearch ingestione. Quando usi Amazon S3 come destinazione, scrivi dati da una pipeline di OpenSearch ingestione su uno o più bucket S3.

Argomenti

Amazon S3 come fonte

Esistono due modi per utilizzare Amazon S3 come origine per elaborare i dati: con l'elaborazione S3-SQS e con le scansioni pianificate.

Utilizza l'elaborazione S3-SQS quando è necessaria una scansione quasi in tempo reale dei file dopo la scrittura su S3. Puoi configurare i bucket Amazon S3 per generare un evento ogni volta che un oggetto viene archiviato o modificato all'interno del bucket. Utilizza una scansione pianificata una tantum o ricorrente per elaborare in batch i dati in un bucket S3.

Argomenti

Prerequisiti

Per utilizzare Amazon S3 come origine per una pipeline di importazione sia per una scansione pianificata che per l' OpenSearch elaborazione S3-SQS, devi prima creare un bucket S3.

> **Note**
>
> Se il bucket S3 utilizzato come origine nella pipeline di OpenSearch Ingestion si trova in un altro, devi anche abilitare le autorizzazioni di lettura tra account sul bucket. Account AWS Ciò consente alla pipeline di leggere ed elaborare i dati. Per abilitare le autorizzazioni per più account, consulta la sezione relativa alla concessione delle autorizzazioni per i bucket tra più account nella Guida per l'utente di Amazon S3.
> Se i tuoi bucket S3 si trovano in più account, usa una mappa. `bucket_owners` Per un esempio, vedi Cross-account S3 access nella documentazione. OpenSearch

Per configurare l'elaborazione S3-SQS, è inoltre necessario eseguire le seguenti operazioni:

1. Crea una coda Amazon SQS.
2. Abilita le notifiche degli eventi sul bucket S3 con la coda SQS come destinazione.

Fase 1: Configurare il ruolo della pipeline

A differenza di altri plugin di origine che inviano dati a una pipeline, il plug-in di origine S3 ha un'architettura basata sulla lettura in cui la pipeline estrae i dati dalla sorgente.

Pertanto, affinché una pipeline possa leggere da S3, è necessario specificare un ruolo all'interno della configurazione di origine S3 della pipeline che abbia accesso sia al bucket S3 che alla coda Amazon SQS. La pipeline assumerà questo ruolo per leggere i dati dalla coda.

> **Note**
>
> Il ruolo specificato nella configurazione di origine di S3 deve essere il ruolo della pipeline.
> Pertanto, il ruolo della pipeline deve contenere due policy di autorizzazione separate, una per la scrittura su un sink e l'altra da estrarre dal codice sorgente S3. È necessario utilizzare lo stesso in tutti i componenti della pipeline. `sts_role_arn`

La seguente politica di esempio mostra le autorizzazioni necessarie per l'utilizzo di S3 come fonte:

```
{
  "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"
    }
  ]
}
```

È necessario associare queste autorizzazioni al ruolo IAM specificato nell'`sts_role_arn`opzione all'interno della configurazione del plug-in di origine S3:

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

Fase 2: Creare la pipeline

Dopo aver impostato le autorizzazioni, puoi configurare una pipeline di OpenSearch ingestione in base al tuo caso d'uso di Amazon S3.

Elaborazione S3-SQS

Per configurare l'elaborazione S3-SQS, configura la pipeline per specificare S3 come origine e configura le notifiche di 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:
        message:
        - "%{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"
```

Se riscontri un basso utilizzo della CPU durante l'elaborazione di file di piccole dimensioni su Amazon S3, valuta la possibilità di aumentare la velocità effettiva modificando il valore dell'opzione. `workers` Per ulteriori informazioni, consulta le opzioni di configurazione del plug-in S3.

Scansione pianificata

Per configurare una scansione pianificata, configura la pipeline con una pianificazione a livello di scansione applicabile a tutti i bucket S3 o a livello di bucket. Una pianificazione a livello di bucket o una configurazione a intervalli di scansione sovrascrive sempre una configurazione a livello di scansione.

È possibile configurare le scansioni pianificate con una scansione singola, ideale per la migrazione dei dati, o una scansione ricorrente, ideale per l'elaborazione in batch.

Per configurare la pipeline in modo che legga da Amazon S3, utilizza i blueprint Amazon S3 preconfigurati. Puoi modificare la `scan` parte della configurazione della pipeline per soddisfare le tue esigenze di pianificazione. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

Scansione una tantum

Una scansione pianificata una tantum viene eseguita una sola volta. Nella configurazione YAML, puoi usare un `start_time` e `end_time` per specificare quando vuoi che gli oggetti nel bucket vengano scansionati. In alternativa, è possibile utilizzare `range` per specificare l'intervallo di tempo relativo all'ora corrente in cui si desidera che gli oggetti nel bucket vengano scansionati.

Ad esempio, un intervallo impostato per PT4H scansionare tutti i file creati nelle ultime quattro ore. Per configurare una scansione singola da eseguire una seconda volta, è necessario arrestare e riavviare la pipeline. Se non hai configurato un intervallo, devi anche aggiornare l'ora di inizio e di fine.

La seguente configurazione imposta una scansione unica per tutti i bucket e tutti gli oggetti in tali bucket:

```
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 seguente configurazione imposta una scansione unica per tutti i bucket durante una finestra temporale specificata. Ciò significa che S3 elabora solo gli oggetti con tempi di creazione che rientrano in questa finestra.

```
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 seguente configurazione imposta una scansione una tantum sia a livello di scansione che a livello di bucket. Gli orari di inizio e fine a livello di bucket sostituiscono gli orari di inizio e fine a livello di scansione.

```
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
```

L'arresto di una pipeline rimuove qualsiasi riferimento preesistente a quali oggetti sono stati scansionati dalla pipeline prima dell'arresto. Se una singola pipeline di scansione viene interrotta, eseguirà nuovamente la scansione di tutti gli oggetti dopo l'avvio, anche se erano già stati scansionati. Se è necessario interrompere una singola pipeline di scansione, si consiglia di modificare la finestra temporale prima di riavviare la pipeline.

Se è necessario filtrare gli oggetti in base all'ora di inizio e all'ora di fine, l'unica opzione è interrompere e avviare la pipeline. Se non è necessario filtrare per ora di inizio e ora di fine, è possibile filtrare gli oggetti per nome. Il filtraggio per nome non richiede di interrompere e avviare la pipeline. Per fare ciò, usa e. `include_prefix` `exclude_suffix`

Scansione ricorrente

Una scansione pianificata ricorrente esegue una scansione dei bucket S3 specificati a intervalli regolari e pianificati. Puoi configurare questi intervalli solo a livello di scansione perché le configurazioni a livello di bucket individuali non sono supportate.

Nella configurazione YAML, `interval` specifica la frequenza della scansione ricorrente e può essere compresa tra 30 secondi e 365 giorni. La prima di queste scansioni si verifica sempre quando si crea la pipeline. `count`Definisce il numero totale di istanze di scansione.

La seguente configurazione imposta una scansione ricorrente, con un ritardo di 12 ore tra le scansioni:

```
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 come destinazione

Per scrivere dati da una pipeline di OpenSearch ingestione a un bucket S3, usa il blueprint S3 preconfigurato per creare una pipeline con un sink S3. Questa pipeline indirizza i dati selettivi verso un sink e invia simultaneamente tutti i dati per l'archiviazione in S3. OpenSearch Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

Quando crei il tuo sink S3, puoi specificare la formattazione preferita tra una varietà di codec sink. Ad esempio, se desideri scrivere dati in formato colonnare, scegli il codec Parquet o Avro. Se preferisci un formato basato su righe, scegli JSON o ND-JSON. Per scrivere dati su S3 in uno schema specificato, puoi anche definire uno schema in linea all'interno dei codec sink utilizzando il formato Avro.

L'esempio seguente definisce uno schema in linea in un sink 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"}
          ]
        }
```

Quando definisci questo schema, specifica un superset di tutte le chiavi che potrebbero essere presenti nei diversi tipi di eventi che la pipeline invia a un sink.

Ad esempio, se in un evento è possibile che manchi una chiave, aggiungete quella chiave allo schema con un `null` valore. Le dichiarazioni di valori nulli consentono allo schema di elaborare dati non uniformi (laddove alcuni eventi abbiano queste chiavi e altri no). Quando negli eventi in entrata sono presenti queste chiavi, i relativi valori vengono scritti nei sink.

Questa definizione dello schema funge da filtro che consente solo l'invio di chiavi definite ai sink e rimuove le chiavi non definite dagli eventi in arrivo.

Puoi anche utilizzare `include_keys` e `exclude_keys` nel tuo sink per filtrare i dati che vengono indirizzati ad altri sink. Questi due filtri si escludono a vicenda, quindi puoi utilizzarne solo uno alla volta nello schema. Inoltre, non è possibile utilizzarli all'interno di schemi definiti dall'utente.

Per creare pipeline con tali filtri, utilizza il blueprint del filtro sink preconfigurato. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

Account multiplo Amazon S3 come fonte

Puoi concedere l'accesso a più account con Amazon S3 in modo che le pipeline di OpenSearch Ingestion possano accedere ai bucket S3 in un altro account come fonte. Per abilitare l'accesso su più account, consulta la sezione relativa alla concessione delle autorizzazioni per i bucket tra più account nella Amazon S3 User Guide. Dopo aver concesso l'accesso, assicurati che il tuo ruolo di pipeline disponga delle autorizzazioni richieste.

Quindi, puoi creare una configurazione YAML utilizzando `bucket_owners` per abilitare l'accesso tra account a un bucket Amazon S3 come origine:

```
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:
     my-bucket-01: 123456789012
     my-bucket-02: 999999999999
    compression: "gzip"
```

Utilizzo di una pipeline OpenSearch di ingestione con Amazon Security Lake

Puoi utilizzare il plug-in sorgente S3 per importare dati da Amazon Security Lake nella tua pipeline di OpenSearch ingestione. Security Lake centralizza automaticamente i dati di sicurezza provenienti da AWS ambienti, ambienti locali e provider SaaS in un data lake appositamente progettato. È possibile creare un abbonamento che replica i dati da Security Lake alla pipeline di OpenSearch Ingestion, che poi li scrive nel dominio di servizio o nella raccolta Serverless. OpenSearch OpenSearch

Per configurare la pipeline in modo che legga da Security Lake, utilizza il blueprint Security Lake preconfigurato. Il blueprint include una configurazione predefinita per l'importazione di file parquet Open Cybersecurity Schema Framework (OCSF) da Security Lake. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

Argomenti

- Prerequisiti
- Fase 1: Configurare il ruolo della pipeline
- Fase 2: Creare la pipeline

Prerequisiti

Prima di creare la pipeline di OpenSearch Ingestion, effettuate le seguenti operazioni:

- Abilita Security Lake.
- Crea un abbonato in Security Lake.

- Scegli le fonti che desideri inserire nella tua pipeline.
- Per le credenziali dell'abbonato, aggiungi l'ID del Account AWS luogo in cui intendi creare la pipeline. Per l'ID esterno, specificare. `OpenSearchIngestion-{accountid}`
- Per il metodo di accesso ai dati, scegli S3.
- Per i dettagli della notifica, scegli SQS queue.

Quando crei un abbonato, Security Lake crea automaticamente due policy di autorizzazione in linea, una per S3 e una per SQS. Le politiche hanno il seguente formato: e. `AmazonSecurityLake-{12345}-S3` `AmazonSecurityLake-{12345}-SQS` Per consentire alla tua pipeline di accedere alle fonti degli abbonati, devi associare le autorizzazioni richieste al tuo ruolo di pipeline.

Fase 1: Configurare il ruolo della pipeline

Crea una nuova politica di autorizzazioni in IAM che combini solo le autorizzazioni richieste dalle due policy create automaticamente da Security Lake. La seguente policy di esempio mostra il privilegio minimo richiesto a una pipeline di OpenSearch Ingestion per leggere i dati da più fonti 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 non gestisce al posto tuo la policy relativa ai ruoli della pipeline. Se aggiungi o rimuovi fonti dal tuo abbonamento a Security Lake, devi aggiornare manualmente la politica. Security Lake crea partizioni per ogni origine di registro, quindi è necessario aggiungere o rimuovere manualmente le autorizzazioni nel ruolo della pipeline.

È necessario associare queste autorizzazioni al ruolo IAM specificato nell'`sts_role_arn`opzione all'interno della configurazione del plug-in di origine S3, sotto. `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:
      ...
```

Fase 2: Creare la pipeline

Dopo aver aggiunto le autorizzazioni al ruolo di pipeline, utilizza il blueprint S3 preconfigurato per creare la pipeline. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

È necessario specificare l'`queue_url`opzione all'interno della configurazione di `s3` origine, che è l'URL della coda di Amazon SQS da cui leggere. Per formattare l'URL, individua l'endpoint Subscription nella configurazione del sottoscrittore e passa a. `arn:aws:` `https://` Ad esempio, `https://sqs.`*`{region}`*`.amazonaws.com/`*`{account-id}`*`/AmazonSecurityLake-`*`abdcef`*`-Main-Queue`.

`sts_role_arn`Quello che specifichi all'interno della configurazione di origine S3 deve essere l'ARN del ruolo della pipeline.

Utilizzo di una pipeline di OpenSearch ingestione con Fluent Bit

Questo file di configurazione Fluent Bit di esempio invia i dati di registro da Fluent Bit a una pipeline di ingestione. OpenSearch Per ulteriori informazioni sull'acquisizione dei dati di registro, consulta Log Analytics nella documentazione di Data Prepper.

Tieni presente quanto segue:

- Il `host` valore deve essere l'endpoint della pipeline. Ad esempio, *`pipeline-endpoint`*`.us-east-1.osis.amazonaws.com`.
- Il valore `aws_service` deve essere `osis`.
- Il `aws_role_arn` valore è l'ARN del ruolo AWS IAM che il client deve assumere e utilizzare per l'autenticazione Signature Version 4.

```
[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
```

È quindi possibile configurare una pipeline di OpenSearch ingestion come la seguente, che ha HTTP come origine:

```
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"
```

Utilizzo di una pipeline di OpenSearch ingestione con Fluentd

Fluentd è un ecosistema di raccolta dati open source che fornisce SDK per diverse lingue e sottoprogetti come Fluent Bit. Questo file di configurazione Fluentd di esempio invia i dati di registro

da Fluentd a una pipeline di Ingestion. OpenSearch Per ulteriori informazioni sull'acquisizione dei dati di registro, consulta Log Analytics nella documentazione di Data Prepper.

Tieni presente quanto segue:

- Il `endpoint` valore deve essere l'endpoint della pipeline. Ad esempio, *`pipeline-endpoint`*`.us-east-1.osis.amazonaws.com/apache-log-pipeline/logs`.
- Il valore `aws_service` deve essere `osis`.
- Il `aws_role_arn` valore è l'ARN del ruolo AWS IAM che il client deve assumere e utilizzare per l'autenticazione Signature Version 4.

```
<source>
  @type tail
  path logs/sample.log
  path_key log
  tag apache
  <parse>
    @type none
  </parse>
</source>

<filter apache>
  @type record_transformer
  <record>
    log ${record["message"]}
  </record>
</filter>

<filter apache>
  @type record_transformer
  remove_keys message
</filter>

<match apache>
  @type http
  endpoint pipeline-endpoint.us-east-1.osis.amazonaws.com/apache-log-pipeline/logs
  json_array true

  <auth>
    method aws_sigv4
    aws_service osis
```

```
    aws_region us-east-1
    aws_role_arn arn:aws:iam::{account-id}:role/ingestion-role
  </auth>

  <format>
    @type json
  </format>

  <buffer>
    flush_interval 1s
  </buffer>
</match>
```

È quindi possibile configurare una pipeline di OpenSearch ingestion come la seguente, che ha HTTP come origine:

```
version: "2"
apache-log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
  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}"
  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
```

Utilizzo di una pipeline di OpenSearch ingestione con Collector OpenTelemetry

Questo file di OpenTelemetry configurazione di esempio esporta i dati di traccia dal OpenTelemetry Collector e li invia a una pipeline di OpenSearch Ingestion. Per ulteriori informazioni sull'importazione dei dati di traccia, consulta Trace Analytics nella documentazione di Data Prepper.

Tieni presente quanto segue:

- Il `endpoint` valore deve includere l'endpoint della pipeline. Ad esempio, `https://pipeline-endpoint.us-east-1.osis.amazonaws.com`.
- Il valore `service` deve essere `osis`.
- L'`compression`opzione per l'esportatore OTLP/HTTP deve corrispondere all'`compression`opzione sull'origine della pipeline. 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]
```

È quindi possibile configurare una pipeline di OpenSearch ingestione come la seguente, che specifica il plug-in Otel Trace come origine:

```
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"
```

Per un altro esempio di pipeline, consultate il blueprint preconfigurato di analisi delle tracce. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

Passaggi successivi

Dopo aver esportato i dati in una pipeline, puoi interrogarli dal dominio di OpenSearch servizio configurato come sink per la pipeline. Le seguenti risorse possono aiutarti a iniziare:

- Osservabilità
- the section called “Trace Analytics”
- the section called “Piped Processing Language (PPL)”

Migrazione dei dati tra domini e raccolte utilizzando Amazon Ingestion OpenSearch

Puoi utilizzare le pipeline OpenSearch di Ingestion per migrare i dati tra domini Amazon OpenSearch Service o OpenSearch raccolte VPC Serverless. A tale scopo, configuri una pipeline in cui configuri un dominio o una raccolta come origine e un altro dominio o raccolta come sink. Questo consente di migrare efficacemente i dati da un dominio o una raccolta all'altra.

Per migrare i dati, è necessario disporre delle seguenti risorse:

- Un dominio di OpenSearch servizio di origine o una raccolta VPC OpenSearch Serverless. Questo dominio o raccolta contiene i dati che desideri migrare. Se utilizzi un dominio, deve eseguire la OpenSearch versione 1.0 o successiva oppure Elasticsearch versione 7.4 o successiva. Il dominio deve inoltre avere una politica di accesso che conceda le autorizzazioni appropriate al tuo ruolo di pipeline.
- Un dominio o una raccolta VPC separata verso cui migrare i dati. Questo dominio o raccolta fungerà da serbatoio della pipeline.
- Un ruolo della pipeline che OpenSearch Ingestion utilizzerà per leggere e scrivere nella raccolta o nel dominio. Includi l'Amazon Resource Name (ARN) di questo ruolo nella configurazione della pipeline. Per ulteriori informazioni, consulta le seguenti risorse:
  - the section called “Concedere alle pipeline l'accesso ai domini”
  - the section called “Concedere alle pipeline l'accesso alle raccolte”

Argomenti

- Limitazioni
- OpenSearch Il servizio come fonte
- Specificazione di più sink di dominio di servizio OpenSearch
- Migrazione dei dati verso una raccolta OpenSearch VPC serverless

Limitazioni

Le seguenti limitazioni si applicano quando si designano domini di OpenSearch servizio o raccolte OpenSearch Serverless come sink:

- Una pipeline non può scrivere su più di un dominio VPC.
- Puoi migrare i dati solo da o verso raccolte OpenSearch Serverless che utilizzano l'accesso VPC. Le raccolte pubbliche non sono supportate.
- Non è possibile specificare una combinazione di VPC e domini pubblici in una configurazione a pipeline singola.
- È possibile avere un massimo di 20 sink non collegati alla pipeline all'interno di una singola configurazione di pipeline.
- È possibile specificare i sink scegliendo tra un massimo di tre tipi diversi Regioni AWS in una configurazione a tubazione singola.
- Una pipeline con più sink potrebbe subire una riduzione della velocità di elaborazione nel tempo se uno dei sink rimane inattivo per troppo tempo o non dispone di una capacità sufficiente per ricevere i dati in entrata.

OpenSearch Il servizio come fonte

Il dominio o la raccolta che specifichi come origine è il luogo da cui vengono migrati i dati.

Creazione di un ruolo di pipeline in IAM

Per creare la pipeline di OpenSearch Ingestion, devi prima creare un ruolo di pipeline per concedere l'accesso in lettura e scrittura tra domini o raccolte. A tale scopo, effettuate le seguenti operazioni:

1. Crea una nuova politica di autorizzazioni in IAM da collegare al ruolo della pipeline. Assicurati di consentire le autorizzazioni per leggere dalla fonte e scrivere nel sink. Per ulteriori informazioni sull'impostazione delle autorizzazioni della pipeline IAM per i domini di OpenSearch servizio, consulta e. the section called “Concedere alle pipeline l'accesso ai domini” the section called “Concedere alle pipeline l'accesso alle raccolte”
2. Specificate le seguenti autorizzazioni all'interno del ruolo della pipeline da leggere dalla fonte:

```
{
   "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"
         ]
      }
   ]
}
```

Creare una pipeline

Dopo aver associato la policy al ruolo della pipeline, utilizza il blueprint di AWSOpenSearchDataMigrationPipelinemigrazione per creare la pipeline. Questo blueprint include una configurazione predefinita per la migrazione dei dati tra OpenSearch domini o raccolte di servizi. Per ulteriori informazioni, consulta the section called “Utilizzo dei blueprint per creare una pipeline”.

> **Note**
>
> OpenSearch Ingestion utilizza la versione e la distribuzione del dominio di origine per determinare il meccanismo da utilizzare per la migrazione. Alcune versioni supportano l'opzione. `point_in_time` OpenSearch Serverless utilizza l'`search_after`opzione perché non supporta `point_in_time` `oscroll`.

È possibile che durante il processo di migrazione siano in corso di creazione nuovi indici oppure che i documenti vengano aggiornati durante la migrazione. Per questo motivo, potrebbe essere necessario eseguire una scansione singola o più scansioni dei dati dell'indice di dominio per raccogliere dati nuovi o aggiornati.

Specificate il numero di scansioni da eseguire configurando la configurazione `index_read_count` e `interval` nella pipeline. L'esempio seguente mostra come eseguire scansioni multiple:

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

OpenSearch Ingestion utilizza la seguente configurazione per garantire che i dati vengano scritti nello stesso indice e mantengano lo stesso ID del documento:

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

Specificazione di più sink di dominio di servizio OpenSearch

È possibile specificare più domini di OpenSearch servizio pubblici come destinazioni per i dati. È possibile utilizzare questa funzionalità per eseguire il routing condizionale o replicare i dati in entrata in più domini di servizio. OpenSearch È possibile specificare fino a 10 diversi domini di servizio pubblici OpenSearch come sink.

Nell'esempio seguente, i dati in entrata vengono instradati in modo condizionale a diversi domini di servizio: OpenSearch

```
...
```

```
  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
```

Migrazione dei dati verso una raccolta OpenSearch VPC serverless

È possibile utilizzare OpenSearch Ingestion per migrare i dati da un dominio di OpenSearch servizio di origine o da una raccolta OpenSearch Serverless a un sink di raccolta VPC. È necessario fornire una politica di accesso alla rete all'interno della configurazione della pipeline. Per ulteriori informazioni sull'inserimento di dati nelle raccolte VPC OpenSearch serverless, vedere. the section called “Tutorial: inserisci dati in una raccolta”

Per migrare i dati in una raccolta VPC

1. Crea una raccolta OpenSearch serverless. Per istruzioni, consulta the section called “Tutorial: inserisci dati in una raccolta”.
2. Crea una politica di rete per la raccolta che specifichi l'accesso VPC sia all'endpoint di raccolta che all'endpoint Dashboards. Per istruzioni, consulta the section called “Accesso alla rete”.
3. Crea il ruolo pipeline se non ne hai già uno. Per istruzioni, consulta the section called “Ruolo Pipeline”.
4. Crea la pipeline. Per istruzioni, consultare the section called “Utilizzo dei blueprint per creare una pipeline”.

Utilizzo degli AWS SDK per interagire con Amazon Ingestion OpenSearch

Questa sezione include un esempio di come utilizzare gli AWS SDK per interagire con Amazon OpenSearch Ingestion. L'esempio di codice dimostra come creare un dominio e una pipeline e quindi inserire dati nella pipeline.

Argomenti

Python

Lo script di esempio seguente utilizza il ruolo della pipeline IAM AWS SDK for Python (Boto3)per creare un ruolo di pipeline IAM, un dominio in cui scrivere dati e una pipeline attraverso cui importare i dati. Quindi inserisce un file di registro di esempio nella pipeline utilizzando la libreria `requests` HTTP.

Per installare le dipendenze richieste, eseguire i seguenti comandi:

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

All'interno dello script, sostituisci gli ID dell'account nelle politiche di accesso con il tuo Account AWS ID. Facoltativamente, è possibile anche modificare la `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()
```

Sicurezza in Amazon OpenSearch Ingestion

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue AWS i servizi nel cloud AWS. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformità AWS.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, le leggi e le normative applicabili.

Questa documentazione OpenSearch faciliticonsenteladicomprensionedelapplicare il modello di responsabilità condivisa quando utilizzusa usa usa usa usa usa. I seguenti argomenti illustrano come configurare OpenSearch Ingestion per soddisfare gli obiettivi di sicurezza e conformità. Vengono inoltre fornite informazioni su come utilizzare altri AWS servizi che consentono di monitorare e proteggere le risorse OpenSearch di Ingestione.

Argomenti

Configurazione dell'accesso VPC per le pipeline di Amazon Ingestion OpenSearch

Puoi accedere alle tue pipeline di Amazon OpenSearch Ingestion utilizzando un endpoint VPC di interfaccia. Un VPC è una rete virtuale dedicata a te. Account AWSÈ logicamente isolato dalle altre reti virtuali nel AWS cloud. L'accesso a una pipeline tramite un endpoint VPC consente una comunicazione sicura OpenSearch tra Ingestion e altri servizi all'interno del VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS

OpenSearch Ingestion stabilisce questa connessione privata creando un endpoint di interfaccia, alimentato da. AWS PrivateLink Creiamo un'interfaccia di rete endpoint in ogni sottorete specificata durante la creazione della pipeline. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato alla pipeline di ingestione. OpenSearch Puoi anche scegliere di creare e gestire tu stesso gli endpoint dell'interfaccia.

L'utilizzo di un VPC consente di imporre il flusso di dati attraverso le pipeline di OpenSearch ingestione entro i confini del VPC, anziché sulla rete Internet pubblica. Le pipeline che non si trovano all'interno di un VPC inviano e ricevono dati su endpoint pubblici e su Internet.

Una pipeline con accesso VPC può scrivere su domini di servizio pubblici o OpenSearch VPC e su raccolte pubbliche o VPC Serverless. OpenSearch

Argomenti

- Prerequisiti
- Configurazione dell'accesso VPC per una pipeline
- Endpoint VPC autogestiti
- Ruolo collegato ai servizi per l'accesso VPC

Considerazioni

Considerate quanto segue quando configurate l'accesso VPC per una pipeline.

- Non è necessario che una pipeline si trovi nello stesso VPC del relativo sink. Inoltre, non è necessario stabilire una connessione tra i due VPC. OpenSearch Ingestion si occupa di collegarli per te.
- Puoi specificare un solo VPC per la tua pipeline.
- A differenza delle pipeline pubbliche, una pipeline VPC deve trovarsi nello Regione AWS stesso dominio o sink di raccolta su cui sta scrivendo.
- Puoi scegliere di implementare una pipeline in una, due o tre sottoreti del tuo VPC. Le sottoreti sono distribuite nelle stesse zone di disponibilità in cui sono distribuite le Ingestion Compute OpenSearch Unit (OCU).
- Se distribuisci una pipeline solo in una sottorete e la zona di disponibilità non funziona, non sarai in grado di importare dati. Per garantire un'elevata disponibilità, consigliamo di configurare le pipeline con due o tre sottoreti.
- La specificazione di un gruppo di sicurezza è facoltativa. Se non fornisci un gruppo di sicurezza, OpenSearch Ingestion utilizza il gruppo di sicurezza predefinito specificato nel VPC.

Limitazioni

Le pipeline con accesso VPC presentano le seguenti limitazioni.

- Non è possibile modificare la configurazione di rete di una pipeline dopo averla creata. Se avvii una pipeline all'interno di un VPC, non puoi modificarla successivamente in un endpoint pubblico e viceversa.
- Puoi avviare la tua pipeline con un endpoint VPC di interfaccia o un endpoint pubblico, ma non puoi fare entrambe le cose. È necessario scegliere l'uno o l'altro quando si crea una pipeline.
- Dopo aver effettuato il provisioning di una pipeline con accesso VPC, non è possibile spostarla su un altro VPC e non è possibile modificarne le sottoreti o le impostazioni del gruppo di sicurezza.

- Se la pipeline scrive su un dominio o un sink di raccolta che utilizza l'accesso VPC, non puoi tornare indietro in un secondo momento e modificare il sink (VPC o pubblico) dopo la creazione della pipeline. È necessario eliminare e ricreare la pipeline con un nuovo sink. Puoi comunque passare da un lavandino pubblico a un lavandino con accesso VPC.
- Non puoi fornire l'accesso di importazione tra account diversi alle pipeline VPC.

Prerequisiti

Prima di poter effettuare il provisioning di una pipeline con accesso VPC, è necessario effettuare le seguenti operazioni:

- Crea un VPC

  Per creare il tuo VPC, puoi utilizzare la console Amazon VPC, la AWS CLI o uno degli SDK. AWS Per ulteriori informazioni, consultare Utilizzo dei VPC nella Guida per l'utente di Amazon VPC. Se hai già un VPC, questa fase può essere ignorata.
- Prenota indirizzi IP

  OpenSearch L'ingestione inserisce un'interfaccia elastica di rete in ogni sottorete specificata durante la creazione della pipeline. Ogni interfaccia di rete è associata a un indirizzo IP. È necessario riservare un indirizzo IP per sottorete per le interfacce di rete.

Configurazione dell'accesso VPC per una pipeline

È possibile abilitare l'accesso VPC per una pipeline all'interno della console di OpenSearch servizio o utilizzando il. AWS CLI

Console

L'accesso al VPC viene configurato durante la creazione della pipeline. In Rete, scegli Accesso VPC e configura le seguenti impostazioni:

Impostazione	Descrizione
Gestione degli endpoint	Scegliete se volete creare voi stessi gli endpoint VPC o lasciateli creare da OpenSearch Ingestion per voi.

Impostazione	Descrizione
VPC	Scegli l'ID per il cloud privato virtuale (VPC) da utilizzare. Il VPC e la pipeline devono trovarsi nello stesso ambiente. Regione AWS
Sottoreti	Scegli una o più sottoreti. OpenSearch Il servizio inserirà un endpoint VPC e interfacce di rete elastiche nelle sottoreti.
Gruppi di sicurezza	Scegli uno o più gruppi di sicurezza VPC che consentano all'applicazione richiesta di raggiungere la pipeline di OpenSearch ingestione sulle porte (80 o 443) e sui protocolli (HTTP o HTTPS) esposti dalla pipeline.
Opzioni di collegamento VPC	Se la tua fonte è un endpoint autogestito, collega la pipeline a un VPC. Scegli una delle opzioni CIDR predefinite fornite o utilizza un CIDR personali zzato.

CLI

Per configurare l'accesso al VPC utilizzando AWS CLI, specificare il `--vpc-options` parametro:

```
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"
```

Endpoint VPC autogestiti

Quando crei una pipeline, puoi utilizzare la gestione degli endpoint per creare una pipeline con endpoint autogestiti o endpoint gestiti dal servizio. La gestione degli endpoint è facoltativa e per impostazione predefinita utilizza gli endpoint gestiti da Ingestion. OpenSearch

Per creare una pipeline con un endpoint VPC autogestito in AWS Management Console, consulta Creazione di pipeline con la console di servizio. OpenSearch Per creare una pipeline con un endpoint VPC autogestito in AWS CLI, puoi utilizzare il `--vpc-options` parametro nel comando create-pipeline:

```
--vpc-options SubnetIds=subnet-abcdef01234567890,VpcEndpointManagement=CUSTOMER
```

Puoi creare tu stesso un endpoint per la tua pipeline quando specifichi il tuo servizio endpoint. Per trovare il tuo servizio endpoint, usa il comando get-pipeline, che restituisce una risposta simile alla seguente:

```
"vpcEndpointService" : "com.amazonaws.osis.us-east-1.pipeline-
id-1234567890abcdef1234567890",
"vpcEndpoints" : [
  {
    "vpcId" : "vpc-1234567890abcdef0",
    "vpcOptions" : {
      "subnetIds" : [ "subnet-abcdef01234567890", "subnet-021345abcdef6789" ],
      "vpcEndpointManagement" : "CUSTOMER"
    }
  }
```

Usa il `vpcEndpointService` from the response per creare un endpoint VPC con o. AWS Management Console AWS CLI

Se utilizzi endpoint VPC autogestiti, devi abilitare gli attributi DNS `enableDnsSupport` e `enableDnsHostnames` nel tuo VPC. Tieni presente che se disponi di una pipeline con un endpoint autogestito che interrompi e riavvii, devi ricreare l'endpoint VPC nel tuo account.

Ruolo collegato ai servizi per l'accesso VPC

Un ruolo collegato ai servizi è un tipo specifico di ruolo IAM che delega le autorizzazioni a un servizio così che possa creare e gestire le risorse per conto dell'utente. Se scegli un endpoint VPC gestito dal servizio, OpenSearch Ingestion richiede un ruolo collegato al servizio chiamato AWSServiceRoleForAmazonOpenSearchIngestionServiceper accedere al tuo VPC, creare l'endpoint della pipeline e posizionare le interfacce di rete in una sottorete del VPC.

Se scegli un endpoint VPC autogestito OpenSearch , Ingestion richiede un ruolo collegato al servizio chiamato. AWSServiceRoleForOpensearchIngestionSelfManagedVpce Per ulteriori informazioni su questi ruoli, le relative autorizzazioni e su come eliminarli, consulta. the section called “Ruolo di creazione della pipeline”

OpenSearch Ingestion crea automaticamente il ruolo quando si crea una pipeline di ingestione. Affinché questa creazione automatica abbia esito positivo, l'utente che crea la prima pipeline in un account deve disporre delle autorizzazioni per l'azione. `iam:CreateServiceLinkedRole` Per

ulteriori informazioni, consultare Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM. Puoi visualizzare il ruolo nella console AWS Identity and Access Management (IAM) dopo la sua creazione.

Identity and Access Management per Amazon OpenSearch Ingestion

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Ingestion. OpenSearch IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Politiche basate sull'identità per Ingestion OpenSearch
- OpenSearch Azioni politiche per Ingestion
- OpenSearch Risorse politiche per Ingestion
- Chiavi delle condizioni delle politiche per Amazon OpenSearch Ingestion
- ABAC con Ingestion OpenSearch
- Utilizzo di credenziali temporanee con Ingestion OpenSearch
- Ruoli collegati ai servizi per Ingestion OpenSearch
- Esempi di policy basate sull'identità per Ingestion OpenSearch

Politiche basate sull'identità per Ingestion OpenSearch

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy

JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per Ingestion OpenSearch

Per visualizzare esempi di politiche basate sull'identità di OpenSearch Ingestion, vedere. the section called “Esempi di policy basate su identità”

OpenSearch Azioni politiche per Ingestion

Supporta le operazioni di policy	Sì

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche in OpenSearch Ingestion utilizzano il seguente prefisso prima dell'azione:

```
osis
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "osis:action1",
      "osis:action2"
         ]
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `List`, includi la seguente azione:

```
"Action": "osis:List*"
```

Per visualizzare esempi di politiche basate sull'identità di OpenSearch Ingestion, vedere. Esempi di policy basate sull'identità per Serverless OpenSearch

OpenSearch Risorse politiche per Ingestion

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Chiavi delle condizioni delle politiche per Amazon OpenSearch Ingestion

Supporta le chiavi di condizione delle policy specifiche del servizio	No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi delle condizioni di OpenSearch ingestione, consulta Condition keys for Amazon OpenSearch Ingestion nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon OpenSearch Ingestion.

ABAC con Ingestion OpenSearch

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Per ulteriori informazioni sull'etichettatura delle risorse di OpenSearch Ingestion, consulta. the section called “Etichettatura delle tubazioni”

Utilizzo di credenziali temporanee con Ingestion OpenSearch

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Ruoli collegati ai servizi per Ingestion OpenSearch

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

OpenSearch Ingestion utilizza un ruolo collegato al servizio chiamato. `AWSServiceRoleForAmazonOpenSearchIngestionService` Il ruolo collegato ai servizi denominato `AWSServiceRoleForOpensearchIngestionSelfManagedVpce` è disponibile anche per le pipeline con endpoint VPC autogestiti. Per informazioni dettagliate sulla creazione e la gestione

dei ruoli collegati al servizio Ingestion, consulta OpenSearch . the section called “Ruolo di creazione della pipeline”

Esempi di policy basate sull'identità per Ingestion OpenSearch

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse di Ingestion. OpenSearch Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Amazon OpenSearch Ingestion, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon OpenSearch Ingestion nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo di OpenSearch Ingestion nella console
- OpenSearch Amministrazione delle pipeline di Ingestion
- Inserimento di dati in una pipeline di ingestione OpenSearch

Best practice per le policy

Le policy basate su identità sono molto efficaci. Determinano se qualcuno può creare, accedere o eliminare le risorse di OpenSearch Ingestion nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di OpenSearch Ingestion nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono

le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo di OpenSearch Ingestion nella console

Per accedere a OpenSearch Ingestion dalla console di OpenSearch servizio, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire all'utente di elencare e visualizzare i dettagli sulle risorse di OpenSearch Ingestion presenti nell'account. AWS Se crei una

policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (come i ruoli IAM) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso o l' AWS CLI API. AWS Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che si sta cercando di eseguire.

La seguente politica consente a un utente di accedere a OpenSearch Ingestion dalla console di servizio: OpenSearch

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ]
        }
    ]
}
```

In alternativa, è possibile utilizzare la policy the section called “AmazonOpenSearchIngestionReadOnlyAccess” AWS gestita, che concede l'accesso in sola lettura a tutte le risorse di Ingestion per un. OpenSearch Account AWS

OpenSearch Amministrazione delle pipeline di Ingestion

Questa policy è un esempio di policy di «pipeline admin» che consente a un utente di gestire e amministrare le pipeline di Amazon OpenSearch Ingestion. L'utente può creare, visualizzare ed eliminare le pipeline.

```
{
    "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"
        }
    ]
}
```

Inserimento di dati in una pipeline di ingestione OpenSearch

Questa policy di esempio consente a un utente o a un'altra entità di inserire dati in una pipeline di Amazon OpenSearch Ingestion nel proprio account. L'utente non può modificare le pipeline.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:Ingest"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Registrazione delle chiamate API OpenSearch di Amazon Ingestion utilizzando AWS CloudTrail

Amazon OpenSearch Ingestion è integrato conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un AWS servizio in OpenSearch Ingestion.

CloudTrailacquisisce tutte le chiamate API per OpenSearch Ingestion come eventi. Le chiamate acquisite includono le chiamate dalla OpenSearch sezione di log e le OpenSearch chiamate di codice alle operazioni API di log alle operazioni API OpenSearch di log.

Se si crea un percorso, è possibile abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per OpenSearch Ingestion. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi).

Le informazioni raccolte da permettono CloudTrail di determinare la richiesta effettuata a OpenSearch Ingestion, l'indirizzo IP da cui è stata effettuata la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, consulta la Guida per l'utente di AWS CloudTrail.

OpenSearchInformazioni sull'ingestione in CloudTrail

CloudTrail è abilitato sull'Account AWS al momento della sua creazione. Quando si verifica un'attività in OpenSearch Ingestione, questa viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi che includa eventi per OpenSearch Ingestion, crea un trail. Account AWS Un trail consente CloudTrail di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS.

Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati

- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni e Ricezione di file di log CloudTrail da più account

Tutte le OpenSearch azioni di importazione vengono registrate CloudTrail e documentate nel riferimento all'API di importazione. OpenSearch Ad esempio, le chiamate alle operazioni `CreateCollection`, `ListCollections` e `DeleteCollection` generano voci nei file di log CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di stabilire:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci OpenSearch di log di log di log di log di log di log

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail contengono una o più voci di log.

Un evento rappresenta una singola richiesta da un'origine. Include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. I file di log di CloudTrail non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione `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"
}
```


Etichettatura delle pipeline di Amazon OpenSearch Ingestion

I tag consentono di assegnare informazioni artibrarie a una pipeline Amazon OpenSearch Ingestion in modo da poter categorizzare e filtrare tali informazioni. Un tag è un'etichetta di metadati assegnata dall'utente o da AWS a una risorsa AWS. Ciascun tag è formato da una chiave e da un valore, Per i tag assegnati da te, puoi definire la chiave e il valore. Ad esempio, potresti definire la chiave come `stage` e il valore di una risorsa come `test`.

I tag consentono di eseguire le seguenti operazioni:

- Identificare e organizzare le risorse AWS. Molti servizi AWS supportano l'assegnazione di tag, perciò è possibile assegnare lo stesso tag a risorse di diversi servizi per indicare che queste sono

correlate. Ad esempio, puoi assegnare a una pipeline di OpenSearch Ingestione lo stesso tag assegnato a un dominio Amazon Service. OpenSearch

- Tenere traccia dei costi AWS. Questi tag vengono attivati nel pannello di controllo AWS Billing and Cost Management. AWS usa i tag per categorizzare i costi e fornire un report di allocazione dei costi mensili. Per ulteriori informazioni, consulta la pagina sull'utilizzo dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing.
- Limita l'accesso alle pipeline utilizzando il controllo degli accessi basato sugli attributi. Per ulteriori informazioni, consulta Controllo dell'accesso in base alle chiavi dei tag delle risorse nella Guida per l'utente IAM.

In OpenSearch Ingestione, la risorsa principale è una pipeline. È possibile utilizzare la console del OpenSearch servizio, la AWS CLI, le API di OpenSearch ingestione o gli AWS SDK per aggiungere, gestire e rimuovere tag da una pipeline.

Argomenti

Autorizzazioni richieste

OpenSearchIngestion utilizza le seguenti autorizzazioni AWS Identity and Access Management Access Analyzer (IAM) per etichettare le pipeline:

- `osis:TagResource`
- `osis:ListTagsForResource`
- `osis:UntagResource`

Per ulteriori informazioni su ogni permesso, consulta Operazioni, risorse e chiavi di condizione per l'OpenSearchinserimento nel Service Authorization Reference.

Utilizzo dei tag (console)

La console è il modo più semplice per assegnare un tag a una pipeline.

Per creare un tag

1. Accedi alla console del OpenSearch servizio Amazon all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegliete Ingestione nel riquadro di navigazione a sinistra.
3. Seleziona la pipeline a cui aggiungere i tag e passa alla scheda Tag.
4. Scegli Gestisci, quindi seleziona Aggiungi nuovo tag.
5. Inserire una chiave di tag e un valore facoltativo.
6. Seleziona Salva.

Per eliminare un tag, esegui la stessa procedura e scegli Rimuovi nella pagina Gestisci tag.

Per ulteriori informazioni sull'utilizzo della console per il funzionamento con i tag, consulta Editor di tag nella Guida alle operazioni di base della Console di gestione AWS.

Utilizzo dei tag (AWS CLI)

Per etichettare una pipeline utilizzando ilAWS CLI, invia una `TagResource` richiesta:

```
aws osis tag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tags Key=service,Value=osis Key=source,Value=otel
```

Rimuovi i tag da una pipeline usando il `UntagResource` comando:

```
aws osis untag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tag-keys service
```

È possibile visualizzare i tag esistenti per una pipeline con il `ListTagsForResource` comando:

```
aws osis list-tags-for-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
```

Registrazione e monitoraggio di Amazon OpenSearch Ingestion con Amazon CloudWatch

Amazon OpenSearch Ingestion pubblica metriche e log su Amazon. CloudWatch

Argomenti

Monaggio aggio aggio aggio aggio aggio aggio aggio aggio

Puoi abilitare la registrazione per le pipeline di Amazon OpenSearch Ingestion per esporre i messaggi di errore e di avviso generati durante le operazioni della pipeline e l'attività di ingestione. OpenSearchIngestion pubblica tutti i log su Amazon Logs. CloudWatch CloudWatchI log possono monitorare le informazioni nei file di log e notificare quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon CloudWatch Logs.

I log di OpenSearch Ingestion potrebbero indicare un'elaborazione non riuscita delle richieste, errori di autenticazione dall'origine al sink e altri avvisi che possono essere utili per la risoluzione dei problemi. Per i suoi log, OpenSearch Ingestion utilizza i livelli di registro di`INFO`,`WARN`, `ERROR` e. `FATAL` Ti consigliamo di abilitare la pubblicazione dei log per tutte le pipeline.

Autorizzazioni richieste

Per abilitare OpenSearch Ingestion per inviare log a CloudWatch Logs, devi essere connesso come un utente che dispone di determinate autorizzazioni IAM.

Sono necessarie le seguenti autorizzazioni CloudWatch Log per creare e aggiornare le risorse di distribuzione dei log:

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

```
                "logs:PutResourcePolicy",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:DescribeResourcePolicies",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries"
            ]
        }
    ]
}
```

Abilitazione aggio aggio aggio aggio

È possibile abilitare la pubblicazione dei log su pipeline esistenti o durante la creazione di una pipeline. Per i passaggi per abilitare la pubblicazione dei log durante la creazione della pipeline, vederethe section called “Creazione di pipeline”.

Console

Come abilitare la pubblicazione di log su una pipeline esistente

1. Accedi alla console di OpenSearch servizio Amazon all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegliete Ingestione nel riquadro di navigazione a sinistra e selezionate la pipeline per cui desiderate abilitare i log.
3. Scegli Modifica le opzioni di pubblicazione del registro.
4. Seleziona Pubblica su CloudWatch registri.
5. Creare un nuovo gruppo di log o selezionane uno esistente. Ti consigliamo di formattare il nome come percorso, ad esempio`/aws/`**`vendedlogs`**`/OpenSearchIngestion/`*`pipeline-name`*`/audit-logs`. Questo formato semplifica l'applicazione di una politica di CloudWatch accesso che concede autorizzazioni a tutti i gruppi di log in un percorso specifico come. `/aws/vendedlogs/OpenSearchService/OpenSearchIngestion`

   > **Important**
   >
   > È necessario includere il prefisso `vendedlogs` nel nome del gruppo di log, altrimenti la creazione non riesce.

6. Seleziona Salva.

CLI

Per abilitare la pubblicazione di log utilizzandoAWS CLI, inviare la seguente richiesta:

```
aws osis update-pipeline \
  --pipeline-name my-pipeline \
  --log-publishing-options  IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="/
aws/vendedlogs/OpenSearchIngestion/pipeline-name"}
```

Monaggio aggio aggio aggio aggio aggio aggio aggio aggio

Puoi monitorare le pipeline di OpenSearch Ingestione utilizzando AmazonCloudWatch, che raccoglie i dati non elaborati e li elabora in parametri leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Guida per CloudWatch l'utente di Amazon.

Nella console OpenSearch Ingestione viene visualizzata una serie di grafici basati sui dati non elaborati della scheda Prestazioni per ciascuna pipeline. CloudWatch

OpenSearchIngestione riporta le metriche della maggior parte dei plugin supportati. Se alcuni plugin non hanno una propria tabella qui sotto, significa che non riportano alcuna metrica specifica del plug-in. Le parametri della pipeline vengono pubblicate nel namespace. `AWS/OSIS`

Argomenti

- Parametri comuni
- Parametri del buffer
- Metriche V4 esclusive
- Metriche limitate del buffer di blocco
- Metriche della fonte di tracciamento Otel
- Metriche di origine delle metriche Otel
- Metriche Http
- Parametri S3
- Parametro Aggregate

- Parametri di data
- Metriche Grok
- Parametri non elaborati
- Parametri Otel Trace Group
- Parametri stateful della mappa servizio
- Parametri OpenSearch
- Parametri di misurazione e di sistema

Parametri comuni

Le seguenti metriche sono comuni a tutti i processori e i sink.

Ogni metrica è preceduta dal nome della sottopipeline e dal nome del plugin, nel formato < sub_pipeline_name >< plugin >< metric_name >. Ad esempio, il nome completo della `recordsIn.count` metrica per una sottopipeline denominata `my-pipeline` e il data processor sarebbero. `my-pipeline.date.recordsIn.count`

Suffisso metrico	Descrizione
`recordsIn.count`	L'ingresso di record in un componente della pipeline. Questa metrica si applica a processori e sink. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`recordsOut.count`	L'uscita di record da un componente della pipeline. Questa metrica si applica a processori e sorgenti. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`timeElapsed.count`	Un numero di punti dati registrati durante l'esecuzione di un componente della pipeline. Questa metrica si applica a processori e sink. Statistiche rilevanti: Sum (Somma)

Suffisso metrico	Descrizione
	Dimensione: `PipelineName`
`timeElapsed.sum`	Il tempo totale trascorso durante l'esecuzione di un componente della pipeline. Questa metrica si applica a processori e pozzi, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`timeElapsed.max`	Il tempo massimo trascorso durante l'esecuzione di un componente della pipeline. Questa metrica si applica a processori e pozzi, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Parametri del buffer

Le seguenti metriche si applicano al buffer di blocco limitato predefinito che OpenSearch Ingestion configura automaticamente per tutte le pipeline.

Ogni metrica è preceduta dal nome della sottopipeline e dal nome del buffer, nel formato < sub_pipeline_name >< buffer_name >< metric_name >. Ad esempio, il nome completo della `recordsWritten.count` metrica per una sottopipeline denominata `my-pipeline` sarebbe. `my-pipeline.BlockingBuffer.recordsWritten.count`

Suffisso metrico	Descrizione
`recordsWritten.count`	Il numero di record scritti in un buffer. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`recordsRead.count`	Il numero di record letti da un buffer.

Suffisso metrico	Descrizione
	Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`recordsInFlight.value`	Il numero di record non controllati letti da un buffer. Statistiche pertinenti: media Dimensione: `PipelineName`
`recordsInBuffer.value`	Il numero di record attualmente in un buffer. Statistiche pertinenti: media Dimensione: `PipelineName`
`recordsProcessed.count`	Il numero di record letti da un buffer ed elaborati da una pipeline. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`recordsWriteFailed.count`	Il numero di record che la pipeline non è riuscita a scrivere nel sink. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`writeTimeElapsed.count`	Un conteggio di punti dati registrati durante la scrittura su un buffer. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`writeTimeElapsed.sum`	Il tempo totale trascorso durante la scrittura su un buffer, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`writeTimeElapsed.max`	Il tempo massimo trascorso durante la scrittura su un buffer, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`
`writeTimeouts.count`	Il conteggio dei timeout di scrittura in un buffer. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`readTimeElapsed.count`	Un conteggio di punti dati registrati durante la lettura da un buffer. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`readTimeElapsed.sum`	Il tempo totale trascorso durante la lettura da un buffer, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`readTimeElapsed.max`	Il tempo massimo trascorso durante la lettura da un buffer, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`checkpointTimeElapsed.count`	Un conteggio dei punti dati registrati durante il checkpoint. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`checkpointTimeElapsed.sum`	Il tempo totale trascorso durante il checkpoint, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`checkpointTimeElapsed.max`	Il tempo massimo trascorso durante il checkpoint, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Metriche V4 esclusive

Le seguenti metriche si applicano all'endpoint di inserimento di una pipeline e sono associate ai plugin di origine (, e). `http` `otel_trace` `otel_metrics` Tutte le richieste all'endpoint di ingestione devono essere firmate utilizzando la versione Signature 4. Queste metriche possono aiutarti a identificare i problemi di autorizzazione durante la connessione alla pipeline o a confermare che l'autenticazione è stata completata correttamente.

Ogni metrica è preceduta dal nome della sottopipeline e. `osis_sigv4_auth` Ad esempio, *`sub_pipeline_name`*`.osis_sigv4_auth.httpAuthSuccess.count`.

Suffisso metrico	Descrizione
`httpAuthSuccess.count`	Il numero di richieste Signature V4 riuscite alla pipeline. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`httpAuthFailure.count`	Il numero di richieste Signature V4 non riuscite alla pipeline. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`httpAuthServerError.count`	Il numero di richieste Signature V4 alla pipeline che hanno restituito errori del server. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Metriche limitate del buffer di blocco

Le seguenti metriche si applicano al buffer di blocco limitato. Ogni metrica è preceduta dal nome della sottopipeline e. `BlockingBuffer` Ad esempio, *`sub_pipeline_name`*`.BlockingBuffer.bufferUsage.value`.

Suffisso metrico	Descrizione
`bufferUsage.value`	Percentuale di utilizzo del in `buffer_size` base al numero di record nel buffer. `buffer_size` rappresenta il numero massimo di registrazioni scritte nel buffer e di registrazioni in volo che non sono state controllate. Statistiche pertinenti: media Dimensione: `PipelineName`

Metriche della fonte di tracciamento Otel

Le seguenti metriche si applicano alla sorgente di traccia OtEL. Ogni metrica è preceduta dal nome della sottopipeline e. `otel_trace_source` Ad esempio, *`sub_pipeline_name`*`.otel_trace_source.requestTimeouts.count`.

Suffisso metrico	Descrizione
`requestTimeouts.count`	Il numero di richieste andate in timeout. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestsReceived.count`	Il numero di richieste ricevute dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`successRequests.count`	Il numero di richieste che sono state elaborate con successo dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`badRequests.count`	Il numero di richieste con un formato non valido che sono state elaborate dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestsTooLarge.count`	Il numero di richieste il cui numero di spazi nel contenuto è maggiore della capacità del buffer. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`internalServerError.count`	Il numero di richieste elaborate dal plugin con un tipo di eccezione personalizzato. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`requestProcessDuration.count`	Un numero di punti dati registrati durante l'elaborazione delle richieste del plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestProcessDuration.sum`	La latenza totale delle richieste elaborate dal plugin, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestProcessDuration.max`	La latenza massima delle richieste elaborate dal plugin, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`
`payloadSize.count`	Conteggio della distribuzione delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`payloadSize.sum`	La distribuzione totale delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`payloadSize.max`	La distribuzione massima delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Metriche di origine delle metriche Otel

Le parametri seguenti si applicano alla fonte di parametri Otel. Ogni metrica è preceduta dal nome della sottopipeline e. `otel_metrics_source` Ad esempio, *`sub_pipeline_name`*`.otel_metrics_source.requestTimeouts.count`.

Suffisso metrico	Descrizione
`requestTimeouts.count`	Il numero di richieste al plugin andate in timeout. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestsReceived.count`	Il numero di richieste ricevute dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`successRequests.count`	Il numero di richieste elaborate con successo (200 codice di stato della risposta) dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestProcessDuration.count`	Un conteggio della latenza delle richieste elaborate dal plugin, in secondi. Statistiche rilevanti: Sum (Somma)

Suffisso metrico	Descrizione
	Dimensione: `PipelineName`
`requestProcessDuration.sum`	La latenza totale delle richieste elaborate dal plugin, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestProcessDuration.max`	La latenza massima delle richieste elaborate dal plugin, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`
`payloadSize.count`	Conteggio della distribuzione delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`payloadSize.sum`	La distribuzione totale delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`payloadSize.max`	La distribuzione massima delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Metriche Http

Le seguenti metriche si applicano alla sorgente HTTP. Ogni metrica è preceduta dal nome della sottopipeline e. `http` Ad esempio, *`sub_pipeline_name`*`.http.requestsReceived.count`.

Suffisso metrico	Descrizione
`requestsReceived.count`	Il numero di richieste ricevute dall'`/log/ingest` endpoint. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestsRejected.count`	Il numero di richieste rifiutate (429 codice di stato della risposta) dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`successRequests.count`	Il numero di richieste elaborate con successo (200 codice di stato della risposta) dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`badRequests.count`	Il numero di richieste con tipo o formato di contenuto non valido (codice di stato della risposta 400) elaborate dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestTimeouts.count`	Il numero di richieste che scadono nel server di origine HTTP (codice di stato della risposta 415). Statistiche rilevanti: Sum (Somma)

Suffisso metrico	Descrizione
	Dimensione: `PipelineName`
`requestsTooLarge.count`	Il numero di richieste la cui dimensione degli eventi nel contenuto è superiore alla capacità del buffer (codice di stato della risposta 413). Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`internalServerError.count`	Il numero di richieste elaborate dal plugin con un tipo di eccezione personalizzato (codice di stato della risposta 500). Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestProcessDuration.count`	Un conteggio della latenza delle richieste elaborate dal plugin, in secondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestProcessDuration.sum`	La latenza totale delle richieste elaborate dal plugin, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`requestProcessDuration.max`	La latenza massima delle richieste elaborate dal plugin, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`payloadSize.count`	Conteggio della distribuzione delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`payloadSize.sum`	La distribuzione totale delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`payloadSize.max`	La distribuzione massima delle dimensioni del payload delle richieste in entrata, in byte. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Parametri S3

Le seguenti metriche si applicano alla fonte S3. Ogni metrica è preceduta dal nome della sottopipeline e. `s3` Ad esempio, *`sub_pipeline_name`*`.s3.s3ObjectsFailed.count`.

Suffisso metrico	Descrizione
`s3ObjectsFailed.count`	Il numero di oggetti S3 che il plugin non è riuscito a leggere. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectsNotFound.count`	Il numero di oggetti S3 che il plugin non è riuscito a leggere a causa di un `Not Found` errore di S3. Queste

Suffisso metrico	Descrizione
	metriche contano anche ai fini della `s3ObjectsFailed` metrica. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectsAccessDenied.count`	Il numero di oggetti S3 che il plugin non è riuscito a leggere a causa di un `Forbidden` errore `Access Denied` o di S3. Queste metriche contano anche ai fini della `s3ObjectsFailed` metrica. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectReadTimeElapsed.count`	Il tempo impiegato dal plugin per eseguire una richiesta GET per un oggetto S3, analizzarlo e scrivere eventi nel buffer. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectReadTimeElapsed.sum`	Il tempo totale impiegato dal plugin per eseguire una richiesta GET per un oggetto S3, analizzarlo e scrivere eventi nel buffer, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectReadTimeElapsed.max`	Il tempo massimo impiegato dal plugin per eseguire una richiesta GET per un oggetto S3, analizzarlo e scrivere eventi nel buffer, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`s3ObjectSizeBytes.count`	Il conteggio della distribuzione delle dimensioni degli oggetti S3, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectSizeBytes.sum`	La distribuzione totale delle dimensioni degli oggetti S3, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectSizeBytes.max`	La distribuzione massima delle dimensioni degli oggetti S3, in byte. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`
`s3ObjectProcessedBytes.count`	Il numero della distribuzione degli oggetti S3 elaborati dal plugin, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectProcessedBytes.sum`	La distribuzione totale degli oggetti S3 elaborati dal plugin, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`s3ObjectProcessedBytes.max`	La distribuzione massima degli oggetti S3 elaborati dal plugin, in byte. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`
`s3ObjectsEvents.count`	Il conteggio della distribuzione degli eventi S3 ricevuti dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectsEvents.sum`	La distribuzione totale degli eventi S3 ricevuti dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3ObjectsEvents.max`	La distribuzione massima degli eventi S3 ricevuti dal plugin. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`
`sqsMessageDelay.count`	Un conteggio dei punti dati registrati mentre S3 registra l'ora di un evento dalla creazione di un oggetto a quando è completamente analizzato. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`sqsMessageDelay.sum`	Il tempo totale che intercorre tra il momento in cui S3 registra un evento per la creazione di un oggetto e il momento in cui viene analizzato completamente, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`sqsMessageDelay.max`	Il periodo di tempo massimo che intercorre tra il momento in cui S3 registra un evento per la creazione di un oggetto e il momento in cui viene analizzato completamente, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`
`s3ObjectsSucceeded.count`	Il numero di oggetti S3 letti con successo dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`sqsMessagesReceived.count`	Il numero di messaggi Amazon SQS ricevuti dalla coda dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`sqsMessagesDeleted.count`	Il numero di messaggi Amazon SQS eliminati dalla coda dal plugin. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`sqsMessagesFailed.count`	Il numero di messaggi Amazon SQS che il plugin non è riuscito ad analizzare. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Parametro Aggregate

Le seguenti metriche si applicano al processore Aggregate. Ogni metrica è preceduta dal nome della sottopipeline e. `aggregate` Ad esempio, *`sub_pipeline_name`*`.aggregate.actionHandleEventsOut.count`.

Suffisso metrico	Descrizione
`actionHandleEvents Out.count`	Il numero di eventi che sono stati restituiti dalla `handleEvent` chiamata all'azione configurata. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`actionHandleEvents Dropped.count`	Il numero di eventi che sono stati restituiti dalla `handleEvent` chiamata all'azione configurata. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`actionHandleEvents ProcessingErrors.count`	Il numero di chiamate effettuate `handleEvent` per l'azione configurata che ha provocato un errore. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`actionConcludeGrou pEventsOut.count`	Il numero di eventi che sono stati restituiti dalla `concludeGroup` chiamata all'azione configurata.

Suffisso metrico	Descrizione
	Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`actionConcludeGroupEventsDropped.count`	Il numero di eventi che non sono stati restituiti dalla `condludeGroup` chiamata all'azione configurata. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`actionConcludeGroupEventsProcessingErrors.count`	Il numero di chiamate effettuate `concludeGroup` per l'azione configurata che ha provocato un errore. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`currentAggregateGroups.value`	Il numero di gruppi. Questo indicatore diminuisce quando i gruppi vengono conclusi e aumenta quando un evento avvia la creazione di un nuovo gruppo. Statistiche pertinenti: media Dimensione: `PipelineName`

Parametri di data

Le seguenti metriche si applicano al Data processor. Ogni metrica è preceduta dal nome della sottopipeline e. `date` Ad esempio, *`sub_pipeline_name`*`.date.dateProcessingMatchSuccess.count`.

Suffisso metrico	Descrizione
`dateProcessingMatchSuccess.count`	Il numero di record che corrispondono ad almeno uno dei modelli specificati nell'opzione `match` di configurazione. Statistiche rilevanti: Sum (Somma)

Suffisso metrico	Descrizione
	Dimensione: `PipelineName`
`dateProcessingMatchFailure.count`	Il numero di record che non corrispondono a nessuno dei modelli specificati nell'opzione `match` di configurazione. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Metriche Grok

Le seguenti metriche si applicano al processore Grok. Ogni metrica è preceduta dal nome della sottopipeline e. `grok` Ad esempio, *`sub_pipeline_name`*`.grok.grokProcessingMatch.count`.

Suffisso metrico	Descrizione
`grokProcessingMatch.count`	Il numero di record che hanno trovato almeno un pattern corrisponde all'opzione `match` di configurazione. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`grokProcessingMismatch.count`	Il numero di record che non corrispondono a nessuno dei modelli specificati nell'opzione `match` di configurazione. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`grokProcessingErrors.count`	Il numero di errori di elaborazione dei record. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`grokProcessingTimeouts.count`	Il numero di record scaduti durante la corrispondenza. Statistiche rilevanti: Sum (Somma)

Suffisso metrico	Descrizione
	Dimensione: `PipelineName`
`grokProcessingTime.count`	Un conteggio dei punti dati registrati mentre un singolo record è stato confrontato con i modelli dell'opzione `match` di configurazione. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`grokProcessingTime.sum`	Il tempo totale impiegato da ogni singolo record per confrontarsi con i modelli dell'opzione di `match` configura zione, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`grokProcessingTime.max`	Il tempo massimo impiegato da ogni singolo record per confrontarsi con i modelli dell'opzione di `match` configura zione, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Parametri non elaborati

Le seguenti metriche si applicano al processore di tracciamento raw OtEL. Ogni metrica è preceduta dal nome della sottopipeline e. `otel_trace_raw` Ad esempio, *`sub_pipeline_name`*`.otel_trace_raw.traceGroupCacheCount.value`.

Suffisso metrico	Descrizione
`traceGroupCacheCou nt.value`	Il numero di gruppi di tracce nella cache dei gruppi di traccia. Statistiche rilevanti: Sum (Somma)

Suffisso metrico	Descrizione
	Dimensione: `PipelineName`
`spanSetCount.value`	Il numero di set di span nella raccolta di span set. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Parametri Otel Trace Group

Le seguenti metriche si applicano al processore del gruppo di tracce OtEL. Ogni metrica è preceduta dal nome della sottopipeline e. `otel_trace_group` Ad esempio, *`sub_pipeline_name`*`.otel_trace_group.recordsInMissingTraceGroup.count`.

Suffisso metrico	Descrizione
`recordsInMissingTraceGroup.count`	Il numero di record in ingresso in cui mancano i campi del gruppo di tracce. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`recordsOutFixedTraceGroup.count`	Il numero di record in uscita con campi del gruppo di tracce che sono stati compilati correttamente. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`recordsOutMissingTraceGroup.count`	Il numero di record in uscita mancanti nei campi del gruppo di tracce. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Parametri stateful della mappa servizio

Le seguenti metriche si applicano al processore stateful di Service-map. Ogni metrica è preceduta dal nome della sottopipeline e. `service-map-stateful` Ad esempio, *`sub_pipeline_name`*`.service-map-stateful.spansDbSize.count`.

Suffisso metrico	Descrizione
`spansDbSize.value`	Le dimensioni in byte in memoria delle estensioni in MapDB tra la durata della finestra corrente e quella precedente. Statistiche pertinenti: media Dimensione: `PipelineName`
`traceGroupDbSize.value`	Le dimensioni dei byte in memoria dei gruppi di tracce in MapDB nella durata attuale e precedente della finestra. Statistiche pertinenti: media Dimensione: `PipelineName`
`spansDbCount.value`	Il numero di intervalli in MapDB tra la durata della finestra corrente e quella precedente. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`traceGroupDbCount.value`	Il numero di gruppi di tracce in MapDB nella durata della finestra corrente e precedente. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`relationshipCount.value`	Il numero di relazioni memorizzate nella durata della finestra corrente e precedente. Statistiche rilevanti: Sum (Somma)

Suffisso metrico	Descrizione
	Dimensione: `PipelineName`

Parametri OpenSearch

Le seguenti metriche si applicano al OpenSearchlavandino. Ogni metrica è preceduta dal nome della sottopipeline e. `opensearch` Ad esempio, *`sub_pipeline_name`*`.opensearch.bulkRequestErrors.count`.

Suffisso metrico	Descrizione
`bulkRequestErrors.count`	Il numero totale di errori riscontrati durante l'invio di richieste in blocco. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`documentsSuccess.count`	Il numero di documenti inviati correttamente al OpenSearch Servizio tramite richiesta in blocco, compresi i nuovi tentativi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`documentsSuccessFirstAttempt.count`	Il numero di documenti inviati correttamente al OpenSearch Servizio tramite richiesta in blocco al primo tentativo. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`documentErrors.count`	Il numero di documenti che non sono stati inviati tramite richieste in blocco. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`bulkRequestFailed.count`	Il numero di richieste di massa non riuscite. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestNumberOfRetries.count`	Il numero di tentativi di richieste di massa non riuscite. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkBadRequestErrors.count`	Il numero di `Bad Request` errori riscontrati durante l'invio di richieste in blocco. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestNotAllowedErrors.count`	Il numero di `Request Not Allowed` errori riscontrati durante l'invio di richieste in blocco. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestInvalidInputErrors.count`	Il numero di `Invalid Input` errori riscontrati durante l'invio di richieste in blocco. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestNotFoundErrors.count`	Il numero di `Request Not Found` errori riscontrati durante l'invio di richieste in blocco. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`bulkRequestTimeoutErrors.count`	Il numero di `Request Timeout` errori riscontrati durante l'invio di richieste in blocco. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestServerErrors.count`	Il numero di `Server Error` errori riscontrati durante l'invio di richieste in blocco. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestSizeBytes.count`	Conteggio della distribuzione delle dimensioni del payload delle richieste in blocco, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestSizeBytes.sum`	La distribuzione totale delle dimensioni del payload delle richieste in blocco, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestSizeBytes.max`	La distribuzione massima delle dimensioni del payload delle richieste in blocco, in byte. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`bulkRequestLatency.count`	Un numero di punti dati registrati durante l'invio delle richieste al plug-in, inclusi i nuovi tentativi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestLatency.sum`	La latenza totale delle richieste inviate al plugin, inclusi i nuovi tentativi, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`bulkRequestLatency.max`	La latenza massima delle richieste inviate al plugin, inclusi i nuovi tentativi, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`
`s3.dlqS3RecordsSuccess.count`	Il numero di record inviati con successo alla coda delle lettere morte S3. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3.dlqS3RecordsFailed.count`	Il numero di record che non sono stati inviati alla coda delle lettere morte S3. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`s3.dlqS3RequestSuccess.count`	Il numero di richieste andate a buon fine alla coda delle lettere morte S3. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3.dlqS3RequestFailed.count`	Il numero di richieste non riuscite alla coda delle lettere morte S3. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3.dlqS3RequestLatency.count`	Numero di punti dati registrati durante l'invio delle richieste alla coda delle lettere morte di S3, compresi i nuovi tentativi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3.dlqS3RequestLatency.sum`	La latenza totale delle richieste inviate alla coda delle lettere morte di S3, inclusi i nuovi tentativi, in millisecondi. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3.dlqS3RequestLatency.max`	La latenza massima delle richieste inviate alla coda delle lettere morte di S3, compresi i nuovi tentativi, in millisecondi. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Suffisso metrico	Descrizione
`s3.dlqS3RequestSizeBytes.count`	Conteggio della distribuzione delle dimensioni del payload delle richieste alla coda di lettere morte di S3, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3.dlqS3RequestSizeBytes.sum`	La distribuzione totale delle dimensioni del payload delle richieste alla coda di lettere morte S3, in byte. Statistiche rilevanti: Sum (Somma) Dimensione: `PipelineName`
`s3.dlqS3RequestSizeBytes.max`	La distribuzione massima delle dimensioni del payload delle richieste alla coda di lettere morte S3, in byte. Statistiche rilevanti: Max (Massimo) Dimensione: `PipelineName`

Parametri di misurazione e di sistema

I parametri seguenti si applicano all'intero sistema di OpenSearch ingaggio. Queste metriche non sono precedute da nulla.

Parametro	Descrizione
`system.cpu.usage.value`	La percentuale di utilizzo della CPU disponibile per tutti i nodi di dati. Statistiche pertinenti: media Dimensione:`PipelineName` ,`area`, `id`
`system.cpu.count.value`	La quantità totale di utilizzo della CPU per tutti i nodi di dati.

Parametro	Descrizione
	Statistiche pertinenti: media Dimensione:`PipelineName ,area, id`
`jvm.memory.max.value`	La quantità di memoria che può essere utilizzata per la gestione della memoria, in byte. Statistiche pertinenti: media Dimensione:`PipelineName ,area, id`
`jvm.memory.used.value`	La quantità di memoria utilizzata, in byte. Statistiche pertinenti: media Dimensione: `PipelineName area, id` signa
`jvm.memory.committ ed.value`	La quantità di memoria che viene impegnata per l'utilizzo da parte della Java Virtual Machine (JVM), in byte. Statistiche pertinenti: media Dimensione:`PipelineName ,area, id`
`computeUnits`	Il numero di Ingestion OpenSearch Compute Unit (Ingestio n OCU) utilizzate da una pipeline. Statistiche pertinenti: Max, Sum, Average Dimensione: `PipelineName`

Le migliori pratiche per Amazon OpenSearch Ingestion

Questo argomento fornisce le best practice per la creazione e la gestione delle pipeline di Amazon OpenSearch Ingestion e include linee guida generali che si applicano a molti casi d'uso. Ogni carico di lavoro è unico, con caratteristiche uniche, quindi nessun suggerimento generico è adatto per ogni caso d'uso.

Argomenti

Best practice generali

Le seguenti best practice generali si applicano alla creazione e alla gestione di pipeline.

- Per garantire un'elevata disponibilità, configura le pipeline VPC con due o tre sottoreti. Se distribuisci una pipeline solo in una sottorete e la zona di disponibilità non funziona, non sarai in grado di importare dati.
- All'interno di ogni pipeline, consigliamo di limitare il numero di sotto-pipeline a 5 o meno.
- Se utilizzi il plug-in sorgente S3, utilizza file S3 di dimensioni uniformi per prestazioni ottimali.
- Se utilizzi il plug-in sorgente S3, aggiungi 30 secondi di timeout di visibilità aggiuntivo per ogni 0,25 GB di dimensione del file nel bucket S3 per prestazioni ottimali.
- Includi una dead-letter queue (DLQ) nella configurazione della pipeline in modo da poter scaricare gli eventi non riusciti e renderli accessibili per l'analisi. Se i tuoi sink rifiutano i dati a causa di mappature errate o altri problemi, puoi indirizzare i dati al DLQ per risolvere il problema e risolverlo.

Allarmi consigliati CloudWatch

CloudWatch gli allarmi eseguono un'azione quando una CloudWatch metrica supera un valore specificato per un certo periodo di tempo. Ad esempio, potrebbe essere opportuno ricevere da AWS un'e-mail se lo stato del cluster è `red` per più di un minuto. Questa sezione include alcuni allarmi consigliati per Amazon OpenSearch Ingestion e come rispondere ad essi.

Per ulteriori informazioni sulla configurazione degli allarmi, consulta Creating Amazon CloudWatch Alarms nella Amazon CloudWatch User Guide.

Allarme	Problema
`computeUnits` il massimo è = quello configurato `maxUnits` per 15 minuti, 3 volte consecutive	La pipeline ha raggiunto la capacità massima e potrebbe richiedere un `maxUnits` aggiornamento. Aumenta la capacità massima della tua pipeline

Allarme	Problema
`opensearch.documentErrors.count` sum is = *{sub_pipeline_name}* `.opensearch.recordsIn.count` somma per 1 minuto, 1 volta consecutiva	La pipeline non è in grado di scrivere nel OpenSearch sink. Controlla le autorizzazioni della pipeline e conferma che il dominio o la raccolta siano integri. Puoi anche controllare la presenza di eventi non riusciti nella coda delle lettere morte (DLQ), se è configurata.
`bulkRequestLatency.max` max è >= x per 1 minuto, 1 volta consecutiva	La pipeline presenta un'elevata latenza nell'invio dei dati al sink. OpenSearch Ciò è probabilmente dovuto al fatto che il sink è sottodimensionato o a una strategia di sharding inadeguata, che sta facendo sì che il sink rimanga indietro. Una latenza elevata e sostenuta può influire sulle prestazioni della pipeline e probabilmente portare a una contropressione sui client.
`httpAuthFailure.count` somma >= 1 per 1 minuto, 1 volta consecutiva	Le richieste di ingestione non vengono autenticate. Verifica che l'autenticazione Signature Version 4 sia abilitata correttamente per tutti i client.
`system.cpu.usage.value` media >= 80% per 15 minuti, 3 volte consecutive	Un utilizzo elevato e prolungato della CPU può essere problematico. Valuta la possibilità di aumentare la capacità massima della pipeline.
`bufferUsage.value` media >= 80% per 15 minuti, 3 volte consecutive	Un utilizzo prolungato e elevato del buffer può essere problematico. Valuta la possibilità di aumentare la capacità massima della pipeline.

Altri allarmi che potresti prendere in considerazione

Valuta la possibilità di configurare i seguenti allarmi a seconda delle funzionalità di Amazon OpenSearch Ingestion che utilizzi regolarmente.

Allarme	Problema
`dynamodb.exportJobFailure.count` somma 1	Il tentativo di attivare un'esportazione in Amazon S3 non è riuscito.
`opensearch.EndtoEndLatency.avg` media > X per 15 minuti, 4 volte consecutive	`EndtoEndLatency` È superiore a quello desiderato per la lettura da flussi DynamoDB. Ciò potrebbe essere causato da un OpenSearch cluster sottodimensionato o da una capacità OCU massima della pipeline troppo bassa per il throughput WCU sulla tabella DynamoDB. `EndtoEndLatency` sarà più alto dopo un'esportazione, ma dovrebbe diminuire nel tempo man mano che raggiunge gli ultimi stream DynamoDB.
`dyanmodb.changeEventsProcessed.count` somma == 0 per X minuti	Nessun record viene raccolto dai flussi DynamoDB. Ciò potrebbe essere causato dall'assenza di attività sulla tabella o da un problema di accesso ai flussi DynamoDB.
`opensearch.s3.dlqS3RecordsSuccess.count` somma >= `opensearch.documentSuccess.count` somma per 1 minuto, 1 volta consecutiva	Al DLQ viene inviato un numero maggiore di record rispetto al OpenSearch sink. Esamina le metriche del plug-in OpenSearch sink per indagare e determinare la causa principale.

Allarme	Problema
`grok.grok Processin gTimeouts .count` sum = RecordsIn.count somma per 1 minuto, 5 volte consecutive	Il timeout di tutti i dati si verifica mentre il processore Grok tenta di creare una corrispondenza tra i modelli. È probabile che ciò influisca sulle prestazioni e rallenti la pipeline. Valuta la possibilità di modificare i tuoi schemi per ridurre i timeout.
`grok.grok Processin gErrors.count` la somma è >= 1 per 1 minuto, 1 volta consecutiva	Il processore Grok non riesce ad abbinare i modelli ai dati nella pipeline, con conseguenti errori. Rivedi i dati e le configurazioni del plug-in Grok per assicurarti che sia prevista la corrispondenza dei modelli.
`grok.grok Processin gMismatch .count` sum = RecordsIn.count somma per 1 minuto, 5 volte consecutive	Il processore Grok non è in grado di abbinare i modelli ai dati nella pipeline. Rivedi i dati e le configurazioni del plug-in Grok per assicurarti che sia prevista la corrispondenza dei modelli.
`date.date Processin gMatchFai lure.count` sum = RecordsIn.count = somma per 1 minuto, 5 volte consecutive	Il processore Date non è in grado di abbinare alcun modello ai dati nella pipeline. Controlla le configurazioni dei dati e del plug-in Date per assicurarti che il modello sia previsto.

Allarme	Problema
`s3.s3ObjectsFailed.count` somma >= 1 per 1 minuto, 1 volta consecutiva	Questo problema si verifica perché l'oggetto S3 non esiste o la pipeline non dispone di privilegi sufficienti. Esamina le `s3ObjectsAccessDenied.count` metriche `s3ObjectsNotFound.count` and per determinare la causa principale. Verifica che l'oggetto S3 esista e/o aggiorna le autorizzazioni.
`s3.sqsMessagesFailed.count` somma >= 1 per 1 minuto, 1 volta consecutiva	Il plug-in S3 non è riuscito a elaborare un messaggio Amazon SQS. Se hai un DLQ abilitato sulla coda SQS, esamina il messaggio di errore. La coda potrebbe ricevere dati non validi che la pipeline sta tentando di elaborare.
`http.badRequests.count` somma >= 1 per 1 minuto, 1 volte consecutive	Il client sta inviando una richiesta errata. Verifica che tutti i client stiano inviando il payload corretto.
`http.requestsTooLarge.count` somma >= 1 per 1 minuto, 1 volta consecutiva	Le richieste provenienti dal plugin sorgente HTTP contengono troppi dati, il che supera la capacità del buffer. Regola la dimensione del batch per i tuoi clienti.
`http.internalServerError.count` somma >= 0 per 1 minuto, 1 volta consecutiva	Il plugin di origine HTTP non riesce a ricevere gli eventi.

Allarme	Problema
`http.requestTimeouts.count` somma >= 0 per 1 minuto, 1 volta consecutiva	I timeout di origine sono probabilmente il risultato di un approvvigionamento insufficiente della pipeline. Valuta la possibilità di aumentare la pipeline `maxUnits` per gestire un carico di lavoro aggiuntivo.
`otel_trace.badRequests.count` somma >= 1 per 1 minuto, 1 volta consecutiva	Il client sta inviando una richiesta errata. Verifica che tutti i client stiano inviando il payload corretto.
`otel_trace.requestsTooLarge.count` somma >= 1 per 1 minuto, 1 volta consecutiva	Le richieste provenienti dal plugin sorgente di Otel Trace contengono troppi dati, il che supera la capacità del buffer. Regola la dimensione del batch per i tuoi clienti.
`otel_trace.internalServerError.count` somma >= 0 per 1 minuto, 1 volta consecutiva	Il plugin sorgente di Otel Trace non riesce a ricevere gli eventi.
`otel_trace.requestTimeouts.count` somma >= 0 per 1 minuto, 1 volta consecutiva	I timeout di origine sono probabilmente il risultato di un approvvigionamento insufficiente della pipeline. Valuta la possibilità di aumentare la pipeline `maxUnits` per gestire un carico di lavoro aggiuntivo.

Allarme	Problema
`otel_metrics.requestTimeouts.count` somma >= 0 per 1 minuto, 1 volta consecutiva	I timeout di origine sono probabilmente il risultato di un approvvigionamento insufficiente della pipeline. Valuta la possibilità di aumentare la pipeline `maxUnits` per gestire un carico di lavoro aggiuntivo.

Amazon OpenSearch Serverless

Amazon OpenSearch Serverless è una configurazione on-demand con scalabilità automatica per Amazon Service. OpenSearch Una raccolta OpenSearch Serverless è un OpenSearch cluster che ridimensiona la capacità di calcolo in base alle esigenze dell'applicazione. Ciò contrasta con i OpenSearch domini OpenSearch Service Provisioned, per i quali la capacità viene gestita manualmente.

OpenSearch Serverless offre un'opzione semplice ed economica per carichi di lavoro poco frequenti, intermittenti o imprevedibili. È vantaggiosa a livello di costi perché dimensiona automaticamente la capacità di calcolo in base all'uso dell'applicazione.

OpenSearch Le raccolte serverless hanno lo stesso tipo di volume di storage ad alta capacità, distribuito e ad alta disponibilità utilizzato dai domini di servizio forniti. OpenSearch

OpenSearch Le raccolte serverless sono sempre crittografate. Puoi scegliere la chiave di crittografia, ma non puoi disabilitare la crittografia. Per ulteriori informazioni, consulta the section called “Crittografia”.

Argomenti

Vantaggi

OpenSearch Serverless offre i seguenti vantaggi:

- Più semplice del provisioning: OpenSearch Serverless elimina gran parte della complessità della gestione OpenSearch dei cluster e della capacità. Dimensiona e ottimizza automaticamente i cluster e si occupa della gestione del ciclo di vita delle partizioni e degli indici. Gestisce inoltre gli aggiornamenti del software di servizio e gli upgrade delle versioni. OpenSearch Tutti gli aggiornamenti e gli upgrade non comportano interruzioni.
- Conveniente: quando utilizzi OpenSearch Serverless, paghi solo per le risorse che consumi. Ciò elimina la necessità di un provisioning anticipato e di un overprovisioning per gestire i picchi dei carichi di lavoro.
- Alta disponibilità: OpenSearch Serverless supporta i carichi di lavoro di produzione con ridondanza per proteggere dalle interruzioni della Availability Zone e dai guasti dell'infrastruttura.
- Scalabile: OpenSearch Serverless ridimensiona automaticamente le risorse per mantenere tassi di ingestione dei dati e tempi di risposta alle query costantemente elevati.

Cos'è Amazon OpenSearch Serverless?

Amazon OpenSearch Serverless è una configurazione serverless su richiesta per Amazon Service. OpenSearch Serverless rimuove le complessità operative legate al provisioning, alla configurazione e all'ottimizzazione dei cluster. OpenSearch È una buona opzione per le organizzazioni che non vogliono gestire autonomamente i propri OpenSearch cluster o per le organizzazioni che non dispongono delle risorse o delle competenze dedicate per gestire cluster di grandi dimensioni. Con OpenSearch Serverless, puoi cercare e analizzare facilmente un grande volume di dati senza doverti preoccupare dell'infrastruttura sottostante e della gestione dei dati.

Una raccolta OpenSearch Serverless è un gruppo di OpenSearch indici che interagiscono per supportare un carico di lavoro o un caso d'uso specifici. Le raccolte sono più facili da usare rispetto ai OpenSearch cluster autogestiti, che richiedono il provisioning manuale.

Le raccolte hanno lo stesso tipo di volume di storage ad alta capacità, distribuito e ad alta disponibilità utilizzato dai domini di OpenSearch servizio assegnati, ma eliminano una maggiore complessità perché non richiedono configurazione e ottimizzazione manuali. I dati vengono crittografati in transito all'interno di una raccolta. OpenSearch Serverless supporta anche OpenSearch Dashboards, che forniscono un'interfaccia intuitiva per l'analisi dei dati.

Le raccolte serverless attualmente eseguono la versione 2.0.x. OpenSearch Man mano che vengono rilasciate nuove versioni, OpenSearch Serverless aggiornerà automaticamente le tue raccolte per utilizzare nuove funzionalità, correzioni di bug e miglioramenti delle prestazioni.

Argomenti

Casi d'uso per Serverless OpenSearch

OpenSearch Serverless supporta due casi d'uso principali:

- Analisi dei log: l'opzione dell'analisi dei log si concentra sull'analisi di grandi volumi di dati di serie temporali semistrutturati generati da macchine per approfondimenti sull'aspetto operativo e sul comportamento degli utenti.
- Ricerca full-text: l'opzione della ricerca full-text supporta le applicazioni nelle reti interne (ad esempio, per i sistemi di gestione dei contenuti, i documenti legali, ecc.) e le applicazioni connesse a Internet (ad esempio, per la ricerca di contenuti nei siti di e-commerce).

Quando crei una raccolta, scegli uno di questi casi d'uso. Per ulteriori informazioni, consulta the section called “Scelta di un tipo di raccolta”.

Nozioni di base

Per iniziare a usare OpenSearch Serverless, crea una o più raccolte utilizzando la console di OpenSearch servizio AWS CLI, o uno degli AWS SDK. Per un tutorial sulla creazione rapida di una raccolta, consulta la sezione the section called “Guida introduttiva a Serverless OpenSearch ”.

OpenSearch Serverless supporta le stesse operazioni API di acquisizione e interrogazione della suite OpenSearch open source, così puoi continuare a utilizzare i client e le applicazioni esistenti. I tuoi client devono essere compatibili con OpenSearch 2.x per poter funzionare con Serverless. OpenSearch Per ulteriori informazioni, consulta the section called “Importazione dei dati nelle raccolte”.

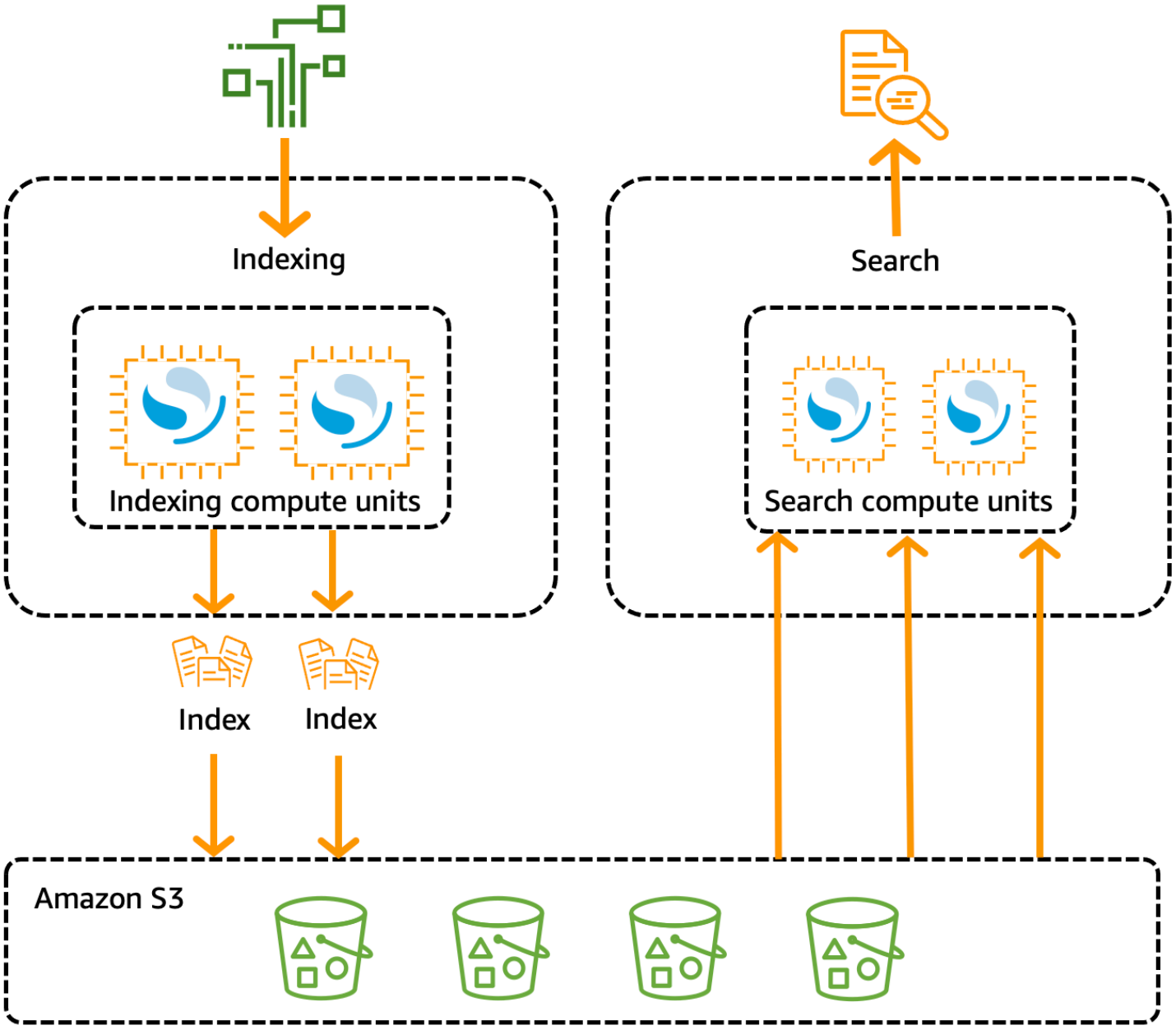
Come funziona

OpenSearch I cluster tradizionali dispongono di un unico set di istanze che eseguono sia operazioni di indicizzazione che di ricerca e lo storage degli indici è strettamente associato alla capacità di elaborazione. Al contrario, OpenSearch Serverless utilizza un'architettura nativa del cloud che separa i componenti di indicizzazione (inserimento) dai componenti di ricerca (query), con Amazon S3 come storage di dati principale per gli indici.

Questa architettura disaccoppiata consente di scalare le funzioni di ricerca e indicizzazione indipendentemente l'una dall'altra, e indipendentemente dai dati indicizzati in S3. Inoltre, l'architettura fornisce l'isolamento per le operazioni di importazione e interrogazione in modo che possano essere eseguite contemporaneamente, senza conflitti tra le risorse.

Quando scrivi dati su una raccolta, Serverless li distribuisce alle unità di calcolo di indicizzazione. OpenSearch Le unità di calcolo di indicizzazione importano i dati in entrata e spostano gli indici su S3. Quando si esegue una ricerca sui dati della raccolta, OpenSearch Serverless indirizza le richieste alle unità di calcolo di ricerca che contengono i dati interrogati. Le unità di calcolo di ricerca scaricano i dati indicizzati direttamente da S3 (se non sono già memorizzati nella cache locale), eseguono operazioni di ricerca ed effettuano aggregazioni.

L'immagine seguente illustra questa architettura disaccoppiata:



OpenSearch La capacità di elaborazione serverless per l'inserimento, la ricerca e l'interrogazione dei dati viene misurata in unità di calcolo (OCU). OpenSearch Ogni OCU è una combinazione di 6 GiB di memoria e della CPU virtuale (vCPU) corrispondente, oltre al trasferimento dei dati su Amazon S3. Ogni OCU include una memoria temporanea a caldo sufficiente per 120 GiB di dati di indice.

Quando crei la tua prima raccolta, OpenSearch Serverless crea un'istanza di due OCU, una per l'indicizzazione e una per la ricerca. Inoltre, avvia anche un set di nodi in standby in un'altra Zona di disponibilità per garantire un'elevata disponibilità. Per scopi di sviluppo e test, è possibile disabilitare l'impostazione Enable redondancy per una raccolta, che elimina le due repliche in standby e crea

solo un'istanza di due OCU. Per impostazione predefinita, le repliche attive ridondanti sono abilitate, il che significa che vengono istanziate un totale di quattro OCU per la prima raccolta in un account.

Queste OCU persistono anche quando non c'è attività su un endpoint di raccolta. Tutte le raccolte successive condividono queste OCU. Quando si creano raccolte aggiuntive nello stesso account, OpenSearch Serverless aggiunge ulteriori OCU per la ricerca e l'inserimento solo se necessario per supportare le raccolte, in base ai limiti di capacità specificati. La capacità si riduce man mano che l'utilizzo dell'elaborazione diminuisce.

Per informazioni sulla fatturazione di queste OCU, consulta la sezione the section called “Prezzi OpenSearch per Serverless”.

Scelta di un tipo di raccolta

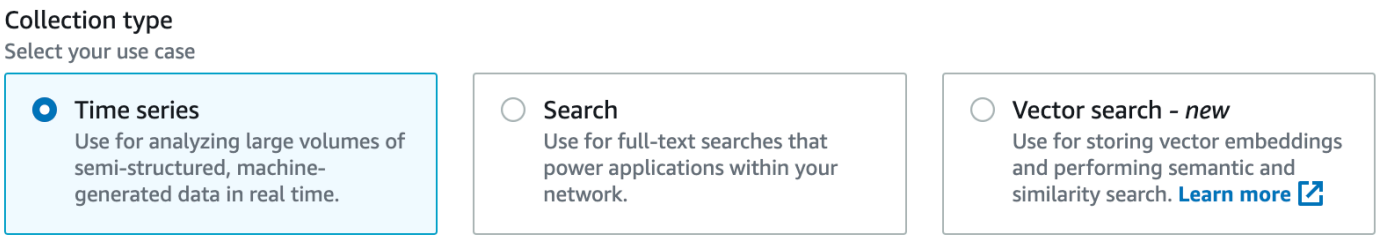
OpenSearch Serverless supporta tre tipi di raccolta principali:

Serie temporali: l'opzione dell'analisi dei log si concentra sull'analisi di grandi volumi di dati semistrutturati generati da macchine in tempo reale per approfondimenti sull'aspetto operativo, aziendale, della sicurezza e del comportamento degli utenti.

Ricerca: l'opzione della ricerca full-text supporta le applicazioni nelle reti interne (ad esempio, per i sistemi di gestione dei contenuti, i documenti legali, ecc.) e le applicazioni connesse a Internet (ad esempio, per la ricerca di contenuti e nei siti Web di e-commerce).

Ricerca vettoriale: ricerca semantica su incorporamenti vettoriali che semplifica la gestione dei dati vettoriali e potenzia le esperienze di ricerca aumentata di machine learning (ML) e le applicazioni di intelligenza artificiale generativa, come chatbot, assistenti personali e rilevamento delle frodi.

Quando all'inizio crei una raccolta, scegli un tipo di raccolta:



Il tipo di raccolta scelto dipende dal tipo di dati che intendi importare nella raccolta e dal modo in cui intendi interrogarli. Non puoi modificare il tipo di raccolta dopo averla creata.

I tipi di raccolta presentano le seguenti differenze rilevanti:

- Per le raccolte di ricerca e di ricerca vettoriale, tutti i dati vengono archiviati in hot storage per garantire tempi di risposta rapidi alle query. Le raccolte di serie temporali utilizzano una combinazione di archiviazione ad accesso frequente e a caldo, in cui i dati più recenti vengono conservati in un'archiviazione ad accesso frequente per ottimizzare i tempi di risposta alle interrogazioni per i dati a cui, come suggerisce il nome, si accede più frequentemente.
- Per le raccolte di serie temporali e di ricerca vettoriale, non è possibile indicizzarle in base a un ID di documento personalizzato o aggiornarle tramite richieste upsert. Questa operazione è riservata ai casi d'uso della ricerca. Puoi invece eseguire l'aggiornamento in base all'ID del documento. Per ulteriori informazioni, consulta the section called “Operazioni e autorizzazioni API supportate OpenSearch ”.
- Per le raccolte di ricerche e serie temporali, non puoi utilizzare indici di tipo k-NN.

Prezzi OpenSearch per Serverless

In OpenSearch Serverless, ti vengono addebitati i seguenti componenti:

- Calcolo dell'importazione dei dati
- Elaborazione di ricerche e query
- Archiviazione conservata in Amazon S3

Le OCU sono fatturate su base oraria, a granularità per secondo. Nel rendiconto dell'account, viene visualizzata una voce relativa al calcolo in ore delle OCU, che sono contrassegnate da un'etichetta per l'importazione dei dati e un'etichetta per la ricerca. Su base mensile vengono fatturati anche i dati archiviati in Amazon S3. Non ti viene addebitato alcun costo per l'utilizzo delle OpenSearch dashboard.

Quando crei una raccolta e abiliti le repliche attive ridondanti, ti vengono fatturati un minimo di 2 OCU [0,5 OCU x 2] per l'ingestione e 1 OCU [0,5 OCU x 2] per la ricerca. Se disabiliti le repliche attive ridondanti, ti verrà addebitato un minimo di 1 OCU [0,5 OCU x 2] per la prima raccolta nel tuo account. Tutte le raccolte successive possono condividere tali OCU.

OpenSearch Serverless aggiunge OCU aggiuntive con incrementi di 1 OCU in base alla potenza di calcolo e allo storage necessari per supportare le tue raccolte. Per tenere sotto controllo i costi, puoi configurare un numero massimo di OCU per il tuo account.

> **Note**
>
> Le raccolte con contenuti unici non AWS KMS keys possono condividere le OCU con altre raccolte.

OpenSearch Serverless tenta di utilizzare le risorse minime richieste per tenere conto dei cambiamenti dei carichi di lavoro. Il numero di OCU fornite in un dato momento può variare e non è esatto. Nel tempo, l'algoritmo utilizzato da OpenSearch Serverless continuerà a migliorare per ridurre al minimo l'utilizzo del sistema.

Per i dettagli completi sui prezzi, consulta i prezzi OpenSearch di Amazon Service.

Supportato Regioni AWS

OpenSearch Serverless è disponibile in un sottoinsieme di Regioni AWS tale OpenSearch servizio disponibile in. Per un elenco delle regioni supportate, consulta gli endpoint e le quote di Amazon OpenSearch Service nel. Riferimenti generali di AWS

Limitazioni

OpenSearch Serverless presenta le seguenti limitazioni:

- Alcune operazioni OpenSearch API non sono supportate. Per informazioni, consulta the section called “Operazioni e autorizzazioni API supportate OpenSearch ”.
- Alcuni OpenSearch plugin non sono supportati. Per informazioni, consulta the section called “ OpenSearch Plugin supportati”.
- Al momento non è possibile migrare automaticamente i dati da un dominio di OpenSearch servizio gestito a una raccolta serverless. È necessario reindicizzare i dati da un dominio a una raccolta.
- L'accesso multi-account alle raccolte non è supportato. Non è possibile includere raccolte da altri account nelle tue policy di crittografia o accesso ai dati.
- I OpenSearch plugin personalizzati non sono supportati.
- Non puoi scattare o ripristinare istantanee di raccolte OpenSearch Serverless.
- La ricerca e la replica tra Regioni non sono supportate.
- Ci sono dei limiti al numero di risorse serverless di cui è possibile disporre in un singolo account e in una sola regione. Vedi Quote OpenSearch Serverless.

- L'intervallo di aggiornamento per gli indici nelle raccolte di ricerca vettoriale è di circa 60 secondi. L'intervallo di aggiornamento per gli indici nelle raccolte di ricerca e di serie temporali è di circa 10 secondi.
- Il numero di shard, il numero di intervalli e l'intervallo di aggiornamento non sono modificabili e vengono gestiti da Serverless. OpenSearch La strategia di sharding si basa sul tipo di raccolta e sul traffico. Ad esempio, una raccolta di serie temporali ridimensiona gli shard primari in base ai colli di bottiglia relativi al traffico di scrittura.
- Sono supportate le funzionalità geospaziali disponibili nelle versioni fino alla 2.1. OpenSearch

Service e Serverless a confronto OpenSearch OpenSearch

In OpenSearch Serverless, alcuni concetti e funzionalità sono diversi dalla funzionalità corrispondente per un dominio di servizio fornito. OpenSearch Ad esempio, una differenza importante è che OpenSearch Serverless non ha il concetto di cluster o nodo.

La tabella seguente descrive in che modo le funzionalità e i concetti importanti di OpenSearch Serverless differiscono dalla funzionalità equivalente in un dominio di servizio fornito. OpenSearch

Funzionalità	OpenSearch Servizio	OpenSearch Senza server
Domini invece di raccolte	Gli indici sono contenuti in domini, che sono cluster preimpostati. OpenSearch Per ulteriori informazioni, consulta Creazione e gestione dei domini.	Gli indici sono contenuti in raccolte, ossia raggruppamenti logici di indici che rappresen tano un carico di lavoro o un caso d'uso specifico. Per ulteriori informazioni, consulta the section called “Creazione, elencazione ed eliminazione di raccolte”.
Tipi di nodi e gestione della capacità	Crei un cluster con i tipi di nodi che soddisfano le tue specifiche di costi e prestazio ni. Devi calcolare i tuoi requisiti di archiviazione e scegliere un tipo di istanza per il tuo dominio.	OpenSearch Serverless ridimensiona e fornisce automaticamente unità di calcolo aggiuntive per l'account in base all'utilizzo della capacità. Per ulteriori informazioni, consulta the section called “Gestione dei limiti di capacità”.

Funzionalità	OpenSearch Servizio	OpenSearch Senza server
	Per ulteriori informazioni, consulta the section called “Dimensionamento dei domini”.	
Fatturazione	Pagherai per ogni ora d'uso di un'istanza EC2 e per le dimensioni complessive di tutti i volumi di archiviazione EBS collegati alle istanze. Per ulteriori informazioni, consulta the section called “Prezzi”.	Per l'elaborazione relativa all'importazione dei dati, l'elaborazione per la ricerca e l'interro gazione, e lo spazio di archiviazione conservat o in S3, ricevi un addebito espresso in OCU all'ora. Per ulteriori informazioni, consulta the section called “Prezzi OpenSearch per Serverless”.
Encryption (Crittografia)	La crittografia dei dati inattivi è facoltativa per i domini. Per ulteriori informazioni, consulta the section called “Crittografia a riposo”.	La crittografia dei dati inattivi è obbligatoria per le raccolte. Per ulteriori informazioni, consulta the section called “Crittografia”.
Controllo dell'accesso ai dati	L'accesso ai dati all'interno dei domini è determinato dalle policy IAM e dal controllo granulare degli accessi.	L'accesso ai dati all'interno delle raccolte è determinato dalle policy di accesso ai dati.
Operazioni supportate OpenSearch	OpenSearch Il servizio supporta un sottoinsieme di tutte le operazioni OpenSearch API. Per ulteriori informazioni, consulta the section called “Operazioni supportate”.	OpenSearch Serverless supporta un sottoinsi eme diverso di OpenSearch operazioni API. Per ulteriori informazioni, consulta the section called “Operazioni e plug-in supportati”.

Funzionalità	OpenSearch Servizio	OpenSearch Senza server
Accesso ai pannelli di controllo	Accedi con nome utente e password. Per ulteriori informazioni, consulta the section called “Accesso alle OpenSearch dashboard come utente principale”.	Se hai effettuato l'accesso alla AWS console e accedi all'URL della dashboard, accederai automaticamente. Per ulteriori informazioni, consulta the section called “Accesso ai OpenSearch pannelli di controllo”.
API	Interagisci in modo programmatico con il OpenSearch servizio utilizzando le operazioni dell'API del OpenSearch servizio.	Interagisci a livello di codice con OpenSearch Serverless utilizzando le operazioni dell'API Serverless. OpenSearch
Accesso alla rete	Le impostazioni di rete per un dominio si applicano all'endpoint del dominio e all'endpoint Dashboards. OpenSearch L'accesso alla rete per entrambi è strettamente accoppiato.	Le impostazioni di rete per l'endpoint del dominio e l'endpoint OpenSearch Dashboards sono disaccoppiate. Puoi scegliere di non configurare l'accesso alla rete per i dashboard. OpenSearch Per ulteriori informazioni, consulta the section called “Accesso alla rete”.
Firma delle richieste	Utilizza i client REST di OpenSearch alto e basso livello per firmare le richieste. Specifica il nome del servizio come `es`.	Al momento, OpenSearch Serverless supporta un sottoinsieme di client supportati OpenSearch da Service. Quando firmi richieste, specifica il nome del servizio come `aoss`. L'intestazione `x-amz-content-sha256` è obbligatoria. Per ulteriori informazioni, consulta the section called “Altri clienti”.

Funzionalità	OpenSearch Servizio	OpenSearch Senza server
OpenSearch aggiornamenti di versione	Aggiorna manualmente i tuoi domini non appena OpenSearch diventano disponibili nuove versioni. Sei responsabile di assicurarti che il tuo dominio soddisfi i requisiti di aggiornamento e di aver apportato eventuali modifiche importanti.	OpenSearch Serverless aggiorna automaticamente le tue raccolte a nuove versioni. OpenSearch Gli aggiornamenti non devono avvenire necessariamente appena diventa disponibile una nuova versione.
Aggiornamenti del software del servizio	Non appena diventano disponibili, puoi applicare manualmente gli aggiornamenti del software del servizio al tuo dominio.	OpenSearch Serverless aggiorna automaticamente le tue raccolte per utilizzare le correzioni di bug, le funzionalità e i miglioramenti delle prestazioni più recenti.
Accesso VPC	Puoi effettuare il provisioning del tuo dominio all'interno di un VPC. Puoi anche creare endpoint OpenSearch VPC aggiuntivi gestiti dal servizio per accedere al dominio.	Crei uno o più endpoint VPC OpenSearch gestiti senza server per il tuo account. Quindi, puoi includere questi endpoint nelle policy di rete.
Autenticazione SAML	Puoi abilitare l'autenticazione SAML in base al dominio. Per ulteriori informazioni, consulta the section called “Autenticazione SAML per dashboard OpenSearch ”.	Puoi configurare uno o più provider SAML a livello di account, quindi puoi includere gli ID utente e di gruppo associati nelle policy di accesso ai dati. Per ulteriori informazioni, consulta the section called “Autenticazione SAML”.
Transport Layer Security (TLS)	OpenSearch Il servizio supporta TLS 1.2 ma si consiglia di utilizzare TLS 1.3.	OpenSearch Serverless supporta TLS 1.2 ma si consiglia di utilizzare TLS 1.3.

Guida introduttiva ad Amazon OpenSearch Serverless

Questo tutorial illustra i passaggi di base per avviare rapidamente una raccolta di ricerche Amazon OpenSearch Serverless. Una raccolta di ricerche ti consente di potenziare le applicazioni nelle tue reti interne e le applicazioni connesse a Internet, come la ricerca di siti di e-commerce e la ricerca di contenuti.

Per informazioni su come utilizzare una raccolta di ricerca vettoriale, consulta. the section called “Lavorare con le raccolte di ricerca vettoriale” Per informazioni più dettagliate sull'uso delle raccolte, consulta the section called “Creazione, elencazione ed eliminazione di raccolte” e gli altri argomenti di questa guida.

In questo tutorial completerai le seguenti fasi:

1. Configurazione delle autorizzazioni
2. Creazione di una raccolta
3. Caricamento e ricerca dei dati
4. Eliminazione della raccolta

Fase 1: configurazione delle autorizzazioni

Per completare questo tutorial e utilizzare OpenSearch Serverless in generale, è necessario disporre delle autorizzazioni IAM corrette. In questo tutorial creerai una raccolta, caricherai i dati e farai una ricerca, quindi eliminerai la raccolta.

L'utente o il ruolo devono avere una policy basata sull'identità allegata con le seguenti autorizzazioni minime:

```
{
  "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": "*"
    }
  ]
}
```

Per ulteriori informazioni sulle autorizzazioni IAM OpenSearch Serverless, consulta. the section called “Identity and Access Management”

Fase 2: creazione di una raccolta

Una raccolta è un gruppo di OpenSearch indici che interagiscono per supportare un carico di lavoro o un caso d'uso specifici.

Per creare una raccolta Serverless OpenSearch

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegli Collections (Raccolte) nel pannello di navigazione a sinistra e scegli Create collection (Crea raccolta).
3. Nomina la raccolta movies (film).
4. Per il tipo di raccolta, scegli Search (Cerca). Per ulteriori informazioni, consulta Scelta di un tipo di raccolta.
5. Per Sicurezza, scegli Standard create.
6. In Crittografia, seleziona Usa Chiave di proprietà di AWS. Questo è AWS KMS key quello che OpenSearch Serverless utilizzerà per crittografare i tuoi dati.
7. In Network (Rete), configura le impostazioni di rete per la raccolta.

   - Per il tipo di accesso, seleziona Public (Pubblico).
   - Per il tipo di risorsa, scegli sia Abilita l'accesso agli OpenSearch endpoint che Abilita l'accesso ai dashboard. OpenSearch Poiché caricherai e cercherai dati utilizzando OpenSearch le dashboard, devi abilitare entrambe.

8. Seleziona Successivo.
9. Per Configure data access (Configura l'accesso ai dati), configura le impostazioni di accesso per la raccolta. Le policy di accesso ai dati consentono a utenti e ruoli di accedere ai dati all'interno di una raccolta. In questo tutorial, forniremo a un singolo utente le autorizzazioni necessarie per indicizzare e cercare i dati nella raccolta denominata movies.

   Crea una singola regola che fornisca l'accesso alla raccolta movies. Nomina la regola Accesso alla raccolta movies.
10. Scegli Aggiungi responsabili, utenti e ruoli IAM e seleziona l'utente o il ruolo che utilizzerai per accedere alle OpenSearch dashboard e indicizzare i dati. Selezionare Salva.
11. In Index permissions (Autorizzazioni relative all'indice), seleziona tutte le autorizzazioni.
12. Seleziona Successivo.
13. Per le impostazioni della policy di accesso, scegli Create a new data access policy (Crea una nuova policy di accesso ai dati) e assegna alla policy il nome movies.
14. Seleziona Successivo.
15. Controlla le impostazioni della raccolta e scegli Submit (Invia). Attendi alcuni minuti affinché lo stato della raccolta diventi `Active`.

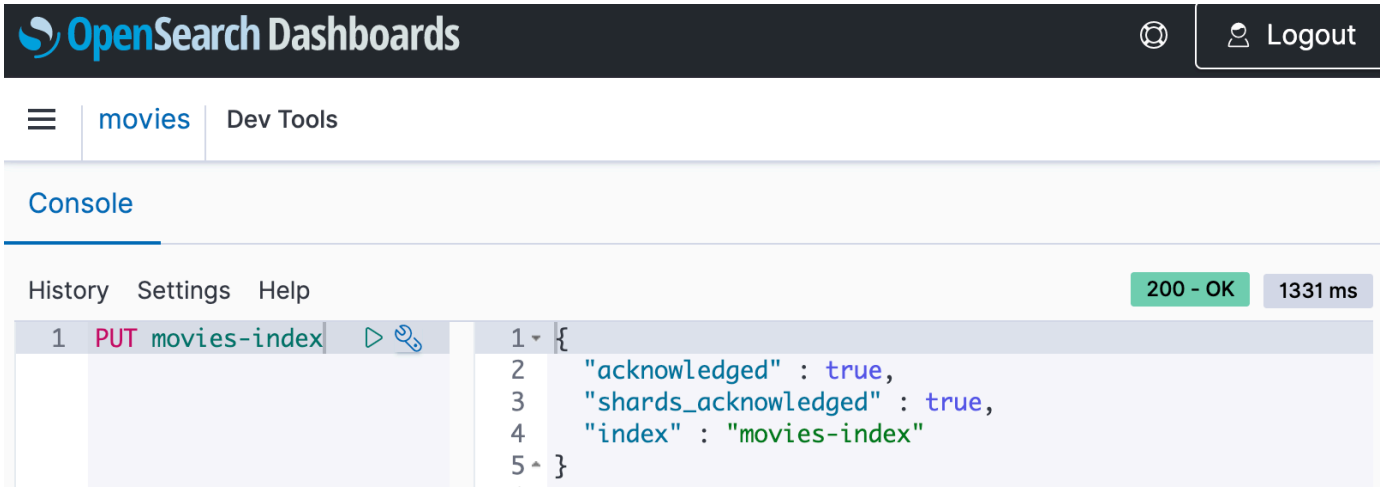
Fase 3: Caricamento e ricerca dei dati

Puoi caricare dati in una raccolta OpenSearch Serverless utilizzando Postman o cURL. Per brevità, questi esempi utilizzano Dev Tools all'interno della console Dashboards. OpenSearch

Indicizzazione e ricerca dei dati nella raccolta movies

1. Scegli Collections (Raccolte) nel pannello di navigazione a sinistra e seleziona la raccolta movies per aprire la rispettiva pagina dei dettagli.
2. Scegli l'URL delle OpenSearch dashboard per la raccolta. L'URL assume il formato `https://dashboards.{region}.aoss.amazonaws.com/_login/?collectionId={collection-id}`.
3. All'interno di OpenSearch Dashboards, apri il riquadro di navigazione a sinistra e scegli Dev Tools.
4. Per creare un singolo indice denominato movies-index, invia la seguente richiesta:

```
PUT movies-index
```



5. Per indicizzare un singolo documento in movies-index, invia la seguente richiesta:

```
PUT movies-index/_doc/1
{
  "title": "Shawshank Redemption",
  "genre": "Drama",
  "year": 1994
}
```

6. Per cercare dati nelle OpenSearch dashboard, devi configurare almeno un modello di indice. OpenSearch utilizza questi modelli per identificare gli indici da analizzare. Apri il pannello di navigazione a sinistra, scegli Stack Management (Gestione stack), scegli Index Patterns (Modelli di indice), quindi scegli Create index pattern (Crea modello di indice). Per questo tutorial, digita movies.
7. Scegliere Fase successiva quindi selezionare Crea modello di indice. Dopo aver creato il modello, è possibile visualizzare i vari campi del documento, ad esempio `title` e `genre`.
8. Per iniziare a cercare i dati, apri di nuovo il pannello di navigazione a sinistra e scegli Discover (Rileva) o utilizza l'API di ricerca nei Dev Tools.

Fase 4: Eliminazione della raccolta

Poiché la raccolta movies è stata creata per finalità di prova, è consigliabile eliminarla una volta terminate le prove in modo da evitare costi aggiuntivi.

Per eliminare una raccolta Serverless OpenSearch

1. Torna alla console di Amazon OpenSearch Service.

2. Scegli Collections (Raccolte) nel pannello di navigazione a sinistra e seleziona la raccolta movies.
3. Scegli Elimina e conferma l'eliminazione.

Passaggi successivi

Adesso che è chiaro come creare una raccolta e i dati di indice, è possibile provare a completare alcuni degli esercizi seguenti:

- Scopri ulteriori opzioni avanzate per la creazione di una raccolta. Per ulteriori informazioni, consulta the section called “Creazione, elencazione ed eliminazione di raccolte”.
- Scopri come configurare le policy di sicurezza per gestire la sicurezza delle raccolte su larga scala. Per ulteriori informazioni, consulta the section called “Sicurezza in modalità serverless OpenSearch ”.
- Scopri altri modi per indicizzare i dati nelle raccolte. Per ulteriori informazioni, consulta the section called “Importazione dei dati nelle raccolte”.

Creazione e gestione di raccolte Amazon OpenSearch Serverless

Puoi creare raccolte Amazon OpenSearch Serverless utilizzando la console, l'API AWS CLI e gli AWS SDK e. AWS CloudFormation

Argomenti

- Creazione, pubblicazione ed eliminazione di raccolte Amazon OpenSearch Serverless
- Lavorare con le raccolte di ricerca vettoriale
- Utilizzo delle politiche del ciclo di vita dei dati con Amazon Serverless OpenSearch
- Utilizzo degli AWS SDK per interagire con Amazon Serverless OpenSearch
- Utilizzo AWS CloudFormation per creare raccolte Amazon OpenSearch Serverless

Creazione, pubblicazione ed eliminazione di raccolte Amazon OpenSearch Serverless

Una raccolta in Amazon OpenSearch Serverless è un raggruppamento logico di uno o più indici che rappresentano un carico di lavoro di analisi. OpenSearch Il servizio gestisce e ottimizza automaticamente la raccolta, richiedendo un input manuale minimo.

Argomenti

Autorizzazioni richieste

OpenSearch Serverless utilizza le seguenti autorizzazioni AWS Identity and Access Management (IAM) per creare e gestire le raccolte. È possibile specificare le condizioni IAM per limitare gli utenti a raccolte specifiche.

- `aoss:CreateCollection`: crea una raccolta.
- `aoss:ListCollections`: elenca le raccolte nell'account corrente.
- `aoss:BatchGetCollection`: ottieni dettagli su una o più raccolte.
- `aoss:UpdateCollection`: modifica una raccolta.
- `aoss:DeleteCollection`: elimina una raccolta.

La seguente policy di accesso basata sull'identità di esempio fornisce le autorizzazioni minime necessarie a un utente per gestire una singola raccolta denominata `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` e `aoss:CreateSecurityPolicy` sono inclusi perché le policy di crittografia, rete e accesso ai dati sono necessarie per il corretto funzionamento di una raccolta. Per ulteriori informazioni, consulta the section called “Identity and Access Management”.

> **Note**
>
> Se stai creando la prima raccolta nel tuo account, hai bisogno anche dell'autorizzazione `iam:CreateServiceLinkedRole`. Per ulteriori informazioni, consulta the section called “Ruolo di creazione della raccolta”.

Creazione di raccolte

È possibile utilizzare la console o il AWS CLI per creare una raccolta serverless. Questi passaggi spiegano come creare una raccolta di ricerche o di serie temporali. Per creare una raccolta di ricerca vettoriale, vedithe section called “Lavorare con le raccolte di ricerca vettoriale”.

Creazione di una raccolta (console)

Creazione di una raccolta tramite la console

1. Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home/.
2. Espandi Serverless nel pannello di navigazione a sinistra e scegli Collections (Raccolte).
3. Scegli Create collection (Crea raccolta).

4. Fornisci un nome e una descrizione per la raccolta. Il nome deve soddisfare i seguenti criteri:

   - È unico per il tuo account e Regione AWS
   - Inizia con una lettera minuscola
   - Contiene da 3 a 32 caratteri
   - Contiene solo lettere minuscole a-z, i numeri da 0 a 9 e i trattini (-)

5. Scegli un tipo di raccolta:

   - Ricerca: l'opzione della ricerca full-text supporta le applicazioni nelle reti interne e le applicazioni connesse a Internet. Tutti i dati di ricerca vengono memorizzati in un'archiviazione ad accesso frequente per garantire tempi di risposta rapidi alle query.
   - Serie temporali: segmento di analisi dei log che si concentra sull'analisi di grandi volumi di dati semistrutturati generati da macchine. Almeno 24 ore di dati vengono archiviate su indici caldi e il resto rimane in una memoria a caldo.
   - Ricerca vettoriale: ricerca semantica sugli incorporamenti vettoriali che semplifica la gestione dei dati vettoriali. Potenzia le esperienze di ricerca aumentata di machine learning (ML) e le applicazioni di intelligenza artificiale generativa come chatbot, assistenti personali e rilevamento delle frodi.

   Per ulteriori informazioni, consulta the section called “Scelta di un tipo di raccolta”.

6. In Tipo di distribuzione, scegli l'impostazione di ridondanza per la tua raccolta. Per impostazione predefinita, ogni raccolta viene creata con ridondanza, il che significa che le unità di OpenSearch calcolo (OCU) di indicizzazione e ricerca hanno ciascuna le proprie repliche in standby in una zona di disponibilità diversa. Per scopi di sviluppo e test, puoi scegliere di disabilitare la ridondanza, in modo da ridurre a due il numero di OCU nella raccolta. Per ulteriori informazioni, consulta the section called “Come funziona”.
7. In Crittografia, scegli una AWS KMS chiave con cui crittografare i tuoi dati. OpenSearch Serverless ti avvisa se il nome della raccolta che hai inserito corrisponde a uno schema definito in una politica di crittografia. Puoi scegliere di mantenere tale corrispondenza o di sostituirla con impostazioni di crittografia specifiche. Per ulteriori informazioni, consulta the section called “Crittografia”.
8. In Network access settings (Impostazioni di accesso alla rete), configura l'accesso alla rete per la raccolta.

- Per Tipo di accesso, seleziona pubblico o privato. Quindi, specifica quali endpoint VPC Servizi AWS possono accedere alla raccolta.
  - Endpoint VPC per l'accesso: specifica uno o più endpoint VPC per consentire l'accesso. Per creare un endpoint VPC, consulta la sezione the section called “Endpoint VPC”.
  - Servizio AWS accesso privato: seleziona uno o più servizi supportati a cui consentire l'accesso.
- Per Tipo di risorsa, seleziona se la raccolta sarà accessibile tramite il relativo OpenSearchendpoint (per effettuare chiamate API tramite curl, Postman e così via), tramite l'endpoint OpenSearch Dashboards (per utilizzare le visualizzazioni ed effettuare chiamate API tramite la console) o tramite entrambi.

> **Note**
>
> Servizio AWS l'accesso privato si applica solo all'endpoint, non all' OpenSearchendpoint Dashboards. OpenSearch

OpenSearch Serverless ti avvisa se il nome della raccolta che hai inserito corrisponde a uno schema definito in una politica di rete. Puoi scegliere di mantenere tale corrispondenza o di sostituirla con impostazioni di rete personalizzate. Per ulteriori informazioni, consulta the section called “Accesso alla rete”.

9. (Facoltativo) Aggiungi uno o più tag alla raccolta. Per ulteriori informazioni, consulta la pagina the section called “Assegnazione di tag alle raccolte”.
10. Seleziona Next (Successivo).
11. Configura le regole di accesso ai dati per la raccolta che definiscono chi può accedere ai dati all'interno della raccolta. Per ogni regola che crei, completa questi passaggi:
    - Scegli Add principals (Aggiungi principali) e seleziona uno o più ruoli IAM o utenti e gruppi SAML a cui fornire l'accesso ai dati.
    - In Grant permissions (Concedi autorizzazioni), seleziona le autorizzazioni per l'alias, il modello e l'indice da concedere ai principali associati. Per un elenco completo delle autorizzazioni e l'accesso che queste concedono, consulta la sezione the section called “Operazioni e autorizzazioni API supportate OpenSearch ”.

OpenSearch Serverless ti avvisa se il nome della raccolta che hai inserito corrisponde a uno schema definito in una politica di accesso ai dati. Puoi scegliere di mantenere tale corrispondenza o di sostituirla con impostazioni di accesso ai dati specifiche. Per ulteriori informazioni, consulta la pagina the section called “Controllo dell'accesso ai dati”.

12. Seleziona Next (Successivo).
13. In Data access policy settings (Impostazioni della policy di accesso ai dati), scegli cosa fare con le regole appena create. È possibile utilizzarle per creare una nuova policy di accesso ai dati o aggiungerle a una policy esistente.
14. Rivedi la configurazione della raccolta e scegli Submit (Invia).

Lo stato della raccolta cambia `Creating` quando OpenSearch Serverless crea la raccolta.

Creazione di una raccolta (CLI)

Prima di creare una raccolta utilizzando il AWS CLI, è necessario disporre di una politica di crittografia con un modello di risorse che corrisponda al nome previsto della raccolta. Ad esempio, se intendi dare un nome all'applicazione dei log della raccolta, potresti creare una policy di crittografia come questa:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource
\":[\"collection\/logs-application\"]}],\"AWSOwnedKey\":true}"
```

Se prevedi di utilizzare la policy per raccolte aggiuntive, puoi rendere la regola più ampia, come `collection/logs*` o `collection/*`.

Inoltre, è necessario configurare le impostazioni di rete per la raccolta sotto forma di una policy di rete. Utilizzando l'esempio precedente applicazione-log, è possibile creare la seguente policy di rete:

```
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**
>
> È possibile creare policy di rete dopo aver creato una raccolta, tuttavia consigliamo di farlo prima.

Per creare una raccolta, invia una CreateCollectionrichiesta:

```
aws opensearchserverless create-collection --name "logs-application" --type SEARCH --
description "A collection for storing log data"
```

Per `type`, specifica `SEARCH` o `TIMESERIES`. Per ulteriori informazioni, consulta the section called "Scelta di un tipo di raccolta".

Risposta di esempio

```
{
    "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
    }
}
```

Se non specifichi un tipo di raccolta nella richiesta, il valore predefinito sarà `TIMESERIES`. Se la tua raccolta è crittografata con una Chiave di proprietà di AWS, la `kmsKeyArn` è `auto` anziché un ARN.

> **Important**
>
> Dopo aver creato una raccolta, non potrai accedervi a meno che non corrisponda a una policy di accesso ai dati. Per istruzioni sulla creazione di policy di accesso ai dati, consulta la sezione the section called "Controllo dell'accesso ai dati".

Accesso ai OpenSearch pannelli di controllo

Dopo aver creato una raccolta con AWS Management Console, puoi accedere all'URL delle OpenSearch dashboard della raccolta. Puoi trovare l'URL delle dashboard scegliendo Raccolte nel riquadro di navigazione a sinistra e selezionando la raccolta per aprirne la pagina dei dettagli. L'URL assume il formato `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc`. Una volta che accedi all'URL, accederai automaticamente alle dashboard.

Se hai già l'URL delle OpenSearch dashboard disponibile ma non lo sei AWS Management Console, chiamando l'URL delle dashboard dal browser verrai reindirizzato alla console. Una volta inserite le AWS credenziali, accederai automaticamente a Dashboards. Per informazioni sull'accesso alle raccolte per SAML, consulta Accesso ai OpenSearch dashboard con SAML.

Il timeout della console OpenSearch Dashboards è di un'ora e non è configurabile.

> **Note**
>
> Il 10 maggio 2023, OpenSearch ha introdotto un endpoint globale comune per Dashboards. OpenSearch Ora puoi accedere alle OpenSearch dashboard nel browser con un URL che assume il formato. `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc` Per garantire la compatibilità con le versioni precedenti, continueremo a supportare gli endpoint OpenSearch Dashboards specifici della raccolta esistenti con il formato. `https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/_dashboards`

Visualizzazione delle raccolte

Puoi visualizzare le raccolte esistenti nella tua Account AWS scheda Raccolte della console di Amazon OpenSearch Service.

Per elencare le raccolte insieme ai relativi ID, invia una ListCollectionsrichiesta.

```
aws opensearchserverless list-collections
```

Risposta di esempio

```
{
```

```
   "collectionSummaries":[
      {
         "arn":"arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "id":"07tjusf2h91cunochc",
         "name":"my-collection",
         "status":"CREATING"
      }
   ]
}
```

Per limitare i risultati della ricerca, utilizza i filtri della raccolta. Questa richiesta filtra la risposta alle raccolte nello stato `ACTIVE`:

```
aws opensearchserverless list-collections --collection-filters '{ "status": "ACTIVE" }'
```

Per ottenere informazioni più dettagliate su una o più raccolte, inclusi l' OpenSearch endpoint e l'endpoint OpenSearch Dashboards, invia una richiesta: BatchGetCollection

```
aws opensearchserverless batch-get-collection --ids ["07tjusf2h91cunochc",
 "1iu5usc4rame"]
```

> **Note**
>
> Nella richiesta puoi includere `--names` o `--ids`, ma non entrambi.

Risposta di esempio

```
{
   "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":[]
}
```


Eliminazione di raccolte

Eliminando una raccolta vengono eliminati anche tutti i relativi dati e gli indici. Non è possibile recuperare le raccolte dopo averle eliminate.

Per eliminare una raccolta tramite la console

1. Dal pannello Raccolte della console Amazon OpenSearch Service, seleziona la raccolta che desideri eliminare.
2. Scegli Elimina e conferma l'eliminazione.

Per eliminare una raccolta utilizzando il AWS CLI, invia una DeleteCollectionrichiesta:

```
aws opensearchserverless delete-collection --id 07tjusf2h91cunochc
```

Risposta di esempio

```
{
   "deleteCollectionDetail":{
      "id":"07tjusf2h91cunochc",
      "name":"my-collection",
      "status":"DELETING"
   }
}
```

Lavorare con le raccolte di ricerca vettoriale

Il tipo di raccolta di ricerca vettoriale in OpenSearch Serverless offre una funzionalità di ricerca per similarità scalabile e ad alte prestazioni. Semplifica la creazione di moderne esperienze di ricerca aumentata di machine learning (ML) e applicazioni generative di intelligenza artificiale (AI) senza dover gestire l'infrastruttura di database vettoriale sottostante.

I casi d'uso per le raccolte di ricerche vettoriali includono la ricerca di immagini, la ricerca di documenti, il recupero di musica, i consigli sui prodotti, le ricerche video, le ricerche basate sulla posizione, il rilevamento di frodi e il rilevamento di anomalie.

Poiché il motore vettoriale per OpenSearch Serverless è alimentato dalla funzionalità di ricerca k-Nearest Neighbor (k-NN) in, ottieni le stesse funzionalità con la semplicità di un ambiente serverless. OpenSearch Il motore supporta le operazioni dell'API k-NN. OpenSearch Con queste operazioni, puoi sfruttare la ricerca full-text, il filtraggio avanzato, le aggregazioni, le query geospaziali, le query annidate per un recupero più rapido dei dati e risultati di ricerca migliorati.

Il motore vettoriale fornisce metriche di distanza come la distanza euclidea, la somiglianza del coseno e la somiglianza del prodotto scalare e può supportare 16.000 dimensioni. È possibile memorizzare campi con vari tipi di dati per i metadati, ad esempio numeri, valori booleani, date, parole chiave e punti geografici. Puoi anche memorizzare campi con testo per informazioni descrittive per aggiungere più contesto ai vettori memorizzati. La colocazione dei tipi di dati riduce la complessità, aumenta la manutenibilità ed evita la duplicazione dei dati, problemi di compatibilità delle versioni e problemi di licenza.

Guida introduttiva alle raccolte di ricerca vettoriale

In questo tutorial, completerai i seguenti passaggi per archiviare, cercare e recuperare gli incorporamenti vettoriali in tempo reale:

1. Configurazione delle autorizzazioni
2. Creazione di una raccolta

3. Caricamento e ricerca dei dati
4. Eliminazione della raccolta

Fase 1: configurazione delle autorizzazioni

Per completare questo tutorial (e per utilizzare OpenSearch Serverless in generale), devi disporre delle autorizzazioni AWS Identity and Access Management (IAM) corrette. In questo tutorial, crei una raccolta, carichi e cerchi dati, quindi elimini la raccolta.

L'utente o il ruolo devono avere una policy basata sull'identità allegata con le seguenti autorizzazioni minime:

```
{
  "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": "*"
    }
  ]
}
```

Per ulteriori informazioni sulle autorizzazioni IAM OpenSearch Serverless, consulta. the section called “Identity and Access Management”

Fase 2: creazione di una raccolta

Una raccolta è un gruppo di OpenSearch indici che interagiscono per supportare un carico di lavoro o un caso d'uso specifici.

Per creare una raccolta Serverless OpenSearch

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Scegli Collections (Raccolte) nel pannello di navigazione a sinistra e scegli Create collection (Crea raccolta).
3. Assegna un nome all'alloggiamento della raccolta.
4. Per il tipo di raccolta, scegli Ricerca vettoriale. Per ulteriori informazioni, consulta the section called “Scelta di un tipo di raccolta”.
5. In Tipo di distribuzione, deseleziona Abilita ridondanza (repliche attive). In questo modo viene creata una raccolta in modalità sviluppo o test e il numero di unità di OpenSearch calcolo (OCU) nella raccolta viene ridotto a due. Se desideri creare un ambiente di produzione in questo tutorial, lascia selezionata la casella di controllo.
6. In Sicurezza, seleziona Easy create per semplificare la configurazione di sicurezza. Per impostazione predefinita, tutti i dati nel motore vettoriale sono crittografati in transito e inattivi. Il motore vettoriale supporta autorizzazioni IAM granulari in modo da poter definire chi può creare, aggiornare ed eliminare crittografie, reti, raccolte e indici.
7. Seleziona Successivo.
8. Controlla le impostazioni della raccolta e scegli Submit (Invia). Attendi alcuni minuti affinché lo stato della raccolta diventi `Active`.

Fase 3: Caricamento e ricerca dei dati

Un indice è una raccolta di documenti con uno schema di dati comune che consente di archiviare, cercare e recuperare gli incorporamenti vettoriali e altri campi. Puoi creare e caricare dati negli indici di una raccolta OpenSearch Serverless utilizzando la console Dev Tools in OpenSearch Dashboards o uno strumento HTTP come Postman o awscurl. Questo tutorial utilizza Dev Tools.

Indicizzazione e ricerca dei dati nella raccolta movies

1. Per creare un singolo indice per la tua nuova collezione, invia la seguente richiesta nella console Dev Tools. Per impostazione predefinita, questo crea un indice con un `nmslib` motore e una distanza euclidea.

```
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. Per indicizzare un singolo documento in housing-index, invia la seguente richiesta:

```
POST housing-index/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Per cercare proprietà simili a quelle del tuo indice, invia la seguente query:

```
GET housing-index/_search
{
    "size": 5,
    "query": {
        "knn": {
            "housing-vector": {
```

```
                "vector": [
                    10,
                    20,
                    30
                ],
                "k": 5
            }
        }
    }
}
```

Fase 4: Eliminazione della raccolta

Poiché la collezione di alloggi è a scopo di test, assicurati di eliminarla quando hai finito di sperimentare.

Per eliminare una raccolta OpenSearch Serverless

1. Torna alla console di Amazon OpenSearch Service.
2. Scegli Raccolte nel riquadro di navigazione a sinistra e seleziona la raccolta delle proprietà.
3. Scegli Elimina e conferma l'eliminazione.

Ricerca filtrata

Puoi utilizzare i filtri per affinare i risultati della ricerca semantica. Per creare un indice ed eseguire una ricerca filtrata sui tuoi documenti, sostituisci Carica e cerca dati nel tutorial precedente con le seguenti istruzioni. Gli altri passaggi rimangono invariati. Per ulteriori informazioni sui filtri, consulta K-nn search with filters.

Indicizzazione e ricerca dei dati nella raccolta movies

1. Per creare un indice singolo per la tua collezione, invia la seguente richiesta nella console 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. Per indicizzare un singolo documento housing-index-filtered, invia la seguente richiesta:

```
POST housing-index-filtered/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Per cercare i tuoi dati relativi a un appartamento a Seattle a un determinato prezzo ed entro una determinata distanza da un punto geografico, invia la seguente richiesta:

```
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
                  }
                }
              }
            ]
          }
        }
      }
    }
  }
}
```

Carichi di lavoro su scala miliardaria

Le raccolte di ricerca vettoriale supportano carichi di lavoro con miliardi di vettori. Non è necessario reindicizzare per scopi di ridimensionamento perché il ridimensionamento automatico lo fa per te. Se hai milioni di vettori (o più) con un numero elevato di dimensioni e hai bisogno di più di 200 OCU, contatta l'AWS assistenza per aumentare il numero massimo di unità di OpenSearch calcolo (OCU) per il tuo account.

Limitazioni

Le raccolte di ricerca vettoriale presentano le seguenti limitazioni:

- Le raccolte di ricerca vettoriale non supportano il motore Apache Lucene ANN.
- Le raccolte di ricerca vettoriale supportano solo l'algoritmo HNSW con Faiss e non supportano IVF e IVFQ.
- Le raccolte di ricerca vettoriale non supportano le operazioni API di warmup, stats e model training.
- Le raccolte di ricerca vettoriale non supportano script in linea o memorizzati.
- Le informazioni sul conteggio degli indici non sono disponibili nelle raccolte AWS Management Console per la ricerca vettoriale.
- L'intervallo di aggiornamento per gli indici nelle raccolte di ricerca vettoriale è di 60 secondi.

Passaggi successivi

Ora che sapete come creare una raccolta di ricerca vettoriale e indicizzare i dati, potreste provare alcuni dei seguenti esercizi:

- Usa il client OpenSearch Python per lavorare con raccolte di ricerca vettoriale. Guarda questo tutorial su. GitHub
- Usa il client OpenSearch Java per lavorare con raccolte di ricerca vettoriale. Guarda questo tutorial su. GitHub
- Configurato LangChain per essere utilizzato OpenSearch come archivio vettoriale. LangChain è un framework open source per lo sviluppo di applicazioni basate su modelli linguistici. Per ulteriori informazioni, consulta la LangChain documentazione.

Utilizzo delle politiche del ciclo di vita dei dati con Amazon Serverless OpenSearch

Una policy sul ciclo di vita dei dati per una raccolta di serie temporali Amazon OpenSearch Serverless determina la durata dei dati in tale raccolta. OpenSearch Serverless conserva i dati per il periodo di tempo che configuri.

Puoi configurare una politica del ciclo di vita dei dati separata per ogni indice di ogni raccolta di serie temporali presente nel tuo. Account AWS OpenSearch Serverless conserva i documenti negli indici almeno per il periodo di conservazione configurato nella policy. Quindi li elimina automaticamente con la massima diligenza possibile, in genere entro 48 ore o il 10% del periodo di conservazione, a seconda di quale sia il più lungo.

Solo le raccolte di serie temporali supportano le politiche relative al ciclo di vita dei dati. Non sono supportate dalle raccolte di ricerca o di ricerca vettoriale.

Argomenti

Politiche relative al ciclo di vita dei dati

In una politica del ciclo di vita dei dati, si specifica una serie di regole. La politica del ciclo di vita dei dati consente di gestire il periodo di conservazione dei dati associati agli indici o alle raccolte che soddisfano queste regole. Queste regole definiscono il periodo di conservazione dei dati in un indice o in un gruppo di indici. Ogni regola è composta da un tipo di risorsa (`index`), un periodo di conservazione e un elenco di risorse (indici) a cui si applica il periodo di conservazione.

Il periodo di conservazione viene definito con uno dei seguenti formati:

- `"MinIndexRetention": "24h"`— OpenSearch Serverless conserva i dati dell'indice per il periodo specificato in ore o giorni. È possibile impostare questo periodo in modo che sia compreso tra`24h`. `3650d`
- `"NoMinIndexRetention": true`— OpenSearch Serverless conserva i dati dell'indice a tempo indeterminato.

Nella seguente politica di esempio, la prima regola specifica un periodo di conservazione di 15 giorni per tutti gli indici della raccolta. `marketing` La seconda regola specifica che per tutti i nomi di indice che iniziano con `log` la `finance` raccolta non è impostato alcun periodo di conservazione e verranno conservati a tempo indeterminato.

```
{
   "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
   }
}
```

Nel seguente esempio di regola politica, OpenSearch Serverless conserva a tempo indeterminato i dati in tutti gli indici per tutte le raccolte all'interno dell'account.

```
{
   "Rules": [
      {
         "ResourceType": "index",
         "Resource": [
            "index/*/*"
         ]
      }
   ],
   "NoMinIndexRetention": true
}
```

Autorizzazioni richieste

Le policy del ciclo di vita per OpenSearch Serverless utilizzano le seguenti autorizzazioni (IAM). AWS Identity and Access Management Puoi specificare le condizioni IAM per limitare gli utenti alle politiche del ciclo di vita dei dati associate a raccolte e indici specifici.

- `aoss:CreateLifecyclePolicy`— Creare una policy sul ciclo di vita dei dati.
- `aoss:ListLifecyclePolicies`— Elenca tutte le politiche relative al ciclo di vita dei dati nell'account corrente.
- `aoss:BatchGetLifecyclePolicy`— Visualizza una politica sul ciclo di vita dei dati associata a un account o al nome di una policy.
- `aoss:BatchGetEffectiveLifecyclePolicy`— Visualizza una politica del ciclo di vita dei dati per una determinata risorsa (`index`è l'unica risorsa supportata).
- `aoss:UpdateLifecyclePolicy`— Modificare una determinata politica del ciclo di vita dei dati e modificarne l'impostazione o la risorsa di conservazione.
- `aoss:DeleteLifecyclePolicy`— Eliminare una politica sul ciclo di vita dei dati.

La seguente politica di accesso basata sull'identità consente a un utente di visualizzare tutte le politiche relative al ciclo di vita dei dati e di aggiornare le politiche in base al modello di risorse: `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": "*"
        }
    ]
}
```

Priorità delle policy

Possono verificarsi situazioni in cui le regole relative al ciclo di vita dei dati si sovrappongono, all'interno o tra le policy. Quando ciò accade, una regola con un nome o uno schema di risorsa più specifico per un indice sostituisce una regola con un nome o uno schema di risorsa più generale per tutti gli indici comuni a entrambe le regole.

Ad esempio, nella politica seguente, due regole si applicano a un indice. `index/sales/logstash` In questa situazione, la seconda regola ha la precedenza perché `index/sales/log*` è la corrispondenza più lunga a. `index/sales/logstash` Pertanto, OpenSearch Serverless non imposta alcun periodo di conservazione per l'indice.

```
{
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/*",
```

```
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/log*",
            ],
            "NoMinIndexRetention": true
         }
      ]
   }
```

Sintassi delle policy

Fornisci una o più regole. Queste regole definiscono le impostazioni del ciclo di vita dei dati per gli indici Serverless. OpenSearch

Ogni regola contiene i seguenti elementi. È possibile fornire `MinIndexRetention` o `NoMinIndexRetention` in ciascuna regola, ma non in entrambe.

Elemento	Descrizione
Tipo di risorsa	Il tipo di risorsa a cui si applica la regola. L'unica opzione supportata per le politiche del ciclo di vita dei dati è. `index`
Resource (Risorsa)	Un elenco di nomi e/o modelli di risorse. I pattern sono costituiti da un prefisso e un carattere jolly (*), che consentono l'applica zione delle autorizzazioni associate a più risorse. Ad esempio, `index/<collection-name|pattern> /<index-name|patter n>` .
MinIndexRetention	Il periodo minimo, in giorni (d) o ore (h), per conservare il documento nell'indice. Il limite inferiore è `24h` e il limite superiore è`3650d`.

Elemento	Descrizione
NoMinIndexRetention	`Set``true`, OpenSearch Serverless conserva i documenti a tempo indeterminato.

Di seguito vengono mostrati alcuni esempi:

```
{
  "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
    }
  ]
}
```

Creazione di politiche per il ciclo di vita dei dati () AWS CLI

Per creare una politica del ciclo di vita dei dati utilizzando le operazioni dell'API OpenSearch Serverless, usa il comando. CreateLifecyclePolicy Questo comando accetta sia le politiche in linea che i file.json. Le policy inline devono essere codificate come una stringa con escape JSON.

La seguente richiesta crea una politica del ciclo di vita dei dati:

```
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}]}"
```

Per fornire la policy in un file JSON, utilizzare il formato `--policy file://my-policy.json`

Visualizzazione delle politiche relative al ciclo di vita dei dati

Prima di creare una raccolta, potresti voler visualizzare in anteprima le politiche sul ciclo di vita dei dati esistenti nel tuo account per vedere quale ha un modello di risorse che corrisponde al nome della tua raccolta. La seguente ListLifecyclePoliciesrichiesta elenca tutte le politiche relative al ciclo di vita dei dati del tuo account:

```
aws opensearchserverless list-lifecycle-policies --type retention
```

La richiesta restituisce informazioni su tutte le politiche configurate per il ciclo di vita dei dati. Per visualizzare le regole del modello definite in una politica specifica, trova le informazioni sulla politica nel contenuto dell'`lifecyclePolicySummaries`elemento nella risposta. Prendi nota della `name` fine `type` di questa politica e utilizza queste proprietà in una BatchGetLifecyclePolicyrichiesta per ricevere una risposta con i seguenti dettagli della politica:

```
{
    "lifecyclePolicySummaries": [
        {
            "type": "retention",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

Per limitare i risultati alle politiche che contengono raccolte o indici specifici, puoi includere filtri di risorse:

```
aws opensearchserverless list-lifecycle-policies --type retention --resources
 "index/autoparts-inventory/*"
```

Per visualizzare informazioni dettagliate su una politica specifica, utilizzare il BatchGetLifecyclePolicycomando.

Aggiornamento delle politiche relative al ciclo di vita dei dati

Quando si modifica una politica del ciclo di vita dei dati, tutte le raccolte associate ne risentono. Per aggiornare una policy sul ciclo di vita dei dati nella console OpenSearch Serverless, espandi Data Lifecycle Policy, seleziona la policy da modificare e scegli Modifica. Apporta le modifiche necessarie, quindi scegli Save (Salva).

Per aggiornare una policy sul ciclo di vita dei dati utilizzando l'API Serverless, usa il comando OpenSearch . UpdateLifecyclePolicy È necessario includere una versione della policy nella richiesta. È possibile recuperare la versione della policy utilizzando i comandi `ListLifecyclePolicies` o `BatchGetLifecyclePolicy`. L'inclusione della versione più recente delle policy garantisce di non sovrascrivere inavvertitamente una modifica apportata da qualcun altro.

La seguente richiesta aggiorna una politica del ciclo di vita dei dati con un nuovo documento JSON di policy:

```
aws opensearchserverless update-lifecycle-policy \
    --name my-policy \
    --type retention \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Potrebbero esserci alcuni minuti di ritardo tra l'aggiornamento della policy e l'applicazione dei nuovi periodi di conservazione.

Eliminazione delle politiche relative al ciclo di vita dei dati

Quando elimini una politica del ciclo di vita dei dati, questa non si applica più agli indici corrispondenti. Per eliminare una policy nella console OpenSearch Serverless, seleziona la policy e scegli Elimina.

Puoi anche usare il DeleteLifecyclePolicycomando:

```
aws opensearchserverless delete-lifecycle-policy --name my-policy --type retention
```

Utilizzo degli AWS SDK per interagire con Amazon Serverless OpenSearch

Questa sezione include esempi di come utilizzare gli AWS SDK per interagire con Amazon OpenSearch Serverless. Questi esempi di codice mostrano come creare raccolte e policy di sicurezza, e come eseguire query sulle raccolte.

> **Note**
>
> Attualmente stiamo sviluppando questi esempi di codice. Se vuoi contribuire con un esempio di codice (Java, Go, ecc.), apri una richiesta pull direttamente all'interno del GitHubrepository.

Argomenti

Python

Il seguente script di esempio utilizza il client AWS SDK for Python (Boto3), così come opensearch-py per Python per creare policy di crittografia, rete e accesso ai dati, creare una raccolta corrispondente e indicizzare alcuni dati di esempio.

Per installare le dipendenze richieste, eseguire i seguenti comandi:

```
pip install opensearch-py
pip install boto3
pip install botocore
pip install requests-aws4auth
```

All'interno dello script, sostituire l'elemento `Principal` con il nome della risorsa Amazon (ARN) dell'utente o il ruolo che sta firmando la richiesta. Facoltativamente, è possibile anche modificare la `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

Lo script di esempio seguente utilizza l'SDK per JavaScript in Node.js e il client opensearch-js per creare politiche di crittografiaJavaScript, rete e accesso ai dati, creare una raccolta corrispondente, creare un indice e indicizzare alcuni dati di esempio.

Per installare le dipendenze richieste, eseguire i seguenti comandi:

```
npm i aws-sdk
npm i aws4
npm i @opensearch-project/opensearch
```

All'interno dello script, sostituire l'elemento `Principal` con il nome della risorsa Amazon (ARN) dell'utente o il ruolo che sta firmando la richiesta. Facoltativamente, è possibile anche modificare la `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()
```

Utilizzo AWS CloudFormation per creare raccolte Amazon OpenSearch Serverless

Puoi utilizzarle AWS CloudFormation per creare risorse Amazon OpenSearch Serverless come raccolte, policy di sicurezza ed endpoint VPC. Per un CloudFormation riferimento completo su OpenSearch Serverless, consulta Amazon OpenSearch Serverless nella Guida per l'utente. AWS CloudFormation

Il seguente CloudFormation modello di esempio crea una semplice politica di accesso ai dati, una politica di rete e una politica di sicurezza, oltre a una raccolta corrispondente. È un buon modo per iniziare rapidamente con Amazon OpenSearch Serverless e fornire gli elementi necessari per creare e utilizzare una raccolta.

> **Important**
>
> Questo esempio utilizza l'accesso alla rete pubblica, che non è consigliato per i carichi di lavoro di produzione. Consigliamo di utilizzare l'accesso VPC per proteggere le raccolte. Per

ulteriori informazioni, consultare AWS::OpenSearchServerless::VpcEndpoint e the section called “Endpoint 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
```

Gestione dei limiti di capacità per Amazon OpenSearch Serverless

Con Amazon OpenSearch Serverless, non devi gestire la capacità da solo. OpenSearch Serverless ridimensiona automaticamente la capacità di elaborazione del tuo account in base al carico di lavoro corrente. La capacità di elaborazione serverless viene misurata in OpenSearch unità di calcolo (OCU). Ogni OCU è una combinazione di 6 GiB di memoria e della CPU virtuale (vCPU) corrispondente, oltre al trasferimento dei dati su Amazon S3. Per ulteriori informazioni sull'architettura disaccoppiata in Serverless, vedere. OpenSearch the section called “Come funziona”

Quando crei la tua prima raccolta, OpenSearch Serverless crea un'istanza totale di quattro OCU (due per l'indicizzazione e due per la ricerca). Queste OCU persistono sempre, anche in assenza di attività di indicizzazione o ricerca. Tutte le raccolte successive possono condividere questi OCU (ad eccezione delle raccolte con AWS KMS chiavi univoche, che istanziano il proprio set di quattro OCU). Se necessario, OpenSearch Serverless si ridimensiona automaticamente e aggiunge ulteriori OCU man mano che l'indicizzazione e l'utilizzo della ricerca aumentano. Quando il traffico sull'endpoint di raccolta diminuisce, la capacità si riduce al numero minimo di OCU richiesto per la dimensione dei dati. Al massimo, verrà ridimensionato a 1 OCU [0,5 OCU x 2] per l'indicizzazione e 1 OCU [0,5 OCU x 2] per la ricerca.

Per le raccolte di ricerca e di ricerca vettoriale, tutti i dati vengono archiviati su indici caldi per garantire tempi di risposta rapidi alle query. Le raccolte di serie temporali utilizzano una combinazione di archiviazione a caldo e a caldo, conservando i dati più recenti in una memoria a caldo per ottimizzare i tempi di risposta alle query per i dati a cui si accede più frequentemente. Per ulteriori informazioni, consulta the section called “Scelta di un tipo di raccolta”.

> **Note**
>
> Una raccolta di ricerca vettoriale non può condividere OCU con raccolte di ricerca e di serie temporali, anche se la raccolta di ricerca vettoriale utilizza la stessa chiave KMS delle raccolte di ricerca o di serie temporali. Verrà creato un nuovo set di OCU per la tua prima raccolta vettoriale. Gli OCU delle raccolte vettoriali sono condivisi tra le stesse raccolte di chiavi KMS.

Per gestire la capacità delle raccolte e controllare i costi, è possibile specificare la capacità massima complessiva di indicizzazione e ricerca per l'account corrente e la regione, mentre OpenSearch Serverless ridimensiona automaticamente le risorse di raccolta in base a queste specifiche.

Poiché la capacità di indicizzazione e di ricerca è scalabile separatamente, è necessario specificare i limiti a livello di account per ciascuna di esse:

- Capacità di indicizzazione massima: OpenSearch Serverless può aumentare la capacità di indicizzazione fino a questo numero di OCU.
- Capacità di ricerca massima: OpenSearch Serverless può aumentare la capacità di ricerca fino a questo numero di OCU.

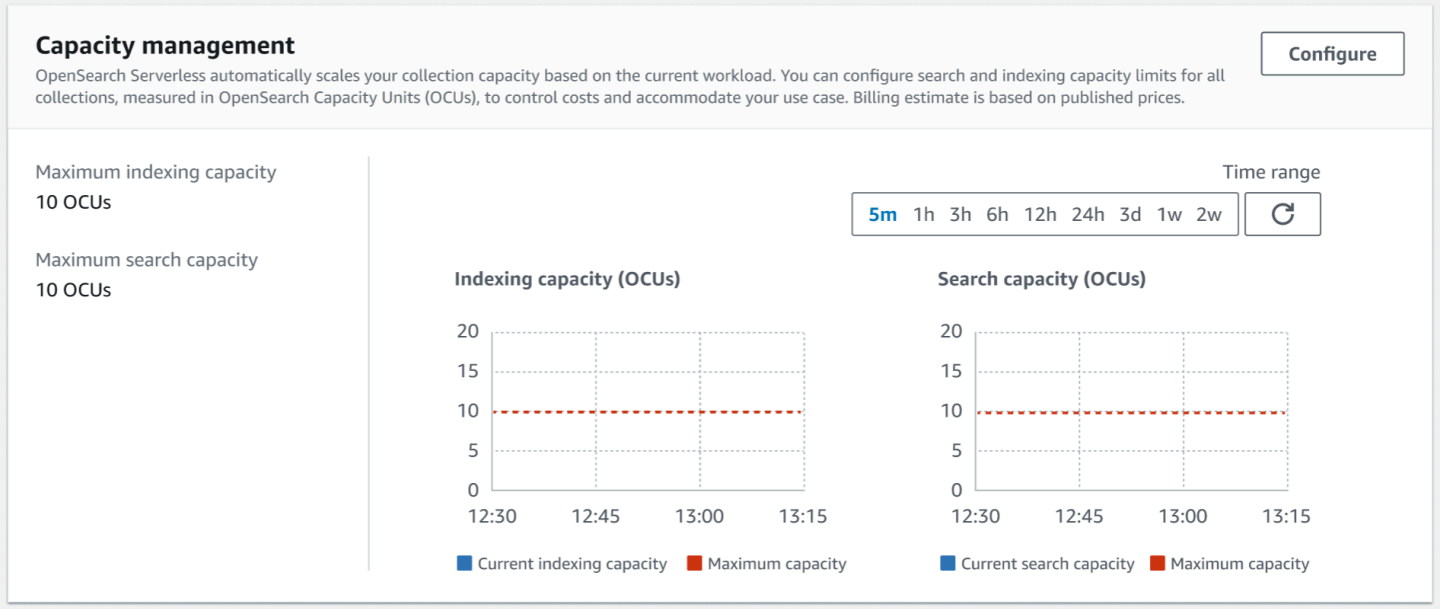
> **Note**
>
> Al momento, le impostazioni relative alla capacità si applicano solo a livello di account. Non è possibile configurare limiti di capacità per ciascuna raccolta.

L'obiettivo è quello di garantire che la capacità massima sia sufficientemente elevata da gestire i picchi del carico di lavoro. In base alle impostazioni, OpenSearch Serverless ridimensiona automaticamente il numero di OCU per le raccolte per elaborare il carico di lavoro di indicizzazione e ricerca.

Argomenti

Configurazione delle impostazioni di capacità

Per configurare le impostazioni di capacità nella console Serverless, espandi OpenSearch Serverless nel riquadro di navigazione a sinistra e seleziona Dashboard. In Capacity management (Gestione della capacità) specifica la capacità massima di indicizzazione e ricerca:



Per configurare la capacità utilizzando AWS CLI, invia una UpdateAccountSettingsrichiesta:

```
aws opensearchserverless update-account-settings \
    --capacity-limits '{ "maxIndexingCapacityInOCU": 8,"maxSearchCapacityInOCU": 9 }'
```

Limiti di capacità massima

Per tutti e tre i tipi di raccolte, la capacità massima predefinita è di 10 OCU per l'indicizzazione e 10 OCU per la ricerca. La capacità minima consentita per un account è di 1 OCU [0,5 OCU x 2] per l'indicizzazione e 1 OCU [0,5 OCU x 2] per la ricerca. Per tutte le raccolte, la capacità massima consentita è di 200 OCU per l'indicizzazione e 200 OCU per la ricerca. È possibile configurare il conteggio delle OCU in modo che sia qualsiasi numero compreso tra 1 e la capacità massima consentita, in multipli di 2.

Ogni OCU include uno storage temporaneo a caldo sufficiente per 120 GiB di dati di indice. OpenSearch Serverless supporta fino a 1 TiB di dati per indice nelle raccolte di ricerca e di ricerca vettoriale e 10 TiB di hot data per indice in una raccolta di serie temporali. Per le raccolte di serie temporali, puoi comunque inserire più dati, che possono essere archiviati come dati «warm data» in S3.

Per un elenco di tutte le quote, vedi OpenSearch Quote serverless.

Monitoraggio dell'utilizzo della capacità

Puoi monitorare le CloudWatch metriche a `Indexing0CU` livello `Search0CU` di account per capire come stanno scalando le tue collezioni. Ti consigliamo di configurare allarmi che possono avvisarti se il tuo account si sta avvicinando a una soglia per i parametri relativi alla capacità, in modo da poter adattare di conseguenza le impostazioni di capacità.

Puoi anche utilizzare questi parametri per determinare se le impostazioni di capacità massima sono appropriate o se è necessario adeguarle. Analizza questi parametri per concentrarti sull'ottimizzazione dell'efficienza delle tue raccolte. Per ulteriori informazioni sulle metriche a cui OpenSearch Serverless invia, consulta. CloudWatch the section called “Monitoraggio senza server OpenSearch ”

Inserimento di dati in raccolte Amazon Serverless OpenSearch

Queste sezioni forniscono dettagli sulle pipeline di importazione supportate per l'inserimento di dati nelle raccolte Amazon OpenSearch Serverless. Esse riguardano anche alcuni client che puoi utilizzare per interagire con le operazioni dell'API. OpenSearch I tuoi client devono essere compatibili con OpenSearch 2.x per integrarsi con OpenSearch Serverless.

Argomenti

- Autorizzazioni minime richieste
- OpenSearch Ingestione
- Fluent Bit
- Amazon Data Firehose
- Fluentd
- Go
- Java
- JavaScript
- Logstash
- Python
- Ruby

- Firma delle richieste HTTP con altri client

Autorizzazioni minime richieste

Per inserire dati in una raccolta OpenSearch Serverless, il responsabile che scrive i dati deve disporre delle seguenti autorizzazioni minime assegnate in una politica di accesso ai dati:

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/target-collection/logs"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:WriteDocument",
               "aoss:UpdateIndex"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/my-user"
      ]
   }
]
```

Le autorizzazioni possono essere più ampie se prevedi di scrivere su indici aggiuntivi. Ad esempio, anziché specificare un singolo indice di destinazione, è possibile consentire l'autorizzazione a tutti gli indici (index/*target-collection*/*) o a un sottoinsieme di indici (index/*target-collection*/*logs**).

Per un riferimento a tutte le operazioni OpenSearch API disponibili e alle relative autorizzazioni, consulta. the section called “Operazioni e plug-in supportati”

OpenSearch Ingestione

Invece di utilizzare un client di terze parti per inviare dati direttamente a una raccolta OpenSearch Serverless, puoi utilizzare Amazon OpenSearch Ingestion. Puoi configurare i tuoi produttori di dati

per inviare dati a OpenSearch Ingestion, che li consegna automaticamente alla raccolta specificata. Puoi anche configurare OpenSearch Ingestion per trasformare i dati prima di consegnarli. Per ulteriori informazioni, consulta OpenSearch Ingestione di Amazon.

Una pipeline OpenSearch di Ingestion necessita dell'autorizzazione per scrivere su una raccolta OpenSearch Serverless configurata come sink. Queste autorizzazioni includono la possibilità di descrivere la raccolta e inviarle richieste HTTP. Per istruzioni su come utilizzare OpenSearch Ingestion per aggiungere dati a una raccolta, consulta. the section called “Concedere alle pipeline l'accesso alle raccolte”

Per iniziare a usare OpenSearch Ingestion, consulta. the section called “Tutorial: inserisci dati in una raccolta”

Fluent Bit

È possibile utilizzare Fluent Bit image e il plug-in di OpenSearch output AWS per inserire dati in raccolte Serverless. OpenSearch

> **Note**
>
> È necessario disporre della versione 2.30.0 o successiva dell'immagine AWS for Fluent Bit per l'integrazione con Serverless. OpenSearch

Configurazione di esempio:

Questa sezione di output di esempio del file di configurazione mostra come utilizzare una raccolta OpenSearch Serverless come destinazione. L'aggiunta importante è il parametro `AWS_Service_Name`, che è `aoss`. `Host` è l'endpoint della raccolta.

```
[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 supporta OpenSearch Serverless come destinazione di consegna. Per istruzioni su come inviare dati in OpenSearch Serverless, consulta Creating a Kinesis Data Firehose Delivery Stream e OpenSearch Choose Serverless for Your Destination nella Amazon Data Firehose Developer Guide.

Il ruolo IAM che fornisci a Firehose per la consegna deve essere specificato all'interno di una policy di accesso ai dati con l'autorizzazione `aoss:WriteDocument` minima per la raccolta di destinazione e devi disporre di un indice preesistente a cui inviare i dati. Per ulteriori informazioni, consulta the section called “Autorizzazioni minime richieste”.

Prima di inviare dati a OpenSearch Serverless, potrebbe essere necessario eseguire delle trasformazioni sui dati. Per ulteriori informazioni su come usare le funzioni Lambda per completare questa attività, consultare Trasformazione dei dati di Amazon Kinesis Data Firehose nella stessa guida.

Fluentd

È possibile utilizzare il OpenSearch plug-in Fluentd per raccogliere dati dall'infrastruttura, dai contenitori e dai dispositivi di rete e inviarli alle raccolte Serverless. OpenSearch Calyptia mantiene una distribuzione di Fluentd che contiene tutte le dipendenze a valle di Ruby e SSL.

Per utilizzare Fluentd per inviare dati a Serverless OpenSearch

1. Scarica la versione 1.4.2 o successiva di Calyptia Fluentd dalla pagina https://www.fluentd.org/download. Questa versione include il OpenSearch plug-in di default, che supporta Serverless. OpenSearch
2. Installare il pacchetto . Segui le istruzioni nella documentazione di Fluentd in base al tuo sistema operativo:

   - Red Hat Enterprise Linux / CentOS / Amazon Linux
   - Debian / Ubuntu
   - Windows

   - MacOSX

3. Aggiungi una configurazione che invia dati a OpenSearch Serverless. Questa configurazione di esempio invia il messaggio "test" a una singola raccolta. Completa le seguenti operazioni:

   - Per`host`, specifica l'endpoint della tua raccolta OpenSearch Serverless.
   - Per `aws_service_name`, specificare `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. Esegui Calyptia Fluentd per iniziare a inviare dati alla raccolta. Ad esempio, su Mac puoi esegui il seguente comando:

```
sudo launchctl load /Library/LaunchDaemons/calyptia-fluentd.plist
```

Go

Il codice di esempio seguente utilizza il client opensearch-go per Go per stabilire una connessione sicura alla raccolta OpenSearch Serverless specificata e creare un singolo indice. È necessario fornire valori per `region` e `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

Il codice di esempio seguente utilizza il client opensearch-java per Java per stabilire una connessione sicura alla raccolta OpenSearch Serverless specificata e creare un singolo indice. È necessario fornire valori per `region` e `host`.

La differenza importante rispetto ai domini di OpenSearch servizio è il nome del servizio (anziché). `aoss` `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();
```

Il codice di esempio seguente stabilisce nuovamente una connessione sicura e quindi esegue la ricerca in un indice.

```
import org.opensearch.client.opensearch.OpenSearchClient;

SdkHttpClient httpClient = ApacheHttpClient.builder().build();

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()
    )
);

Response response = client.generic()
    .execute(
        Requests.builder()
            .endpoint("/" + "users" + "/_search?typed_keys=true")
            .method("GET")
            .json("{"
                + "    \"query\": {"
                + "        \"match_all\": {}"
                + "    }"
                + "}")
            .build());

httpClient.close();
```

JavaScript

Il codice di esempio seguente utilizza il client opensearch-js per JavaScript stabilire una connessione sicura alla raccolta OpenSearch Serverless specificata, creare un singolo indice, aggiungere un documento ed eliminare l'indice. È necessario fornire valori per `node` e `region`.

La differenza importante rispetto ai domini di OpenSearch servizio è il nome del servizio (anziché). `aoss` `es`

Version 3

Questo esempio utilizza la versione 3 dell'SDK for JavaScript in 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

Questo esempio utilizza la versione 2 dell'SDK for JavaScript in 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

È possibile utilizzare il OpenSearch plug-in Logstash per pubblicare i log nelle raccolte Serverless. OpenSearch

Per utilizzare Logstash per inviare dati a Serverless OpenSearch

1. Installa la versione 2.0.0 o successiva del logstash-output-opensearchplug-in utilizzando Docker o Linux.

   Docker

   Docker ospita il software Logstash OSS con il plug-in di OpenSearch output preinstallato: opensearchproject/ -output-plugin. logstash-oss-with-opensearch Puoi estrarre l'immagine come qualsiasi altra immagine:

   ```
   docker pull opensearchproject/logstash-oss-with-opensearch-output-plugin:latest
   ```

   Linux

   Per prima cosa, se ancora non è stato fatto, installa la versione più recente di Logstash. Quindi, installa la versione 2.0.0 del plug-in di output:

   ```
   cd logstash-8.5.0/
   bin/logstash-plugin install --version 2.0.0 logstash-output-opensearch
   ```

   Se il plug-in è già installato, aggiornalo alla versione più recente:

   ```
   bin/logstash-plugin update logstash-output-opensearch
   ```

   A partire dalla versione 2.0.0 del plugin, l'SDK utilizza la versione 3. AWS Se utilizzi una versione di Logstash precedente alla 8.4.0, devi rimuovere tutti i plugin AWS preinstallati e installare il plug-in: `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. Affinché il plugin OpenSearch di output funzioni con OpenSearch Serverless, devi apportare le seguenti modifiche alla sezione di output di logstash.conf: `opensearch`

   - Specifica `aoss` come `service_name` in `auth_type`.
   - Specifica l'endpoint di raccolta per `hosts`.
   - Aggiungi i parametri `default_server_major_version` e `legacy_template`. Questi parametri sono necessari per il funzionamento del plugin con Serverless. OpenSearch

```
output {
  opensearch {
    hosts => "collection-endpoint:443"
    auth_type => {
      ...
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

Questo file di configurazione di esempio prende l'input dai file in un bucket S3 e li invia a una OpenSearch raccolta 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. Quindi, esegui Logstash con la nuova configurazione per testare il plug-in:

```
bin/logstash -f config/test-plugin.conf
```

Python

Il codice di esempio seguente utilizza il client opensearch-py per Python per stabilire una connessione sicura alla raccolta OpenSearch Serverless specificata, creare un singolo indice e cercare nell'indice. È necessario fornire valori per `region` e `host`.

La differenza importante rispetto ai domini di OpenSearch servizio è il nome del servizio (anziché). `aoss` `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` gemma fornisce l'accesso OpenSearch immediato a Serverless, insieme a OpenSearch Service. Ha tutte le funzionalità del client opensearch-ruby perché è una dipendenza di questo pacchetto gem.

Quando si crea un'istanza del firmatario Sigv4, specifica `aoss` come nome del servizio:

```
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 delle richieste HTTP con altri client

I seguenti requisiti si applicano quando si firmano le richieste nelle raccolte OpenSearch Serverless quando si creano richieste HTTP con altri client.

- È necessario specificare il nome del servizio come `aoss`.
- L'intestazione `x-amz-content-sha256` è obbligatoria per tutte le richieste di AWS Signature Version 4. Fornisce un hash del payload di richiesta. Se c'è un payload di richiesta, imposta il valore sul relativo hash crittografico (SHA256) Secure Hash Algorithm (SHA). Se non c'è alcun payload di richiesta, imposta il valore su `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`, che è l'hash di una stringa vuota.

Argomenti

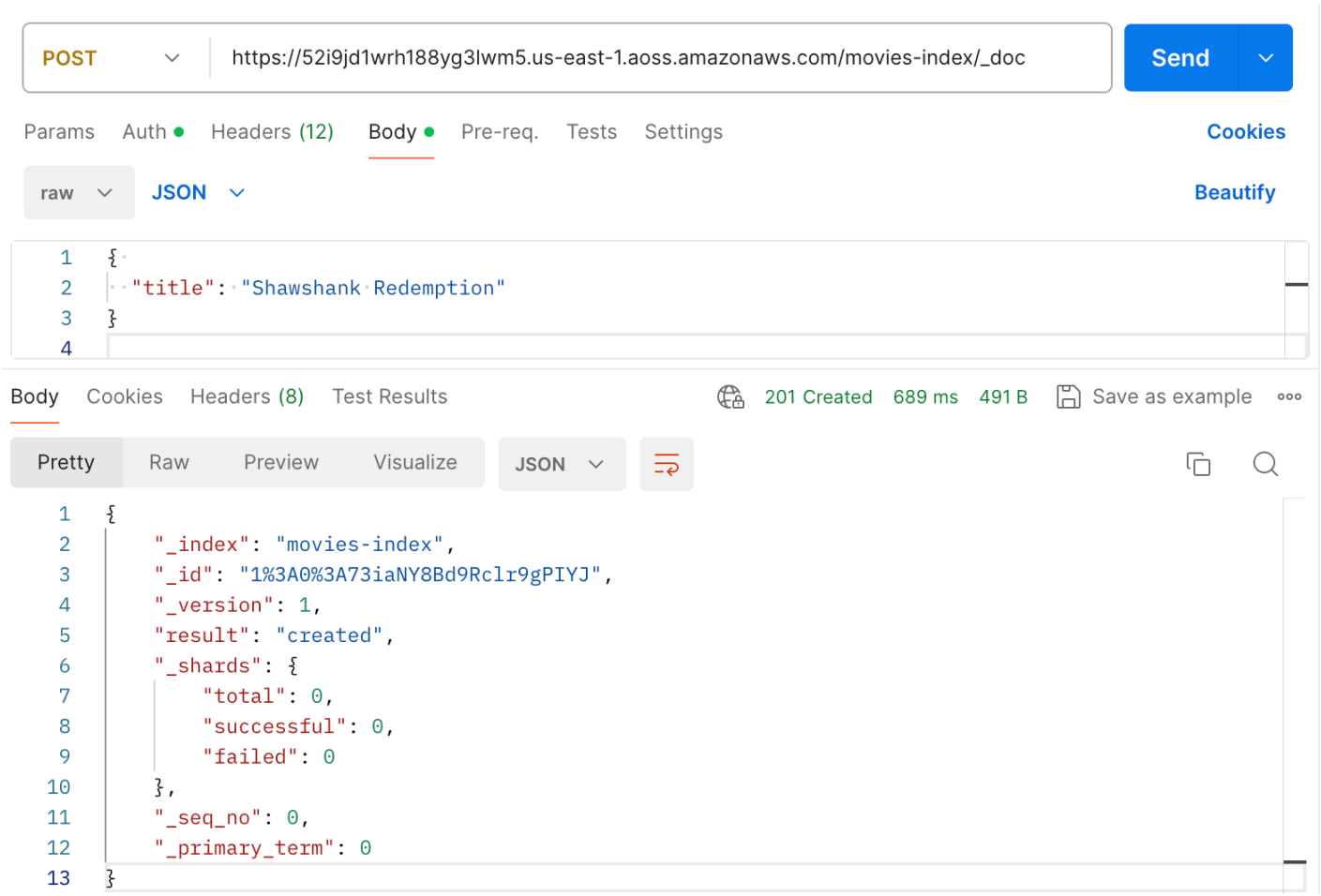
Indicizzazione con cURL

La seguente richiesta di esempio utilizza la Client URL Request Library (cURL) per inviare un singolo documento a un indice denominato `movies-index` all'interno di una raccolta:

```
curl -XPOST \
    --user "$AWS_ACCESS_KEY_ID":"$AWS_SECRET_ACCESS_KEY" \
    --aws-sigv4 "aws:amz:us-east-1:aoss" \
    --header "x-amz-content-sha256: $REQUEST_PAYLOAD_SHA_HASH" \
    --header "x-amz-security-token: $AWS_SESSION_TOKEN" \
    "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com/movies-index/_doc" \
    -H "Content-Type: application/json" -d '{"title": "Shawshank Redemption"}'
```

Indicizzazione con Postman

L'immagine seguente mostra come inviare una richiesta a una raccolta utilizzando Postman. Per istruzioni sull'autenticazione, consulta il flusso di lavoro di autenticazione Authenticate with AWS Signature in Postman.



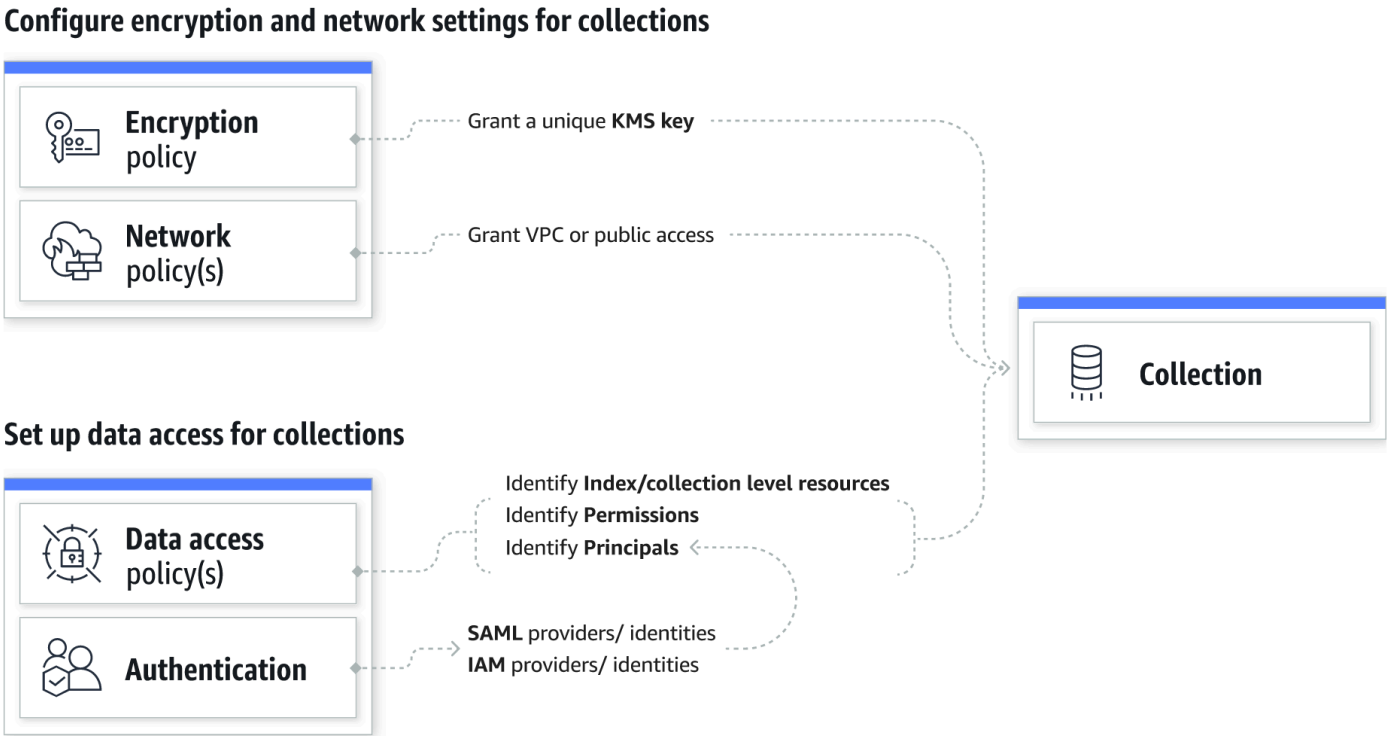
Panoramica della sicurezza in Amazon OpenSearch Serverless

La sicurezza in Amazon OpenSearch Serverless si differenzia fondamentalmente dalla sicurezza in Amazon OpenSearch Service nei seguenti modi:

Funzionalità	OpenSearch Servizio	OpenSearch Senza server
Controllo dell'accesso ai dati	L'accesso ai dati è determinato dalle policy IAM e dal controllo granulare degli accessi.	L'accesso ai dati è determinato dalle policy di accesso ai dati.
Crittografia dei dati inattivi	La crittografia dei dati inattivi è facoltativa per i domini.	La crittografia dei dati inattivi è obbligatoria per le raccolte.

Funzionalità	OpenSearch Servizio	OpenSearch Senza server
Configurazione e amministrazione della sicurezza	È necessario configurare la rete, la crittografia e l'accesso ai dati singolarmente per ogni dominio.	Puoi utilizzare le policy di sicurezza per gestire le impostazioni di sicurezza per più raccolte su larga scala.

Il diagramma seguente illustra i componenti di sicurezza che costituiscono una raccolta funzionale. Una raccolta deve avere una chiave di crittografia assegnata, impostazioni di accesso alla rete e una policy di accesso ai dati corrispondente che garantisca l'autorizzazione alle relative risorse.



Argomenti

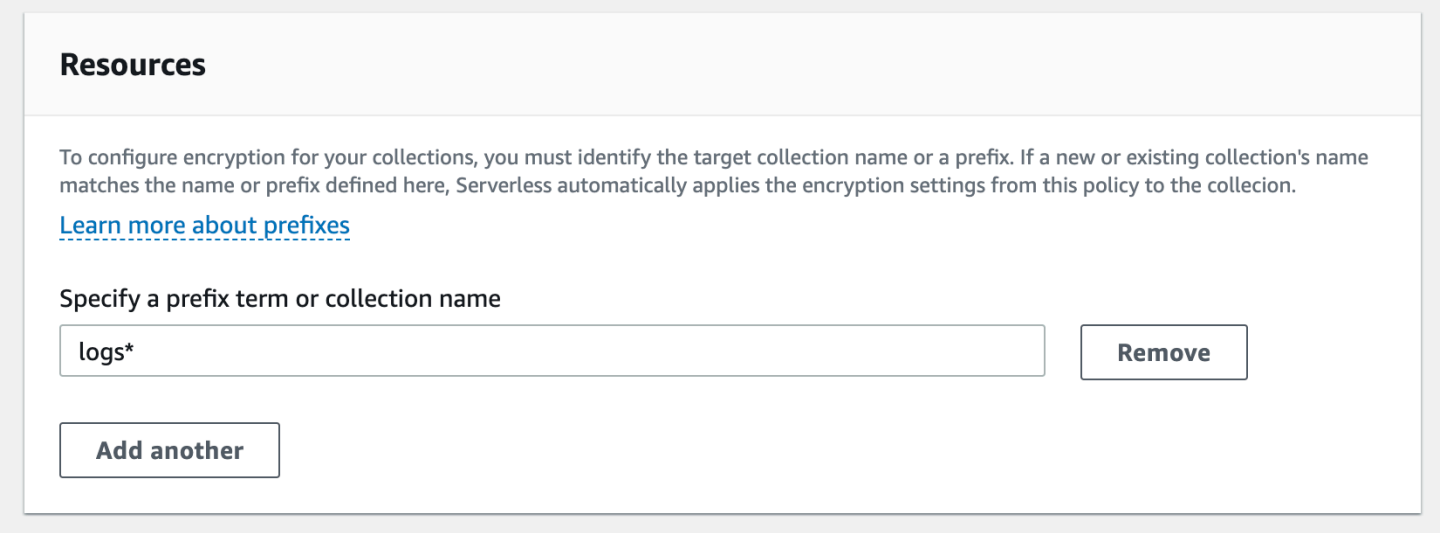
- Policy di crittografia
- Policy di rete
- Policy di accesso ai dati
- Autenticazione IAM e SAML
- Sicurezza dell'infrastruttura
- Guida introduttiva alla sicurezza in Amazon OpenSearch Serverless

- Identity and Access Management per Amazon OpenSearch Serverless
- Crittografia in Amazon OpenSearch Serverless
- Accesso alla rete per Amazon OpenSearch Serverless
- Controllo dell'accesso ai dati per Amazon OpenSearch Serverless
- Accedi ad Amazon OpenSearch Serverless utilizzando un endpoint di interfaccia ()AWS PrivateLink
- Autenticazione SAML per Amazon Serverless OpenSearch
- Convalida della conformità per Amazon Serverless OpenSearch

Policy di crittografia

Le politiche di crittografia definiscono se le raccolte sono crittografate con una chiave Chiave di proprietà di AWS o con una chiave gestita dal cliente. Le policy di crittografia sono costituite da due componenti: un modello di risorse e una chiave di crittografia. Il modello di risorse definisce a quale raccolta o raccolte si applica la policy. La chiave di crittografia determina il modo in cui verranno protette le raccolte associate.

Per applicare una policy a più raccolte, includi un carattere jolly (*) nella regola della policy. Ad esempio, la seguente policy si applica a tutte le raccolte i cui nomi iniziano con "log".

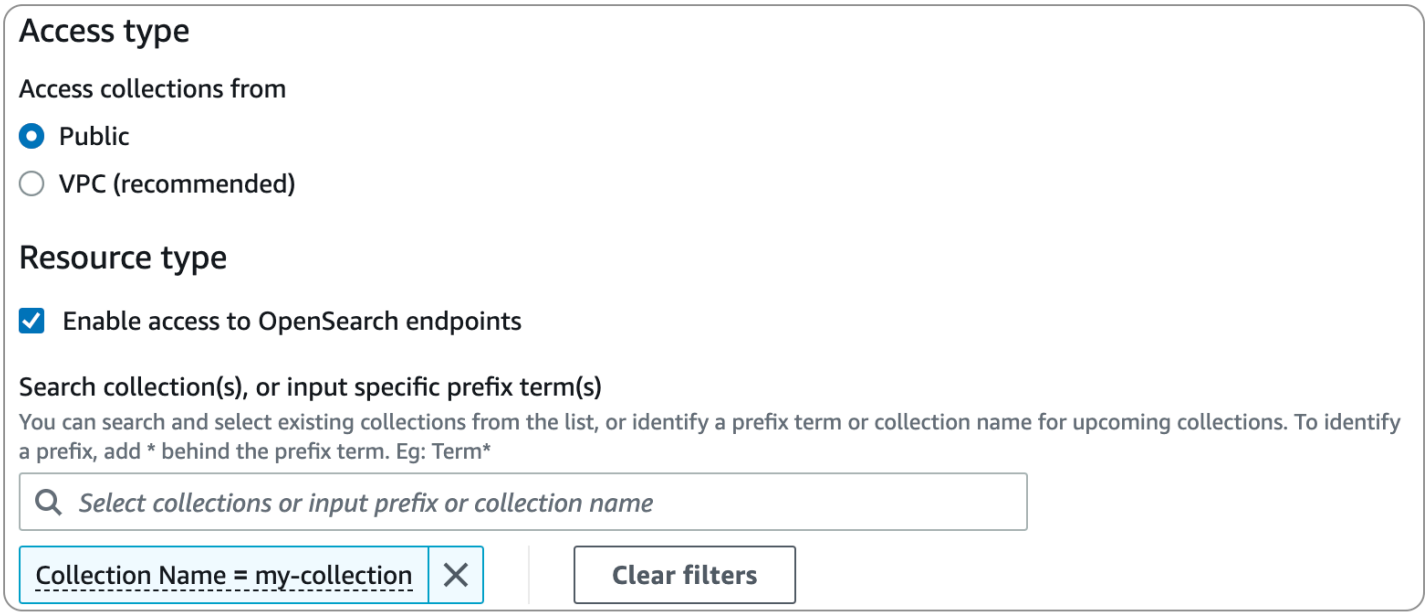


Le policy di crittografia semplificano il processo di creazione e gestione delle raccolte, soprattutto quando lo si fa a livello di programmazione. È possibile creare una raccolta semplicemente specificando un nome e al momento della creazione viene assegnata automaticamente una chiave di crittografia.

Policy di rete

Le politiche di rete definiscono se le raccolte sono accessibili privatamente o tramite Internet da reti pubbliche. È possibile accedere alle raccolte private tramite endpoint OpenSearch VPC gestiti senza server o tramite dispositivi specifici Servizi AWS come Amazon Bedrock che utilizzano l'accesso privato.Servizio AWS Proprio come le policy di crittografia, le policy di rete possono essere applicate a più raccolte e questo consente di gestire l'accesso alla rete per molte raccolte su larga scala.

Le policy di rete sono costituite da due componenti: un tipo di accesso e un tipo di risorsa. Il tipo di accesso può essere pubblico o privato. Il tipo di risorsa determina se l'accesso scelto si applica all'endpoint di raccolta, all'endpoint OpenSearch Dashboards o a entrambi.



Se prevedi di configurare l'accesso VPC all'interno di una policy di rete, devi prima creare uno o più endpoint VPC gestiti OpenSearch senza server. Questi endpoint ti consentono di accedere a OpenSearch Serverless come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect

L'accesso privato a Servizi AWS può essere applicato solo all'endpoint della raccolta, non all' OpenSearch endpoint Dashboards. OpenSearch Servizi AWS non può essere concesso l'accesso alle dashboard. OpenSearch

Policy di accesso ai dati

Le policy di accesso ai dati definiscono il modo in cui gli utenti accedono ai dati all'interno delle raccolte. Le policy di accesso ai dati consentono di gestire le raccolte su larga scala assegnando

automaticamente autorizzazioni di accesso a raccolte e indici che corrispondono a uno schema specifico. È possibile applicare più policy a una singola risorsa.

Le policy di accesso ai dati sono costituite da un insieme di regole, ciascuna con tre componenti: un tipo di risorsa, le risorse concesse e un elenco delle autorizzazioni. Il tipo di risorsa può essere una raccolta o un indice. Le risorse concesse possono essere nomi di raccolte/indici o modelli con un carattere jolly (*). L'elenco delle autorizzazioni specifica a quali operazioni OpenSearch API la policy concede l'accesso. Inoltre, la policy contiene un elenco di principali, che specificano i ruoli IAM, gli utenti e le identità SAML a cui concedere l'accesso.

Per ulteriori informazioni sul formato di una policy di accesso ai dati, consulta la sintassi della policy.

Prima di creare una policy di accesso ai dati, è necessario disporre di uno o più utenti o ruoli IAM, o identità SAML, a cui fornire l'accesso nella policy. Per ulteriori informazioni, consulta la prossima sezione.

Autenticazione IAM e SAML

I principali IAM e le identità SAML sono uno degli elementi costitutivi di una policy di accesso ai dati. All'interno dell'istruzione `principal` di una policy di accesso, è possibile includere ruoli IAM, utenti e identità SAML. A questi principali vengono quindi concesse le autorizzazioni specificate nelle regole delle policy associate.

```
[
   {
      "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"
      ]
   }
]
```

L'autenticazione SAML viene configurata direttamente all'interno di Serverless. OpenSearch Per ulteriori informazioni, consulta the section called “Autenticazione SAML”.

Sicurezza dell'infrastruttura

Amazon OpenSearch Serverless è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon OpenSearch Serverless attraverso la rete. I client devono supportare Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3. Per un elenco dei codici supportati per TLS 1.3, consulta i protocolli e le cifrari TLS nella documentazione di Elastic Load Balancing.

Inoltre, è necessario firmare le richieste utilizzando un ID di chiave di accesso e una chiave di accesso segreta associata a un'entità IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Guida introduttiva alla sicurezza in Amazon OpenSearch Serverless

I seguenti tutorial ti aiutano a iniziare a usare Amazon OpenSearch Serverless. Entrambi i tutorial completano le stesse fasi di base, ma uno utilizza la console mentre l'altro utilizza la AWS CLI.

Tieni presente che i casi d'uso in questi tutorial sono semplificati. Le policy di rete e di sicurezza sono relativamente aperte. Nei carichi di lavoro di produzione, si consiglia di configurare funzionalità di

sicurezza più affidabili come l'autenticazione SAML, l'accesso al VPC e le policy restrittive di accesso ai dati.

Argomenti

- Tutorial: Guida introduttiva alla sicurezza in Amazon OpenSearch Serverless (console)
- Tutorial: Guida introduttiva alla sicurezza in Amazon OpenSearch Serverless (CLI)

Tutorial: Guida introduttiva alla sicurezza in Amazon OpenSearch Serverless (console)

Questo tutorial illustra i passaggi di base per creare e gestire le policy di sicurezza utilizzando la console Amazon OpenSearch Serverless.

In questo tutorial completerai le seguenti fasi:

1. Configurazione delle autorizzazioni
2. Creazione di una policy di crittografia
3. Creazione di una policy di rete
4. Configurazione di una policy di accesso ai dati
5. Creazione di una raccolta
6. Caricamento e ricerca dei dati

Questo tutorial ti guiderà nella creazione di una raccolta utilizzando la AWS Management Console. Per le stesse fasi utilizzando la AWS CLI, consulta la sezione the section called “Tutorial: nozioni di base sulla sicurezza (CLI)”.

Fase 1: configurazione delle autorizzazioni

> **Note**
>
> Puoi saltare questa fase se stai già utilizzando una policy più ampia basata sull'identità, ad esempio `Action":"aoss:*"` o `Action":"*"`. Negli ambienti di produzione, tuttavia, si consiglia di seguire il principio del privilegio minimo e di assegnare solo le autorizzazioni minime necessarie per completare un'attività.

Per completare questo tutorial è necessario disporre delle autorizzazioni IAM corrette. L'utente o il ruolo devono avere una policy basata sull'identità allegata con le seguenti autorizzazioni minime:

```
{
  "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": "*"
    }
  ]
}
```

Per un elenco completo delle autorizzazioni OpenSearch Serverless, consulta. the section called “Identity and Access Management”

Fase 2: creazione di una policy di crittografia

Le politiche di crittografia specificano la AWS KMS chiave che OpenSearch Serverless utilizzerà per crittografare la raccolta. È possibile crittografare le raccolte con una Chiave gestita da AWS o una chiave diversa. Per semplicità, in questo tutorial crittograferemo la nostra raccolta con una Chiave gestita da AWS.

Creazione di una policy di crittografia

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Espandi Serverless nel pannello di navigazione a sinistra e scegli Encryption policies (Policy di crittografia).
3. Scegli Create encryption policy (Crea policy di crittografia).
4. Nomina la policy books-policy. Nella descrizione, inserisci Crittografia per una raccolta di libri.

5. In Resources (Risorse), inserisci books (libri), che è il nome che darai alla tua raccolta. Se si desidera essere più generici, è possibile includere un asterisco (`books*`) per applicare la policy a tutte le raccolte che iniziano con la parola "books".
6. Per la crittografia, mantieni selezionata l'opzione Usa chiave AWS di proprietà.
7. Scegli Crea.

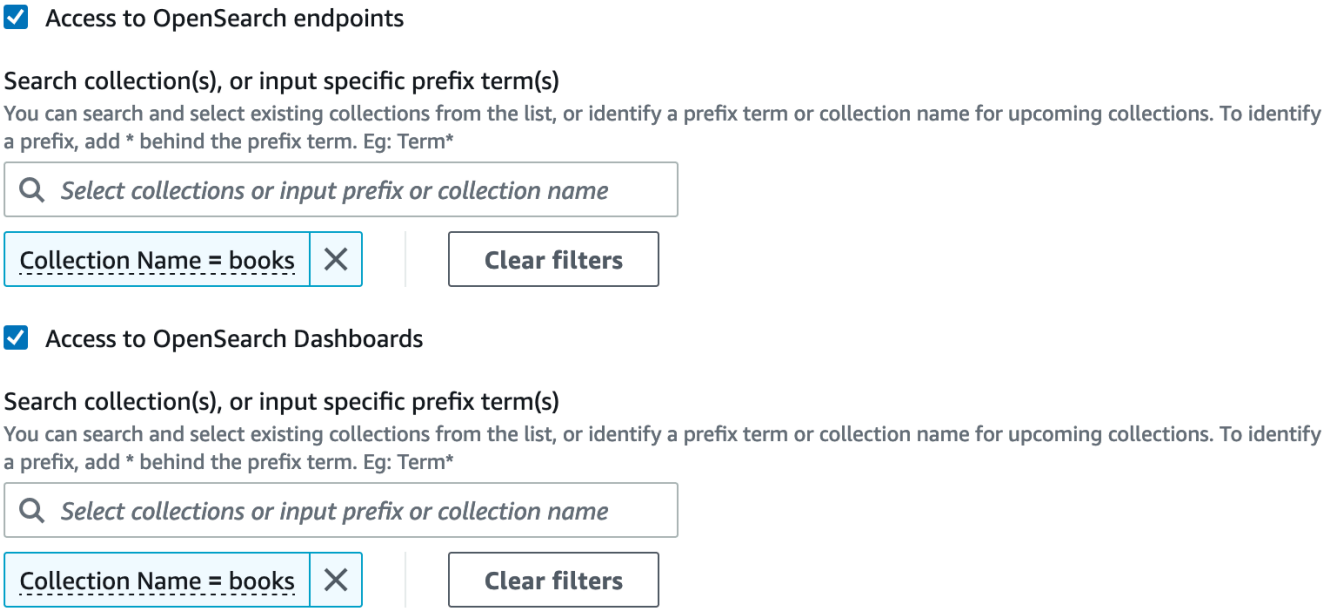
Fase 3: Creare una politica di rete

Le politiche di rete determinano se la raccolta è accessibile su Internet dalle reti pubbliche o se è necessario accedervi tramite endpoint VPC OpenSearch gestiti senza server. In questo tutorial, configureremo l'accesso pubblico.

Creazione di una policy di rete

1. Nel pannello di navigazione a sinistra, scegli Network policies (Policy di rete) e Create network policy (Crea policy di rete).
2. Nomina la policy books-policy. Nella descrizione, inserisci Policy di rete per una raccolta di libri.
3. Nella Regola 1, nomina la regola Accesso pubblico per una raccolta di libri.
4. Per semplicità, in questo tutorial configureremo l'accesso pubblico alla raccolta books. Per il tipo di accesso, seleziona Public (Pubblico).
5. Accederemo alla raccolta da Dashboards. OpenSearch Per fare ciò, devi configurare l'accesso alla rete per le dashboard e l' OpenSearch endpoint, altrimenti le dashboard non funzioneranno.

   Per il tipo di risorsa, abilita sia Access to OpenSearch endpoint che Access to Dashboards. OpenSearch
6. In entrambe le caselle di input, inserisci Collection Name = books (Nome raccolta = libri). Questa impostazione riduce l'ambito della policy in modo che si applichi solo a una singola raccolta (`books`). La tua regola dovrebbe assomigliare a questa:



7. Scegli Crea.

Passaggio 4: Creare una politica di accesso ai dati

I dati della raccolta non saranno accessibili finché non configuri l'accesso ai dati. Le policy di accesso ai dati sono separate dalla policy basata sull'identità IAM configurata nella fase 1. Consentono agli utenti di accedere ai dati effettivi all'interno di una raccolta.

In questo tutorial, forniremo a un singolo utente le autorizzazioni necessarie per indicizzare i dati nella raccolta denominata books.

Creazione di una policy di accesso ai dati

1. Nel pannello di navigazione a sinistra, scegli Data access policies (Policy di accesso ai dati) e Create access policy (Crea policy di accesso).
2. Nomina la policy books-policy. Nella descrizione, inserisci policy di accesso ai dati per la raccolta di libri.
3. Per il metodo di definizione della policy seleziona JSON e incolla la seguente policy nell'editor JSON.

   Sostituisci l'ARN principale con l'ARN dell'account che utilizzerai per accedere alle OpenSearch dashboard e ai dati degli indici.

```
[
```

```
   {
      "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"
      ]
   }
]
```

Questa policy fornisce a un singolo utente le autorizzazioni minime necessarie per creare un indice nella raccolta books, indicizzare alcuni dati e cercarli.

4. Scegli Crea.

Fase 5: Creare una raccolta

Ora che hai configurato la crittografia e le policy di rete, puoi creare una raccolta corrispondente e le impostazioni di sicurezza verranno applicate automaticamente ad essa.

Per creare una raccolta OpenSearch Serverless

1. Scegli Collections (Raccolte) nel pannello di navigazione a sinistra e scegli Create collection (Crea raccolta).
2. Nomina la raccolta books.
3. Per il tipo di raccolta, scegli Search (Cerca).
4. In Encryption, OpenSearch Serverless informa che il nome della raccolta corrisponde alla `books-policy` politica di crittografia.

5. In Impostazioni di accesso alla rete, OpenSearch Serverless informa che il nome della raccolta corrisponde alla politica di rete. `books-policy`
6. Seleziona Avanti.
7. In Opzioni della politica di accesso ai dati, OpenSearch Serverless ti informa che il nome della raccolta corrisponde alla politica di accesso ai `books-policy` dati.
8. Seleziona Avanti.
9. Rivedi la configurazione della raccolta e scegli Submit (Invia). Generalmente, l'inizializzazione delle raccolte richiede meno di un minuto.

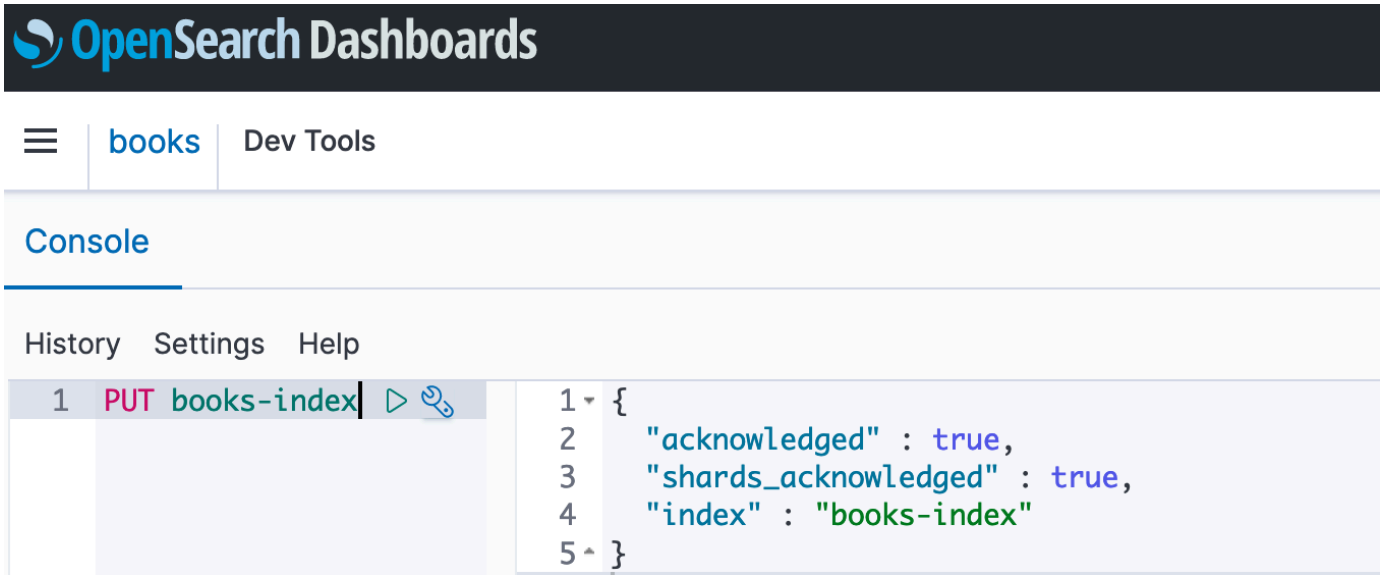
Fase 6: caricamento e ricerca dei dati

Puoi caricare dati in una raccolta OpenSearch Serverless utilizzando Postman o curl. Per brevità, questi esempi utilizzano Dev Tools all'interno della console Dashboards. OpenSearch

Indicizzazione e ricerca di dati in una raccolta

1. Scegli Collections (Raccolte) nel pannello di navigazione a sinistra e scegli la raccolta books per aprirne la pagina dei dettagli.
2. Scegli l'URL delle OpenSearch dashboard per la raccolta. L'URL assume il formato `https://collection-id.us-east-1.aoss.amazonaws.com/_dashboards`.
3. Accedi alle OpenSearch dashboard utilizzando le chiavi di AWS accesso e segrete per il principale che hai specificato nella politica di accesso ai dati.
4. All'interno di OpenSearch Dashboards, apri il menu di navigazione a sinistra e scegli Dev Tools.
5. Per creare un singolo indice chiamato books-index, esegui il seguente comando:

```
PUT books-index
```



6. Per indicizzare un singolo documento in books-index, esegui il seguente comando:

```
PUT books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

7. Per cercare dati nelle OpenSearch dashboard, devi configurare almeno un modello di indice. OpenSearch utilizza questi modelli per identificare gli indici da analizzare. Apri il menu principale di Dashboards, scegliere Gestione stack, scegliere Modelli di indice, quindi scegliere Crea modello di indice. Per questo tutorial, inserisci books-index.
8. Scegliere Fase successiva quindi selezionare Crea modello di indice. Dopo aver creato il modello, è possibile visualizzare i vari campi del documento, ad esempio `author` e `title`.
9. Per iniziare a cercare i dati, apri di nuovo il menu principale e scegli Discover (Rileva) o utilizza l'API di ricerca.

Tutorial: Guida introduttiva alla sicurezza in Amazon OpenSearch Serverless (CLI)

Questo tutorial illustra i passaggi descritti nel tutorial introduttivo per la sicurezza della console, ma utilizza la console di servizio AWS CLI anziché la console di OpenSearch servizio.

In questo tutorial completerai le seguenti fasi:

1. Crea una politica di autorizzazioni IAM
2. Associa la policy IAM a un ruolo IAM
3. Creare una policy di crittografia
4. Creazione di una policy di rete
5. Creare una raccolta
6. Configurazione di una policy di accesso ai dati
7. Recupera l'endpoint di raccolta
8. Carica i dati sulla tua connessione
9. Cerca i dati nella tua raccolta

L'obiettivo di questo tutorial è configurare un'unica raccolta OpenSearch Serverless con impostazioni di crittografia, rete e accesso ai dati abbastanza semplici. Ad esempio, configureremo l'accesso alla rete pubblica, una Chiave gestita da AWS per la crittografia e una policy di accesso ai dati semplificata che concede autorizzazioni minime a un singolo utente.

In uno scenario di produzione, ti consigliamo di implementare una configurazione più affidabile, che includa l'autenticazione SAML, una chiave di crittografia personalizzata e l'accesso al VPC.

Per iniziare con le politiche di sicurezza in Serverless OpenSearch

1.
> **Note**
>
> Puoi saltare questa fase se stai già utilizzando una policy più ampia basata sull'identità, ad esempio `Action":"aoss:*"` o `Action":"*"`. Negli ambienti di produzione, tuttavia, si consiglia di seguire il principio del privilegio minimo e di assegnare solo le autorizzazioni minime necessarie per completare un'attività.

   Per iniziare, crea una policy AWS Identity and Access Management con le autorizzazioni minime necessarie per seguire le fasi di questo tutorial. Denomineremo la policy `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\": \"*\"}]}"
```

Risposta di esempio

```
{
    "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. Allega la `TutorialPolicy` al ruolo IAM che indicizzerà e cercherà i dati nella raccolta. Denomineremo l'utente `TutorialRole`:

```
aws iam attach-role-policy \
  --role-name TutorialRole \
  --policy-arn arn:aws:iam::123456789012:policy/TutorialPolicy
```

3. Prima di creare una raccolta, è necessario creare una policy di crittografia che assegni una Chiave di proprietà di AWS alla raccolta books che creerai in una fase successiva.

   Invia la seguente richiesta per creare una policy di crittografia per la raccolta books:

```
aws opensearchserverless create-security-policy \
  --name books-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection\/books\"]}],\"AWSOwnedKey\":true}"
```

   Risposta di esempio

```
{
    "securityPolicyDetail": {
```

```
        "type": "encryption",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDAwNTk5MF8x",
        "policy": {
            "Rules": [
                {
                    "Resource": [
                        "collection/books"
                    ],
                    "ResourceType": "collection"
                }
            ],
            "AWSOwnedKey": true
        },
        "createdDate": 1669240005990,
        "lastModifiedDate": 1669240005990
    }
}
```

4. Crea una policy di rete che fornisca l'accesso pubblico alla raccolta books:

```
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}]"
```

Risposta di esempio

```
{
    "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 raccolta books:

```
aws opensearchserverless create-collection --name books --type SEARCH
```

Risposta di esempio

```
{
    "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. Crea una policy di accesso ai dati che fornisca le autorizzazioni minime per indicizzare e cercare i dati nella raccolta books. Sostituisci l'ARN principale con l'ARN del `TutorialRole` dalla fase 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\"]}]"
```

Risposta di esempio

```
{
    "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
    }
}
```

Ora `TutorialRole` dovrebbe essere in grado di indicizzare e cercare documenti nella raccolta books.

7. Per effettuare chiamate all' OpenSearch API, è necessario l'endpoint di raccolta. Invia la seguente richiesta per recuperare il parametro `collectionEndpoint`:

```
aws opensearchserverless batch-get-collection --names books
```

Risposta di esempio

```
{
    "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**
>
> Non sarà possibile visualizzare l'endpoint della nuova raccolta fino a quando lo stato della nuova raccolta non sarà `ACTIVE`. Potrebbe essere necessario effettuare più chiamate per verificare lo stato fino a quando la raccolta non viene creata correttamente.

8. Usa uno strumento HTTP come Postman o curl per indicizzare i dati nella raccolta books. Creeremo un indice denominato books-index e aggiungeremo un singolo documento.

Invia la richiesta seguente all'endpoint di raccolta recuperato nella fase precedente, utilizzando le credenziali del `TutorialRole`.

```
PUT https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

Risposta di esempio

```
{
  "_index" : "books-index",
  "_id" : "1",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 0,
    "successful" : 0,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 0
}
```

9. Per iniziare a cercare i dati nella raccolta, usa l'API di ricerca. La seguente query esegue una ricerca di base:

```
GET https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_search
```

Risposta di esempio

```
{
    "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 per Amazon OpenSearch Serverless

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Serverless. OpenSearch IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

- Policy basate sull'identità per Serverless OpenSearch
- Azioni politiche per Serverless OpenSearch
- Risorse politiche per Serverless OpenSearch
- Chiavi delle condizioni delle policy per Amazon OpenSearch Serverless
- ABAC con Serverless OpenSearch
- Utilizzo di credenziali temporanee con Serverless OpenSearch
- Ruoli collegati ai servizi per Serverless OpenSearch

- Esempi di policy basate sull'identità per Serverless OpenSearch

Policy basate sull'identità per Serverless OpenSearch

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per Serverless OpenSearch

Per visualizzare esempi di policy basate sull'identità OpenSearch serverless, vedere. the section called “Esempi di policy basate su identità”

Azioni politiche per Serverless OpenSearch

Supporta le operazioni di policy	Sì

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le operazioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche in OpenSearch Serverless utilizzano il seguente prefisso prima dell'azione:

```
aoss
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "aoss:action1",
      "aoss:action2"
         ]
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Describe`, includi la seguente operazione:

```
"Action": "aoss:List*"
```

Per visualizzare esempi di politiche basate sull'identità OpenSearch Serverless, vedere. Esempi di policy basate sull'identità per Serverless OpenSearch

Risorse politiche per Serverless OpenSearch

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Chiavi delle condizioni delle policy per Amazon OpenSearch Serverless

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Oltre al controllo degli accessi basato sugli attributi (ABAC), OpenSearch Serverless supporta le seguenti chiavi di condizione:

- `aoss:collection`
- `aoss:CollectionId`
- `aoss:index`

È possibile utilizzare le chiavi di condizione anche quando si forniscono le autorizzazioni per le policy di accesso e le policy di sicurezza. Per esempio:

```
[
   {
      "Effect":"Allow",
      "Action":[
         "aoss:CreateAccessPolicy",
         "aoss:CreateSecurityPolicy"
      ],
      "Resource":"*",
      "Condition":{
         "StringLike":{
            "aoss:collection":"log"
         }
      }
   }
]
```

In questo esempio, la condizione si applica alle policy che contengono regole che corrispondono al nome o al modello di una raccolta. Le condizioni hanno il seguente comportamento:

- `StringEquals` - Si applica alle policy con regole che contengono la stringa di risorsa esatta "log" (ad esempio, `collection/log`).
- `StringLike` - Si applica alle policy con regole che contengono una stringa di risorsa che include "log" (ad esempio, `collection/log` ma anche `collection/logs-application` o `collection/applogs123`).

> **Note**
>
> Le chiavi di condizione raccolta non si applicano a livello di indice. Ad esempio, nella policy precedente, la condizione non si applicherebbe ad una policy di accesso o di sicurezza contenente la stringa di risorsa `index/logs-application/*`.

Per visualizzare un elenco di chiavi di condizione OpenSearch Serverless, consulta Condition keys for Amazon OpenSearch Serverless nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon OpenSearch Serverless.

ABAC con Serverless OpenSearch

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Per ulteriori informazioni sull'etichettatura delle risorse OpenSearch Serverless, vedere. the section called “Assegnazione di tag alle raccolte”

Utilizzo di credenziali temporanee con Serverless OpenSearch

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWSnon funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Consoleutilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Ruoli collegati ai servizi per Serverless OpenSearch

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione e la gestione di ruoli OpenSearch Serverless collegati ai servizi, consulta. the section called “Ruolo di creazione della raccolta”

Esempi di policy basate sull'identità per Serverless OpenSearch

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Serverless. OpenSearch Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Amazon OpenSearch Serverless, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon OpenSearch Serverless nel Service Authorization Reference.

Argomenti

Best practice per le policy

Le policy basate su identità sono molto efficaci. Determinano se qualcuno può creare, accedere o eliminare risorse OpenSearch Serverless nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse OpenSearch Serverless nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS

CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo di Serverless OpenSearch nella console

Per accedere a OpenSearch Serverless dalla console OpenSearch di servizio, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse OpenSearch Serverless presenti nel tuo account. AWS Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (come i ruoli IAM) associate a tale policy.

Non sono necessarie le autorizzazioni minime della console per gli utenti che effettuano chiamate solo alla AWS CLIo all'API AWS. Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che si sta cercando di eseguire.

La seguente politica consente a un utente di accedere a OpenSearch Serverless dalla console di servizio: OpenSearch

```
{
    "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"
            ]
        }
    ]
}
```

Amministrazione delle raccolte Serverless OpenSearch

Questa policy è un esempio di policy «collection admin» che consente a un utente di gestire e amministrare raccolte Amazon OpenSearch Serverless. L'utente può creare, visualizzare ed eliminare le raccolte.

```
{
    "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"
        }
```

```
    ]
}
```

Visualizzazione delle raccolte Serverless OpenSearch

Questa policy di esempio consente a un utente di visualizzare i dettagli di tutte le raccolte Amazon OpenSearch Serverless nel proprio account. L'utente non può modificare le raccolte o le policy di sicurezza associate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:ListCollections",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:BatchGetCollection"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Utilizzo delle operazioni OpenSearch API

Le operazioni API del piano dati sono costituite dalle funzioni utilizzate in OpenSearch Serverless per ricavare valore in tempo reale dal servizio. Le operazioni API del piano di controllo sono costituite dalle funzioni utilizzate per configurare l'ambiente.

Per accedere alle API e ai OpenSearch dashboard del piano dati di Amazon OpenSearch Serverless dal browser, devi aggiungere due autorizzazioni IAM per le risorse di raccolta. Queste autorizzazioni sono e. `aoss:APIAccessAll` `aoss:DashboardsAccessAll`

> **Note**
>
> A partire dal 10 maggio 2023, OpenSearch Serverless richiede queste due nuove autorizzazioni IAM per le risorse di raccolta. L'`aoss:APIAccessAll`autorizzazione consente l'accesso al piano dati e l'`aoss:DashboardsAccessAll`autorizzazione consente

l'accesso alle OpenSearch dashboard dal browser. La mancata aggiunta delle due nuove autorizzazioni IAM genera un errore 403.

Questa policy di esempio consente a un utente di accedere alle API del piano dati per una raccolta specifica nel proprio account e di accedere alle OpenSearch dashboard per tutte le raccolte nel proprio account.

```
{
    "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"
        }
    ]
}
```

Entrambi `aoss:APIAccessAll` `aoss:DashboardsAccessAll` concedono l'autorizzazione IAM completa alle risorse di raccolta, mentre l'autorizzazione Dashboards fornisce OpenSearch anche l'accesso alle dashboard. Ogni autorizzazione funziona in modo indipendente, quindi una negazione esplicita `aoss:APIAccessAll` non blocca `aoss:DashboardsAccessAll` l'accesso alle risorse, inclusi Dev Tools. Lo stesso vale per una negazione dell'accesso. `aoss:DashboardsAccessAll`

OpenSearch Serverless supporta l'indirizzo IP di origine solo nelle condizioni impostate nella politica IAM del principale per le chiamate sul piano dati:

```
"Condition": {
    "IpAddress": {
         "aws:SourceIp": "52.95.4.14"
    }
}
```

Crittografia in Amazon OpenSearch Serverless

Crittografia a riposo

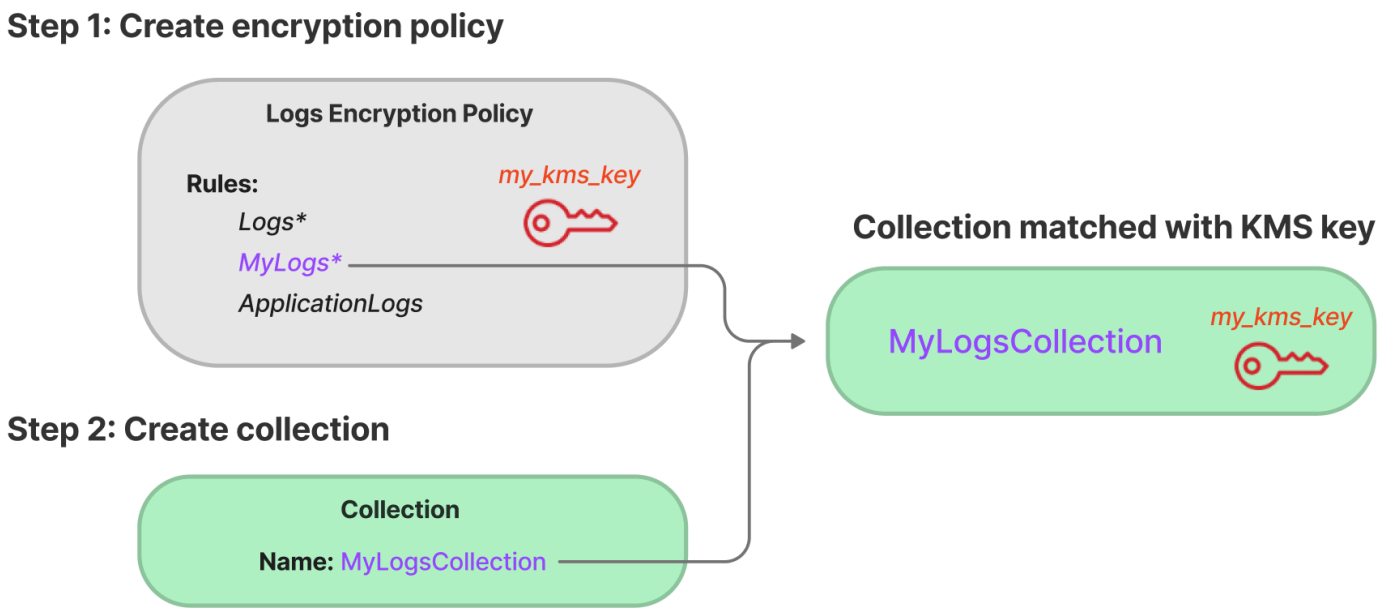
Ogni raccolta Amazon OpenSearch Serverless che crei è protetta con la crittografia dei dati inattivi, una funzionalità di sicurezza che aiuta a prevenire l'accesso non autorizzato ai tuoi dati. Encryption at rest utilizza AWS Key Management Service (AWS KMS) per archiviare e gestire le chiavi di crittografia. Per eseguire la crittografia, utilizza l'algoritmo Advanced Encryption Standard con chiavi a 256 bit (AES-256).

Argomenti

Policy di crittografia

Con le policy di crittografia è possibile gestire molte raccolte su larga scala assegnando automaticamente una chiave di crittografia alle raccolte appena create che corrispondono a un nome o a un modello specifico.

Quando si crea una policy di crittografia, è possibile specificare un prefisso, ossia una regola di corrispondenza basata su caratteri jolly come `MyCollection*`, oppure inserire un unico nome di raccolta. Quindi, quando si crea una raccolta che corrisponde a tale modello di prefisso o nome, ad essa vengono assegnate automaticamente la policy e la chiave KMS corrispondenti.



Le policy di crittografia contengono i seguenti elementi:

- `Rules`: una o più regole di abbinamento delle raccolte, ciascuna con i seguenti sottoelementi:
  - `ResourceType`: attualmente l'unica opzione è "raccolta". Le policy di crittografia si applicano solo alle risorse di raccolta.
  - `Resource`: uno o più nomi o modelli di raccolta a cui si applicherà la policy, nel formato `collection/<collection name|pattern>`.
- `AWSOwnedKey`: se usare o meno una Chiave di proprietà di AWS.
- `KmsARN`: se impostati `AWSOwnedKey` su falso, specifica il nome della risorsa Amazon (ARN) della chiave KMS con cui crittografare le raccolte associate. Se si include questo parametro, OpenSearch Serverless ignora il `AWSOwnedKey` parametro.

La seguente policy di esempio assegnerà una chiave gestita dal cliente a qualsiasi raccolta futura denominata `autopartsinventory`, nonché alle raccolte che iniziano con il termine "vendite":

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
```

```
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

Anche se una policy corrisponde al nome di una raccolta, è possibile scegliere di sovrascrivere tale assegnazione automatica durante la creazione della raccolta se il modello di risorsa contiene un carattere jolly (*). Se scegli di ignorare l'assegnazione automatica delle chiavi, OpenSearch Serverless crea per te una politica di crittografia denominata auto-**< *collection-name* >** e la allega alla raccolta. La policy inizialmente si applica solo a una singola raccolta, ma è possibile modificarla per includere raccolte aggiuntive.

Se modifichi le regole delle policy in modo che non corrispondano più a una raccolta, la chiave KMS associata non verrà annullata da tale raccolta. La raccolta rimane sempre crittografata con la sua chiave di crittografia iniziale. Se desideri modificare la chiave di crittografia per una raccolta, è necessario creare nuovamente la raccolta.

Se a una raccolta corrispondono le regole di più policy, viene utilizzata la regola più specifica. Ad esempio, se una policy contiene una regola per `collection/log*` e un'altra per `collection/logSpecial`, la chiave di crittografia per la seconda policy viene utilizzata in quanto è più specifica.

Non è possibile utilizzare un nome o un prefisso in una politica se esiste già in un'altra politica. OpenSearch Serverless visualizza un errore se si tenta di configurare modelli di risorse identici in diverse politiche di crittografia.

Considerazioni

Quando configuri la crittografia per le tue raccolte considera quanto segue:

- La crittografia dei dati inattivi è obbligatoria per tutte le raccolte serverless.
- Hai la possibilità di utilizzare una chiave gestita dal cliente o una Chiave di proprietà di AWS. Se scegli una chiave gestita dal cliente, ti consigliamo di abilitare la rotazione automatica delle chiavi.
- Dopo la creazione di una raccolta non è possibile modificarne la chiave di crittografia. Scegliete con AWS KMS attenzione quale utilizzare la prima volta che configurate una raccolta.
- Una raccolta può corrispondere solo a una singola policy di crittografia.
- Le raccolte con chiavi KMS uniche non possono condividere le unità di OpenSearch calcolo (OCU) con altre raccolte. Ogni raccolta con una chiave univoca richiede le proprie 4 OCU.

- Se aggiorni la chiave KMS in una policy di crittografia, la modifica non influirà sulle corrispondenti raccolte esistenti a cui sono state già assegnate chiavi KMS.
- OpenSearch Serverless non controlla esplicitamente le autorizzazioni degli utenti sulle chiavi gestite dal cliente. Se un utente dispone delle autorizzazioni per accedere a una raccolta tramite una policy di accesso ai dati, sarà in grado di inserire e interrogare i dati crittografati con la chiave associata.

Autorizzazioni richieste

Encryption at rest for OpenSearch Serverless utilizza le seguenti autorizzazioni AWS Identity and Access Management (IAM). È possibile specificare le condizioni IAM per limitare gli utenti a raccolte specifiche.

- `aoss:CreateSecurityPolicy`: crea una policy di crittografia.
- `aoss:ListSecurityPolicies`: elenca tutte le policy e le raccolte di crittografia a cui sono allegate.
- `aoss:GetSecurityPolicy`: visualizza i dettagli di una policy di crittografia specifica.
- `aoss:UpdateSecurityPolicy`: modifica una policy di crittografia.
- `aoss:DeleteSecurityPolicy`: elimina una policy di crittografia.

Il seguente esempio di policy di accesso basata sull'identità fornisce le autorizzazioni minime necessarie all'utente per gestire le policy di crittografia con il modello di risorsa `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":"*"
      }
   ]
}
```

Policy delle chiavi per una chiave gestita dal cliente

Se si seleziona una chiave gestita dal cliente per proteggere una raccolta, OpenSearch Serverless ottiene l'autorizzazione a utilizzare la chiave KMS per conto del principale che effettua la selezione. Tale principale, un utente o un ruolo, deve disporre delle autorizzazioni sulla chiave KMS richieste da Serverless. OpenSearch Puoi fornire queste autorizzazioni in una policy delle chiavi o in una policy IAM.

OpenSearch Serverless richiede almeno le seguenti autorizzazioni su una chiave gestita dal cliente:

- km: DescribeKey
- km: CreateGrant

Per esempio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:CreateGrant"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
          "kms:ViaService": "aoss.us-east-1.amazonaws.com"
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        }
      }
    }
  ]
}
```

OpenSearch Serverless crea una concessione con le autorizzazioni kms: GenerateDataKey e kms:decrypt.

Per ulteriori informazioni, consulta Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

In OpenSearch che modo Serverless utilizza le sovvenzioni in AWS KMS

OpenSearch Serverless richiede una concessione per utilizzare una chiave gestita dal cliente.

Quando crei una politica di crittografia nel tuo account con una nuova chiave, OpenSearch Serverless crea una concessione per tuo conto inviando una CreateGrantrichiesta a. AWS KMS Le concessioni AWS KMS vengono utilizzate per fornire a OpenSearch Serverless l'accesso a una chiave KMS in un account cliente.

OpenSearch Serverless richiede la concessione per utilizzare la chiave gestita dal cliente per le seguenti operazioni interne:

- Invia DescribeKeyrichieste AWS KMS a per verificare che l'ID della chiave gestita dal cliente simmetrico fornito sia valido.
- Invia GenerateDataKeyle richieste alla chiave KMS per creare chiavi di dati con cui crittografare gli oggetti.
- Invia richieste Decrypt a per AWS KMS decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per crittografare i dati.

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. In tal caso, OpenSearch Serverless non sarà in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influirà su tutte le operazioni che dipendono da tali dati, causando `AccessDeniedException` errori e guasti nei flussi di lavoro asincroni.

OpenSearch Serverless annulla le sovvenzioni in un flusso di lavoro asincrono quando una determinata chiave gestita dal cliente non è associata a politiche o raccolte di sicurezza.

Creazione di policy di crittografia (console)

In una policy di crittografia, si specifica una chiave KMS e una serie di modelli di raccolta a cui verrà applicata la policy. A qualsiasi nuova raccolta che corrisponde a uno dei modelli definiti nella policy verrà assegnata la chiave KMS corrispondente al momento della creazione della raccolta. Consigliamo di creare policy di crittografia prima di iniziare a creare raccolte.

Per creare una politica di crittografia Serverless OpenSearch

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel pannello di navigazione a sinistra, espandi Serverless e scegli Encryption policies (Policy di crittografia).
3. Scegli Create encryption policy (Crea policy di crittografia).
4. Fornisci un nome e una descrizione per la policy.
5. In Resources (Risorse), inserisci uno o più modelli di risorse per questa policy di crittografia. Tutte le nuove raccolte create nella Regione e nell' Account AWS attuali che corrispondono a uno dei modelli vengono automaticamente assegnate a questa policy. Ad esempio, se inserisci `ApplicationLogs` (senza caratteri jolly) e successivamente crei una raccolta con quel nome, la policy e la chiave KMS corrispondente vengono assegnate a tale raccolta.

   Puoi anche fornire un prefisso, ad esempio `Logs*`, che assegni la policy a tutte le nuove raccolte i cui nomi iniziano con `Logs`. Utilizzando i caratteri jolly, puoi gestire le impostazioni di crittografia per varie raccolte su larga scala.
6. In Encryption (Crittografia), scegli una chiave KMS da usare.
7. Seleziona Create (Crea).

Fase successiva: creazione di raccolte

Dopo aver configurato una o più policy di crittografia, puoi iniziare a creare raccolte che corrispondono alle regole definite in tali policy. Per istruzioni, consulta the section called “Creazione di raccolte”.

Nella fase di crittografia della creazione della raccolta, OpenSearch Serverless ti informa che il nome che hai inserito corrisponde al modello definito in una politica di crittografia e assegna

automaticamente la chiave KMS corrispondente alla raccolta. Se il modello di risorsa contiene un carattere jolly (*), puoi scegliere di ignorare la corrispondenza e selezionare la tua chiave.

Creazione di policy di crittografia (AWS CLI)

Per creare una politica di crittografia utilizzando le operazioni dell'API OpenSearch Serverless, si specificano modelli di risorse e una chiave di crittografia in formato JSON. La CreateSecurityPolicyrichiesta accetta sia le politiche in linea che i file.json.

Le policy di crittografia assumono il formato seguente. Questo file `my-policy.json` di esempio corrisponde a qualsiasi raccolta futura denominata `autopartsinventory`, nonché a qualsiasi raccolta con nomi che iniziano 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"
}
```

Per utilizzare una chiave di proprietà del servizio, imposta `AWSOwnedKey` su `true`:

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":true
}
```

La seguente richiesta crea la policy di crittografia:

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy file://my-policy.json
```

Quindi, utilizzate l'operazione CreateCollectionAPI per creare una o più raccolte che corrispondono a uno dei modelli di risorse.

Visualizzazione delle policy di crittografia

Prima di creare una raccolta, hai la possibilità di visualizzare in anteprima le policy di crittografia esistenti nel tuo account per vedere quali hanno uno schema di risorse che corrisponde al nome della raccolta. La seguente ListSecurityPoliciesrichiesta elenca tutte le politiche di crittografia del tuo account:

```
aws opensearchserverless list-security-policies --type encryption
```

La richiesta restituisce informazioni su tutte le policy di crittografia configurate. Utilizza i contenuti dell'elemento `policy` per visualizzare le regole del modello definite nella policy:

```
{
   "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"
      }
   ]
}
```

Per visualizzare informazioni dettagliate su una politica specifica, inclusa la chiave KMS, usa il GetSecurityPolicycomando.

Aggiornamento di policy di crittografia

Se aggiorni la chiave KMS in una policy di crittografia, la modifica verrà applicata solo alle raccolte appena create che corrispondono al nome o al modello configurato. Non influisce sulle raccolte esistenti a cui sono già assegnate chiavi KMS.

Lo stesso vale per le regole di abbinamento delle policy. Se aggiungi, modifichi o elimini una regola, la modifica si applica solo alle raccolte appena create. Se modifichi le regole di una policy in modo che non corrisponda più al nome di una raccolta, le raccolte esistenti non perdono la chiave KMS assegnata.

Per aggiornare una politica di crittografia nella console OpenSearch Serverless, scegli Politiche di crittografia, seleziona la politica da modificare e scegli Modifica. Apporta le modifiche necessarie, quindi scegli Save (Salva).

Per aggiornare una politica di crittografia utilizzando l'API OpenSearch Serverless, utilizza l'UpdateSecurityPolicyoperazione. La seguente richiesta aggiorna una policy di crittografia con un nuovo documento JSON della policy:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy-version 2 \
    --policy file://my-new-policy.json
```

Eliminazione delle policy di crittografia

Quando elimini una policy di crittografia, tutte le raccolte che attualmente utilizzano la chiave KMS definita nella policy non saranno modificate. Per eliminare una policy nella console OpenSearch Serverless, seleziona la policy e scegli Elimina.

Puoi anche utilizzare l'DeleteSecurityPolicyoperazione:

```
aws opensearchserverless delete-security-policy --name my-policy --type encryption
```

Crittografia in transito

In OpenSearch Serverless, tutti i percorsi di una raccolta sono crittografati in transito utilizzando Transport Layer Security 1.2 (TLS) con un codice AES-256 standard di settore. L'accesso a tutte le API e le dashboard per Opensearch avviene anche tramite TLS 1.2. TLS è un insieme di protocolli crittografici standard del settore utilizzati per crittografare le informazioni scambiate sulla rete.

Accesso alla rete per Amazon OpenSearch Serverless

Le impostazioni di rete per una raccolta Amazon OpenSearch Serverless determinano se la raccolta è accessibile su Internet da reti pubbliche o se è necessario accedervi privatamente.

L'accesso privato può applicarsi a uno o entrambi i seguenti elementi:

- OpenSearch Endpoint VPC gestiti senza server
- Supportato Servizi AWS come Amazon Bedrock

Puoi configurare l'accesso alla rete separatamente per l'endpoint di una raccolta e l'OpenSearchendpoint OpenSearch Dashboards corrispondente.

L'accesso alla rete è il meccanismo di isolamento che consente l'accesso da diverse reti di origine. Ad esempio, se l'endpoint OpenSearch Dashboards di una raccolta è accessibile pubblicamente ma l'endpoint OpenSearch API no, un utente può accedere ai dati della raccolta solo tramite Dashboards quando si connette da una rete pubblica. Se provano a chiamare le OpenSearch API direttamente da una rete pubblica, verranno bloccati. Le impostazioni di rete possono essere utilizzate per tali permutazioni dall'origine al tipo di risorsa. Amazon OpenSearch Serverless supporta sia la connettività IPv4 che IPv6.

Argomenti

Policy di rete

Le policy di rete consentono di gestire molte raccolte su larga scala assegnando automaticamente le impostazioni di accesso alla rete alle raccolte che corrispondono alle regole definite nella policy.

In una policy di rete, si specifica una serie di regole. Queste regole definiscono le autorizzazioni di accesso agli endpoint di raccolta e agli endpoint di Dashboards. OpenSearch Ogni regola è composta da un tipo di accesso (pubblico o privato) e da un tipo di risorsa (raccolta e/o OpenSearch endpoint Dashboards). Per ogni tipo di risorsa (`collection` e `dashboard`), si specifica una serie di regole che definiscono a quali raccolte si applicherà la policy.

In questa policy di esempio, la prima regola specifica l'accesso degli endpoint VPC sia all'endpoint di raccolta che all'endpoint Dashboards per tutte le raccolte che iniziano con il termine. `marketing*` Specifica inoltre l'accesso ad Amazon Bedrock.

> **Note**
>
> L'accesso privato Servizi AWS ad Amazon Bedrock si applica solo all'endpoint della raccolta, non all' OpenSearch endpoint OpenSearch Dashboards. Anche se lo `ResourceType` è`dashboard`, Servizi AWS non può essere concesso l'accesso alle dashboard. OpenSearch

La seconda regola specifica l'accesso pubblico alla raccolta `finance`, ma solo per l'endpoint di raccolta (nessun accesso a Dashboards).

```
[
   {
      "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
   }
]
```

Questa politica fornisce l'accesso pubblico solo alle OpenSearch dashboard per le raccolte che iniziano con «finanza». Qualsiasi tentativo di accedere direttamente all' OpenSearch API fallirà.

```
[
  {
    "Description": "Dashboards access",
    "Rules": [
      {
        "ResourceType": "dashboard",
        "Resource": [
          "collection/finance*"
        ]
      }
    ],
    "AllowFromPublic": true
  }
]
```

Le policy di rete possono essere applicate alle raccolte esistenti e alle raccolte future. Ad esempio, è possibile creare una raccolta e quindi creare una policy di rete con una regola che corrisponda al nome della raccolta. Non è necessario creare policy di rete prima di creare le raccolte.

Considerazioni

Quando configuri l'accesso di rete per le tue raccolte considera quanto segue:

- Se prevedi di configurare l'accesso agli endpoint VPC per una raccolta, devi prima creare almeno un endpoint VPC gestito senza server. OpenSearch
- L'accesso privato a si applica Servizi AWS solo all'endpoint della raccolta, non all' OpenSearchendpoint Dashboards. OpenSearch Anche se lo `ResourceType` è`dashboard`, Servizi AWS non può essere concesso l'accesso alle dashboard. OpenSearch
- Se una raccolta è accessibile dalle reti pubbliche, è accessibile anche da tutti gli endpoint VPC OpenSearch gestiti senza server e tutto il resto. Servizi AWS
- A una singola raccolta possono essere applicate più policy di rete. Per ulteriori informazioni, consulta the section called “Priorità delle policy”.

Autorizzazioni necessarie per configurare le politiche di rete

L'accesso alla rete per OpenSearch Serverless utilizza le seguenti autorizzazioni AWS Identity and Access Management (IAM). È possibile specificare le condizioni IAM per limitare gli utenti alle policy di rete associate a raccolte specifiche.

- `aoss:CreateSecurityPolicy`: crea una policy di accesso alla rete.
- `aoss:ListSecurityPolicies`: elenca tutte le policy di rete nell'account corrente.
- `aoss:GetSecurityPolicy`: visualizza una specifica della policy di accesso alla rete.
- `aoss:UpdateSecurityPolicy`: modifica una determinata policy di accesso alla rete e modifica l'ID VPC o la designazione di accesso pubblico.
- `aoss:DeleteSecurityPolicy`: elimina una policy di accesso alla rete (dopo che è stata scollegata da tutte le raccolte).

La seguente policy di accesso basata sull'identità consente a un utente di visualizzare tutte le policy di rete e di aggiornarle in base al modello delle risorse `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": "*"
        }
    ]
}
```

> **Note**
>
> Inoltre, OpenSearch Serverless richiede le autorizzazioni `aoss:APIAccessAll` e le `aoss:DashboardsAccessAll` autorizzazioni per le risorse di raccolta. Per ulteriori informazioni, consulta the section called “Utilizzo delle operazioni OpenSearch API”.

Priorità delle policy

Possono verificarsi situazioni in cui le regole delle policy di rete si sovrappongono, all'interno delle policy o tra di esse. Quando ciò accade, una regola che specifica l'accesso pubblico ha la precedenza su una regola che specifica l'accesso privato per tutte le raccolte comuni a entrambe le regole.

Ad esempio, nella policy seguente, entrambe le regole assegnano l'accesso di rete alla raccolta `finance`, ma una regola specifica l'accesso VPC mentre l'altra specifica l'accesso pubblico. In questa situazione, l'accesso pubblico prevale sull'accesso al VPC solo per la raccolta "finance" (poiché esiste in entrambe le regole), quindi la raccolta "finance" sarà accessibile dalle reti pubbliche. La raccolta delle vendite avrà accesso al VPC dall'endpoint specificato.

```
[
   {
      "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
   }
]
```

Se a una raccolta si applicano più endpoint VPC di regole diverse, la raccolta sarà accessibile da tutti gli endpoint specificati in quanto le regole sono additive. Se lo `AllowFromPublic` imposti `true` ma ne fornisci anche uno o più `SourceVPCEs` oppure`SourceServices`, OpenSearch Serverless ignora gli endpoint VPC e gli identificatori del servizio e le raccolte associate avranno accesso pubblico.

Creazione di policy di rete (console)

Le policy di rete possono essere applicate sia alle policy esistenti che a quelle future. Consigliamo di creare le policy di rete prima di iniziare a creare raccolte.

Per creare una policy di rete Serverless OpenSearch

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel pannello di navigazione a sinistra, espandi Serverless e scegli Network policies (Policy di rete).

3. Scegli Create network policy (Crea policy di rete).
4. Fornisci un nome e una descrizione per la policy.
5. Fornisci una o più regole. Queste regole definiscono le autorizzazioni di accesso per le tue raccolte OpenSearch Serverless e i relativi endpoint OpenSearch Dashboards.

   Ogni regola contiene i seguenti elementi:

Elemento	Descrizione
Nome regola	Un nome che descrive i contenuti della regola. Ad esempio, "Accesso al VPC per il team di marketing".
Tipo di accesso	Scegli l'accesso pubblico o privato. Quindi, seleziona una o entrambe le seguenti opzioni: • Endpoint VPC per l'accesso: specifica uno o più endpoint VPC gestiti senza server, endpoint VPC gestitiOpenSearch . • Servizio AWS accesso privato: seleziona uno o Servizi AWS più supporti.
Tipo di risorsa	Seleziona se fornire l'accesso agli OpenSearch endpoint (che consente di effettuare chiamate all' OpenSearch API), alle OpenSearch dashboard (che consente l'accesso alle visualizzazioni e all'interfaccia utente per i OpenSearch plug-in) o entrambi. **Note** Servizio AWS l'accesso privato si applica solo all'endpoint della raccolta, non all' OpenSearch endpoint Dashboards. OpenSearc h Anche se selezioni OpenSearc

Elemento	Descrizione
	h Dashboards, Servizi AWS può essere concesso solo l'accesso all'endpoint.

Per ogni tipo di risorsa selezionato, puoi scegliere raccolte esistenti a cui applicare le impostazioni delle policy e/o creare uno o più modelli di risorse. I modelli di risorse sono costituiti da un prefisso e da un carattere jolly (*), e definiscono a quali raccolte si applicheranno le impostazioni delle policy.

Ad esempio, se includi un modello denominato `Marketing*`, a qualsiasi raccolta nuova o esistente il cui nome inizia con "Marketing" verranno applicate automaticamente le impostazioni di rete di questa policy. Una singolo carattere jolly (`*`) applica la policy a tutte le raccolte attuali e future.

Inoltre, potete specificare il nome di una collezione futura senza caratteri jolly, ad esempio`Finance`. OpenSearch Serverless applicherà le impostazioni dei criteri a qualsiasi raccolta appena creata con quel nome esatto.

6. Quando sei soddisfatto della configurazione della policy, scegli Create (Crea).

Creazione di policy di rete (AWS CLI)

Per creare una politica di rete utilizzando le operazioni dell'API OpenSearch Serverless, specificate le regole in formato JSON. La CreateSecurityPolicyrichiesta accetta sia le politiche in linea che i file.json. Tutte le raccolte e i modelli devono assumere la forma `collection/<collection name|pattern>`.

> **Note**
>
> Il tipo di risorsa consente `dashboards` solo l'autorizzazione alle OpenSearch dashboard, ma per far funzionare le OpenSearch dashboard è necessario consentire anche l'accesso alla raccolta dalle stesse fonti. Osserva la seconda policy di seguito per un esempio.

Per specificare l'accesso privato, includi uno o entrambi i seguenti elementi:

- `SourceVPCEs`— Specificare uno o più endpoint OpenSearch VPC gestiti senza server.
- `SourceServices`— Specificare l'identificatore di uno o più supportati. Servizi AWS Attualmente sono supportati i seguenti identificatori di servizio:
  - `bedrock.amazonaws.com`— Amazon Bedrock

La seguente policy di rete di esempio fornisce l'accesso privato, a un endpoint VPC e Amazon Bedrock, agli endpoint di raccolta solo per le raccolte che iniziano con il prefisso. `log*` Gli utenti autenticati non possono accedere alle OpenSearch dashboard; possono solo accedere all'endpoint di raccolta a livello di codice.

```
[
   {
      "Description":"Private access for log collections",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/log*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   }
]
```

La seguente politica fornisce l'accesso pubblico all' OpenSearch endpoint e alle OpenSearch dashboard per una singola raccolta denominata. `finance` Se la raccolta non esiste, le impostazioni di rete verranno applicate alla raccolta se e quando viene creata.

```
[
   {
      "Description":"Public access for finance collection",
      "Rules":[
         {
```

```
            "ResourceType":"dashboard",
            "Resource":[
               "collection/finance"
            ]
         },
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

La seguente richiesta crea la policy di rete di cui sopra:

```
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}]"
```

Per fornire la policy in un file JSON, utilizzare il formato `--policy file://my-policy.json`

Visualizzazione delle policy di rete

Prima di creare una raccolta, hai la possibilità di visualizzare in anteprima le policy di rete esistenti nel tuo account per vedere quali hanno uno schema di risorse che corrisponde al nome della raccolta. La ListSecurityPoliciesrichiesta seguente elenca tutte le politiche di rete del tuo account:

```
aws opensearchserverless list-security-policies --type network
```

La richiesta restituisce informazioni su tutte le policy di rete configurate. Per visualizzare le regole del modello definite in una politica specifica, trova le informazioni sulla politica nel contenuto dell'`securityPolicySummaries`elemento nella risposta. Prendi nota della `name` fine `type` di questa politica e utilizza queste proprietà in una GetSecurityPolicyrichiesta per ricevere una risposta con i seguenti dettagli della politica:

```
{
    "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
        }
    ]
}
```

Per visualizzare informazioni dettagliate su una politica specifica, utilizzare il GetSecurityPolicycomando.

Aggiornamento delle policy di rete

Quando si modificano gli endpoint VPC o la designazione di accesso pubblico per una rete, vengono interessate anche tutte le raccolte associate. Per aggiornare una politica di rete nella console OpenSearch Serverless, espandi Criteri di rete, seleziona la politica da modificare e scegli Modifica. Apporta le modifiche necessarie, quindi scegli Save (Salva).

Per aggiornare una politica di rete utilizzando l'API OpenSearch Serverless, usa il UpdateSecurityPolicycomando. È necessario includere una versione della policy nella richiesta. È possibile recuperare la versione della policy utilizzando i comandi `ListSecurityPolicies` o `GetSecurityPolicy`. L'inclusione della versione più recente delle policy garantisce di non sovrascrivere inavvertitamente una modifica apportata da qualcun altro.

La seguente richiesta aggiorna una policy di rete con un nuovo documento JSON della policy:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type network \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Eliminazione delle policy di rete

Prima di eliminare una policy di rete, è necessario scollegarla da tutte le raccolte. Per eliminare una policy nella console OpenSearch Serverless, seleziona la policy e scegli Elimina.

Puoi anche usare il DeleteSecurityPolicycomando:

```
aws opensearchserverless delete-security-policy --name my-policy --type network
```

Controllo dell'accesso ai dati per Amazon OpenSearch Serverless

Con il controllo dell'accesso ai dati in Amazon OpenSearch Serverless, puoi consentire agli utenti di accedere a raccolte e indici, indipendentemente dal meccanismo di accesso o dalla fonte di rete. Puoi fornire l'accesso ai ruoli IAM e alle identità SAML.

Puoi gestire le autorizzazioni di accesso tramite le policy di accesso ai dati, che si applicano alle raccolte e alle risorse dell'indice. Le policy di accesso ai dati consentono di gestire le raccolte su larga scala assegnando automaticamente autorizzazioni di accesso a raccolte e indici che corrispondono a uno schema specifico. È possibile applicare più policy di accesso ai dati a una singola risorsa. Tieni presente che devi disporre di una politica di accesso ai dati per la tua raccolta per poter accedere all'URL delle dashboard OpenSearch .

Argomenti

- Policy di accesso ai dati rispetto alle policy IAM
- Autorizzazioni IAM necessarie per configurare le politiche di accesso ai dati
- Sintassi delle policy
- Autorizzazioni delle policy supportate
- Set di dati di esempio nelle dashboard OpenSearch
- Creazione di policy di accesso ai dati (console)
- Creazione di policy di accesso ai dati (AWS CLI)
- Visualizzazione di policy di accesso ai dati
- Aggiornamento delle policy di accesso ai dati
- Eliminazione delle policy di accesso ai dati
- Accesso ai dati tra account

Policy di accesso ai dati rispetto alle policy IAM

Le policy di accesso ai dati sono logicamente separate dalle policy AWS Identity and Access Management (IAM). Le autorizzazioni IAM controllano l'accesso alle operazioni API serverless, come `CreateCollection` e `ListAccessPolicies`. Le politiche di accesso ai dati controllano l'accesso alle OpenSearch operazioni supportate da OpenSearch Serverless, come `PUT <index>` o. `GET _cat/indices`

Le autorizzazioni IAM che controllano l'accesso alle operazioni dell'API della policy di accesso ai dati, come `aoss:CreateAccessPolicy` e `aoss:GetAccessPolicy` (descritte nella sezione successiva), non influiscono sull'autorizzazione specificata in una policy di accesso ai dati.

Ad esempio, supponiamo che una policy IAM impedisca a un utente di creare policy di accesso ai dati per `collection-a`, ma gli consenta di creare policy di accesso ai dati per tutte le raccolte (`*`):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aoss:collection": "collection-a"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Se l'utente crea una policy di accesso ai dati che consente determinate autorizzazioni per tutte le raccolte (`collection/*` o `index/*/*`), la policy si applicherà a tutte le raccolte, inclusa la raccolta A.

> **Important**
>
> La concessione delle autorizzazioni nell'ambito di una politica di accesso ai dati non è sufficiente per accedere ai dati della raccolta OpenSearch Serverless. A un principale associato deve inoltre essere concesso l'accesso alle autorizzazioni `aoss:APIAccessAll` IAM e. `aoss:DashboardsAccessAll` Entrambe le autorizzazioni garantiscono l'accesso completo alle risorse di raccolta, mentre l'autorizzazione Dashboards fornisce anche l'accesso alle dashboard. OpenSearch Se un principale non dispone di entrambe queste autorizzazioni IAM, riceverà 403 errori quando tenta di inviare richieste alla raccolta. Per ulteriori informazioni, consulta the section called “Utilizzo delle operazioni OpenSearch API”.

Autorizzazioni IAM necessarie per configurare le politiche di accesso ai dati

Il controllo dell'accesso ai dati per OpenSearch Serverless utilizza le seguenti autorizzazioni IAM. È possibile specificare condizioni IAM per limitare gli utenti a nomi di policy di accesso specifici.

- `aoss:CreateAccessPolicy`: crea una policy di accesso.
- `aoss:ListAccessPolicies`: elenca tutte le policy di accesso.
- `aoss:GetAccessPolicy`: visualizza i dettagli su una policy di accesso specifica.
- `aoss:UpdateAccessPolicy`: modifica una policy di accesso.
- `aoss:DeleteAccessPolicy`: elimina una policy di accesso.

La seguente policy di accesso basata sull'identità consente a un utente di visualizzare tutte le policy di accesso e aggiornare le policy che contengono il modello delle risorse `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"
                    ]
                }
            }
        }
    ]
}
```

> **Note**
>
> Inoltre, OpenSearch Serverless richiede le autorizzazioni `aoss:APIAccessAll` e le `aoss:DashboardsAccessAll` autorizzazioni per le risorse di raccolta. Per ulteriori informazioni, consulta the section called “Utilizzo delle operazioni OpenSearch API”.

Sintassi delle policy

Una policy di accesso ai dati include una serie di regole, ognuna con i seguenti elementi:

Elemento	Descrizione
`ResourceType`	Il tipo di risorsa (raccolta o indice) a cui si applicano le autorizzazioni. Le autorizzazioni degli alias e dei modelli sono a livello di raccolta, mentre le autorizzazioni per la creazione, la modifica e la ricerca dei dati sono a livello di indice. Per ulteriori informazioni, consulta la sezione Supported policy permissions (Autorizzazioni delle policy supportate).

Elemento	Descrizione
`Resource`	Un elenco di nomi e/o modelli di risorse. I modelli sono prefissi seguiti da un carattere jolly (*), che consentono di applicare le autorizzazioni associate a più risorse. • Le raccolte hanno il formato `collection/` *`<name|pattern>`* . • Gli indici hanno il formato `index/`*`<collection-name|pattern>`* */*`<index-name|pattern/>` .
`Permission`	Un elenco di autorizzazioni da concedere per le risorse specificate. Per un elenco completo delle autorizzazioni e delle operazioni dell'API che queste concedono, consulta la sezione the section called “Operazioni e autorizzazioni API supportate OpenSearch ”.
`Principal`	Un elenco di uno o più principali a cui concedere l'accesso. I principali possono essere ARN di ruoli IAM o identità SAML. Questi principali devono essere all'interno dell' Account AWS corrente. Le policy di accesso ai dati non supportano direttamente l'accesso tra account diversi, ma puoi includere nella policy un ruolo che un utente di un altro account Account AWS può assumere nell'account proprietario della raccolta. Per ulteriori informazioni, consulta the section called “Accesso ai dati tra account”.

La seguente policy di esempio concede autorizzazioni di alias e modello alla raccolta denominata `autopartsinventory`, nonché a tutte le raccolte che iniziano con il prefisso `sales*`. Inoltre, concede autorizzazioni di lettura e scrittura a tutti gli indici della raccolta `autopartsinventory` e a tutti gli indici della raccolta `salesorders` che iniziano con il prefisso `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"
      ]
   }
]
```

Non puoi negare esplicitamente l'accesso all'interno di una policy. Pertanto, tutte le autorizzazioni delle policy sono additive. Ad esempio, se a un utente una policy concede `aoss:ReadDocument` e un'altra concede `aoss:WriteDocument`, l'utente avrà entrambe le autorizzazioni. Se una terza policy concede `aoss:*` allo stesso utente, l'utente può eseguire tutte le azioni sull'indice associato; le autorizzazioni più restrittive non sostituiscono quelle meno restrittive.

Autorizzazioni delle policy supportate

Le seguenti autorizzazioni sono supportate nelle policy di accesso ai dati. Per le operazioni OpenSearch API consentite da ciascuna autorizzazione, consulta. the section called “Operazioni e autorizzazioni API supportate OpenSearch ”

Autorizzazioni della raccolta

- `aoss:CreateCollectionItems`
- `aoss:DeleteCollectionItems`

- aoss:UpdateCollectionItems
- aoss:DescribeCollectionItems
- aoss:*

Autorizzazioni dell'indice

- aoss:ReadDocument
- aoss:WriteDocument
- aoss:CreateIndex
- aoss:DeleteIndex
- aoss:UpdateIndex
- aoss:DescribeIndex
- aoss:*

Set di dati di esempio nelle dashboard OpenSearch

OpenSearch Dashboards fornisce set di dati di esempio che includono visualizzazioni, dashboard e altri strumenti per aiutarti a esplorare le dashboard prima di aggiungere i tuoi dati. Per creare indici a partire da questi dati di esempio, è necessaria una politica di accesso ai dati che fornisca le autorizzazioni per il set di dati con cui desideri lavorare. La seguente politica utilizza un wildcard (*) per fornire le autorizzazioni per tutti e tre i set di dati di esempio.

```
[
  {
    "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>"
    ]
  }
]
```

Creazione di policy di accesso ai dati (console)

È possibile creare una policy di accesso ai dati utilizzando l'editor visivo o in formato JSON. A qualsiasi nuova raccolta che corrisponde a uno dei modelli definiti nella policy verranno assegnate le autorizzazioni corrispondenti al momento della creazione della raccolta.

Per creare una politica di accesso ai dati OpenSearch Serverless

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel pannello di navigazione a sinistra, espandi Serverless e scegli Data access control (Controllo dell'accesso ai dati).
3. Scegli Create access policy (Crea policy di accesso).
4. Fornisci un nome e una descrizione per la policy.
5. Fornisci un nome per la prima regola nella policy. Ad esempio, "Accesso alla raccolta di log".
6. Scegli Add principals (Aggiungi principali) e seleziona uno o più ruoli IAM o utenti e gruppi SAML a cui fornire l'accesso ai dati.

   > **Note**
   >
   > Per poter selezionare i principali dai menu a discesa, è necessario disporre delle autorizzazioni `iam:ListUsers` e `iam:ListRoles` (per i principali IAM) e dell'autorizzazione `aoss:ListSecurityConfigs` (per le identità SAML).

7. Scegli Grant (Concedi) e seleziona le autorizzazioni per l'alias, il modello e l'indice da concedere ai principali associati. Per un elenco completo delle autorizzazioni e l'accesso che queste concedono, consulta la sezione the section called “Operazioni e autorizzazioni API supportate OpenSearch ”.
8. (Facoltativo) Configurazione di regole aggiuntive per la policy.
9. Scegli Crea. Potrebbe esserci circa un minuto di ritardo tra il momento in cui si crea la policy e il momento in cui vengono applicate le autorizzazioni. Se occorrono più di 5 minuti, contatta AWS Support.

> **Important**
>
> Se la policy include solo le autorizzazioni dell'indice (e nessuna autorizzazione della raccolta), potresti comunque visualizzare un messaggio per le raccolte corrispondenti che indica `Collection cannot be accessed yet. Configure data access policies so that users can access the data within this collection`. Tale avviso si può ignorare. I principali autorizzati possono comunque eseguire le operazioni relative all'indice assegnate sulla raccolta.

Creazione di policy di accesso ai dati (AWS CLI)

Per creare una politica di accesso ai dati utilizzando l'API OpenSearch Serverless, usa il `CreateAccessPolicy` comando. Il comando accetta sia policy inline che file .json. Le policy inline devono essere codificate come una stringa con escape JSON.

La seguente richiesta crea una policy di accesso ai dati:

```
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\"]}]"
```

Per fornire la policy all'interno di un file .json, utilizza il formato `--policy file://my-policy.json`.

I principali inclusi nella policy possono ora utilizzare le OpenSearch operazioni a cui hanno avuto accesso.

Visualizzazione di policy di accesso ai dati

Prima di creare una raccolta, hai la possibilità di visualizzare in anteprima le policy di accesso ai dati esistenti nel tuo account per vedere quali hanno un modello di risorse che corrisponde al nome della raccolta. La seguente ListAccessPoliciesrichiesta elenca tutte le politiche di accesso ai dati del tuo account:

```
aws opensearchserverless list-access-policies --type data
```

La richiesta restituisce informazioni su tutte le policy di accesso ai dati configurate. Per visualizzare le regole del modello definite in una politica specifica, trova le informazioni sulla politica nel contenuto dell'`accessPolicySummaries`elemento nella risposta. Prendi nota della `name` fine `type` di questa politica e utilizza queste proprietà in una GetAccessPolicyrichiesta per ricevere una risposta con i seguenti dettagli della politica:

```
{
    "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
        }
    ]
}
```

Puoi includere filtri di risorse per limitare i risultati alle policy che contengono raccolte o indici specifici:

```
aws opensearchserverless list-access-policies --type data --resource
 "index/autopartsinventory/*"
```

Per visualizzare i dettagli su una politica specifica, utilizzare il GetAccessPolicycomando.

Aggiornamento delle policy di accesso ai dati

Quando aggiorni una policy di accesso ai dati, vengono interessate anche tutte le altre raccolte associate. Per aggiornare una politica di accesso ai dati nella console OpenSearch Serverless, scegli Controllo dell'accesso ai dati, seleziona la politica da modificare e scegli Modifica. Apporta le modifiche necessarie, quindi scegli Save (Salva).

Per aggiornare una politica di accesso ai dati utilizzando l'API OpenSearch Serverless, invia una `UpdateAccessPolicy` richiesta. È necessario includere una versione della policy, che è possibile recuperare utilizzando i comandi `ListAccessPolicies` o `GetAccessPolicy`. L'inclusione della versione più recente delle policy garantisce di non sovrascrivere inavvertitamente una modifica apportata da qualcun altro.

La seguente UpdateAccessPolicyrichiesta aggiorna una politica di accesso ai dati con un nuovo documento JSON di policy:

```
aws opensearchserverless update-access-policy \
    --name sales-inventory \
    --type data \
    --policy-version MTY2NDA1NDE4MDg1OF8x \
    --policy file://my-new-policy.json
```

Potrebbero verificarsi alcuni minuti di ritardo tra l'aggiornamento della policy e il momento in cui vengono applicate le nuove autorizzazioni.

Eliminazione delle policy di accesso ai dati

Quando si elimina una policy di accesso ai dati, tutte le raccolte associate perdono l'accesso definito nella policy stessa. Prima di eliminare una policy, assicurati che i tuoi utenti IAM e SAML abbiano l'accesso appropriato alla raccolta. Per eliminare una policy nella console OpenSearch Serverless, seleziona la policy e scegli Elimina.

Puoi anche usare il DeleteAccessPolicycomando:

```
aws opensearchserverless delete-access-policy --name my-policy --type data
```

Accesso ai dati tra account

Sebbene non sia possibile creare una politica di accesso ai dati con identità o raccolte tra più account, puoi comunque configurare l'accesso su più account con l'opzione Assumi ruolo. Ad esempio, se *account-a* possiede una raccolta a cui *account-b* deve accedere, l'utente di *account-b* può assumere un ruolo in. *account-a* Il ruolo deve disporre delle autorizzazioni IAM `aoss:APIAccessAll` ed `aoss:DashboardsAccessAll` essere incluso nella politica di accesso ai dati su*account-a*.

Accedi ad Amazon OpenSearch Serverless utilizzando un endpoint di interfaccia ()AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e Amazon OpenSearch Serverless. Puoi accedere a OpenSearch Serverless come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere a OpenSearch Serverless.

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da specificare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato a Serverless. OpenSearch

Per ulteriori informazioni, consulta la sezione Accesso a Servizi AWS tramite AWS PrivateLink nella Guida di AWS PrivateLink .

Argomenti

Risoluzione DNS degli endpoint di raccolta

Quando crei un endpoint VPC, il servizio crea una nuova zona ospitata Amazon Route 53 privata e la collega al VPC. Questa zona ospitata privata è costituita da un record per risolvere il record DNS wildcard per le raccolte OpenSearch Serverless (`*.aoss.us-east-1.amazonaws.com`) negli indirizzi di interfaccia utilizzati per l'endpoint. È sufficiente un solo endpoint VPC OpenSearch serverless in un VPC per accedere a tutte le raccolte e i dashboard di ciascuno di essi. Regione AWS Ogni VPC con un endpoint per OpenSearch Serverless ha una propria zona ospitata privata collegata.

OpenSearch Serverless crea anche un record DNS wildcard pubblico della Route 53 per tutte le raccolte della regione. Il nome DNS viene risolto negli indirizzi IP pubblici Serverless. OpenSearch I client in VPC che non dispongono di un endpoint OpenSearch VPC Serverless o i client in reti pubbliche possono utilizzare il resolver pubblico Route 53 e accedere alle raccolte e ai dashboard con tali indirizzi IP. Il tipo di indirizzo IP (IPv4, IPv6 o Dualstack) dell'endpoint VPC viene determinato in base alle sottoreti fornite durante la creazione di un endpoint di interfaccia per Serverless. OpenSearch

> **Note**
>
> È possibile aggiornare l'endpoint VPC IPv4 esistente a Dualstack utilizzando il comando in. update-vpc-endpoint AWS CLI

L'indirizzo del resolver DNS per un determinato VPC è il secondo indirizzo IP del VPC CIDR. Qualsiasi client nel VPC deve utilizzare quel resolver per ottenere l'indirizzo dell'endpoint VPC per qualsiasi raccolta. Il resolver utilizza una zona ospitata privata creata da Serverless. OpenSearch È sufficiente utilizzare quel resolver per tutte le raccolte di qualsiasi account. È anche possibile utilizzare il resolver VPC per alcuni endpoint di raccolta e il resolver pubblico per altri, sebbene in genere non sia necessario.

VPC e politiche di accesso alla rete

Per concedere l'autorizzazione di rete alle OpenSearch API e ai dashboard per le tue raccolte, puoi utilizzare le policy di accesso alla rete OpenSearch Serverless. Puoi controllare questo accesso alla rete dagli endpoint VPC o dalla rete Internet pubblica. Poiché la policy di rete controlla solo le autorizzazioni relative al traffico, è necessario impostare anche una policy di accesso ai dati che specifichi l'autorizzazione a operare sui dati di una raccolta e sui relativi indici. Pensate a un endpoint VPC OpenSearch serverless come punto di accesso al servizio, a una policy di accesso alla rete come punto di accesso a livello di rete a raccolte e dashboard e a una politica di accesso ai dati come punto di accesso per il controllo granulare degli accessi per qualsiasi operazione sui dati della raccolta.

Poiché puoi specificare più ID di endpoint VPC in una policy di rete, ti consigliamo di creare un endpoint VPC per ogni VPC che deve accedere a una raccolta. Questi VPC possono appartenere a AWS account diversi rispetto all'account che possiede la raccolta Serverless e la OpenSearch policy di rete. Non è consigliabile creare un peering da VPC a VPC o un'altra soluzione di proxy tra due account in modo che il VPC di un account possa utilizzare l'endpoint VPC di un altro account. Si tratta

di una soluzione meno sicura ed economica rispetto a ogni VPC con il proprio endpoint. Il primo VPC non sarà facilmente visibile all'amministratore dell'altro VPC, che ha impostato l'accesso all'endpoint di quel VPC nella policy di rete.

VPC e politiche degli endpoint

Amazon OpenSearch Serverless supporta le policy degli endpoint per i VPC. Una policy per gli endpoint è una policy basata sulle risorse IAM che colleghi a un endpoint VPC per controllare quali AWS responsabili possono utilizzare l'endpoint per accedere al tuo servizio. AWS Per ulteriori informazioni, consulta Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint.

Per utilizzare una policy per gli endpoint, devi prima creare un endpoint di interfaccia. È possibile creare un endpoint di interfaccia utilizzando la console Serverless o l' OpenSearch API Serverless. OpenSearch Dopo aver creato l'endpoint di interfaccia, dovrai aggiungere la policy dell'endpoint all'endpoint. Per ulteriori informazioni, consulta Accedere ad Amazon OpenSearch Serverless utilizzando un endpoint di interfaccia ()AWS PrivateLink.

> **Note**
>
> Non è possibile definire una policy per gli endpoint direttamente nella console di servizio. OpenSearch

Una policy per gli endpoint non sostituisce né sostituisce altre politiche basate sull'identità, politiche basate sulle risorse, politiche di rete o politiche di accesso ai dati che potresti aver configurato. Per ulteriori informazioni sull'aggiornamento delle policy degli endpoint, consulta Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint.

Per impostazione predefinita, una policy per gli endpoint garantisce l'accesso completo all'endpoint VPC.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
```

```
}
```

Sebbene la policy degli endpoint VPC predefinita garantisca l'accesso completo agli endpoint, puoi configurare una policy degli endpoint VPC per consentire l'accesso a ruoli e utenti specifici. A tale scopo, consulta l'esempio seguente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012",
                    "987654321098"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Puoi specificare una raccolta OpenSearch Serverless da includere come elemento condizionale nella tua policy degli endpoint VPC. A tale scopo, consulta l'esempio seguente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CollectionName": [
                        "coll-abc"
                    ]
                }
            }
        }
```

```
    ]
}
```

Puoi utilizzare le identità SAML nella tua policy degli endpoint VPC per determinare l'accesso agli endpoint VPC. È necessario utilizzare un carattere jolly (*) nella sezione principale della policy degli endpoint VPC. A tale scopo, consulta l'esempio seguente:

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Inoltre, puoi configurare la tua policy sugli endpoint per includere una politica principale SAML specifica. A tale scopo, consulta quanto segue:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SamlPrincipal": [
```

```
                        "saml/123456789012/idp123/user/user1234"]
                    }
                }
            }
        ]
    }
```

Per ulteriori informazioni sull'utilizzo dell'autenticazione SAML con Amazon OpenSearch Serverless, consulta Autenticazione SAML per Amazon Serverless. OpenSearch

Puoi anche includere utenti IAM e SAML nella stessa policy degli endpoint VPC. A tale scopo, consulta l'esempio seguente:

```
{
    "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": "*"
        }
    ]
}
```

Considerazioni

Prima di configurare un endpoint di interfaccia per OpenSearch Serverless, considera quanto segue:

- OpenSearch Serverless supporta l'esecuzione di chiamate a tutte le operazioni OpenSearch API supportate (non le operazioni API di configurazione) tramite l'endpoint dell'interfaccia.
- Dopo aver creato un endpoint di interfaccia per OpenSearch Serverless, è comunque necessario includerlo nelle politiche di accesso alla rete per consentirgli di accedere alle raccolte serverless.
- Per impostazione predefinita, l'accesso completo a OpenSearch Serverless è consentito tramite l'endpoint dell'interfaccia. È possibile associare un gruppo di sicurezza alle interfacce di rete degli endpoint per controllare il traffico verso OpenSearch Serverless attraverso l'endpoint dell'interfaccia.
- Un singolo dispositivo Account AWS può avere un massimo di 50 endpoint VPC OpenSearch serverless.
- Se abiliti l'accesso pubblico a Internet all'API o alle dashboard della tua raccolta in una politica di rete, la raccolta è accessibile da qualsiasi VPC e dalla rete Internet pubblica.
- Se sei in locale e all'esterno del VPC, non puoi utilizzare direttamente un resolver DNS per OpenSearch la risoluzione degli endpoint VPC Serverless. Se hai bisogno di un accesso VPN, il VPC necessita di un resolver proxy DNS da utilizzare da client esterni. Route 53 offre un'opzione di endpoint in entrata che puoi utilizzare per risolvere le query DNS sul tuo VPC dalla rete locale o da un altro VPC.
- La zona ospitata privata che OpenSearch Serverless crea e collega al VPC è gestita dal servizio, ma compare nelle tue Amazon Route 53 risorse e viene fatturata sul tuo account.
- Per altre considerazioni, consulta la sezione Considerazioni nella Guida AWS PrivateLink .

Autorizzazioni richieste

L'accesso VPC per OpenSearch Serverless utilizza le seguenti autorizzazioni AWS Identity and Access Management (IAM). È possibile specificare le condizioni IAM per limitare gli utenti a raccolte specifiche.

- `aoss:CreateVpcEndpoint` - Creazione di un endpoint VPC.
- `aoss:ListVpcEndpoints` - Elencazione di tutti gli endpoint VPC.
- `aoss:BatchGetVpcEndpoint` - Visualizzazione dei dettagli su un sottoinsieme di endpoint VPC.
- `aoss:UpdateVpcEndpoint` - Modifica di un endpoint VPC.

- `aoss:DeleteVpcEndpoint` - Eliminazione di un endpoint VPC.

Inoltre, sono necessarie le seguenti autorizzazioni Amazon EC2 e Route 53 per creare un endpoint 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`

Crea un endpoint di interfaccia per Serverless OpenSearch

Puoi creare un endpoint di interfaccia per OpenSearch Serverless utilizzando la console o l'API Serverless. OpenSearch

Per creare un endpoint di interfaccia per una raccolta Serverless OpenSearch

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel pannello di navigazione a sinistra, espandi Serverless e seleziona endpoint VPC.

3. Scegli Create VPC endpoint (Crea endpoint VPC).
4. Fornisci un nome per l'endpoint.
5. Per VPC, seleziona il VPC da cui accederai Serverless. OpenSearch
6. Per le sottoreti, seleziona una sottorete da cui accederai a Serverless. OpenSearch

   - L'indirizzo IP e il tipo DNS dell'endpoint si basano sul tipo di sottorete
     - Dualstack: se tutte le sottoreti hanno intervalli di indirizzi sia IPv4 che IPv6
     - IPv6: se tutte le sottoreti sono solo sottoreti IPv6
     - IPv4: se tutte le sottoreti hanno intervalli di indirizzi IPv4
7. Per Security groups (Gruppi di sicurezza), seleziona i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint. Si tratta di un passaggio fondamentale per limitare le porte, i protocolli e le origini per il traffico in ingresso che si sta autorizzando per l'endpoint. Assicurati che le regole del gruppo di sicurezza consentano alle risorse che utilizzeranno l'endpoint VPC di comunicare con OpenSearch Serverless di comunicare con l'interfaccia di rete dell'endpoint.
8. Seleziona Crea endpoint.

Per creare un endpoint VPC utilizzando l'API OpenSearch Serverless, usa il comando. `CreateVpcEndpoint`

> **Note**
>
> Dopo aver creato un endpoint, annotane l'ID (ad esempio, `vpce-050f79086ee71ac05`). Per fornire all'endpoint l'accesso alle raccolte, è necessario includere questo ID in una o più policy di accesso alla rete.

Fase successiva: concedere all'endpoint l'accesso a una raccolta

Dopo aver creato un endpoint di interfaccia, è necessario fornirgli l'accesso alle raccolte tramite policy di accesso alla rete. Per ulteriori informazioni, consulta the section called “Accesso alla rete”.

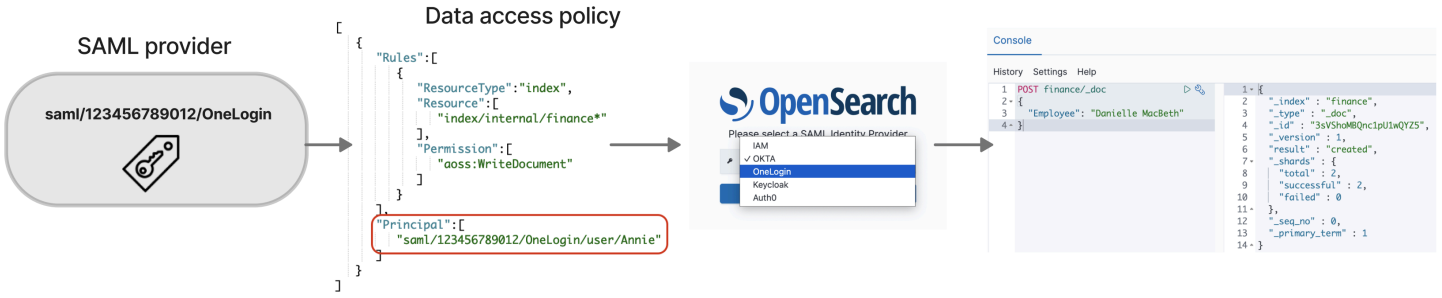
Autenticazione SAML per Amazon Serverless OpenSearch

Con l'autenticazione SAML per Amazon OpenSearch Serverless, puoi utilizzare il tuo provider di identità esistente per offrire il Single Sign-On (SSO) per gli endpoint OpenSearch Dashboards delle raccolte serverless.

L'autenticazione SAML consente di utilizzare provider di identità di terze parti per accedere alle dashboard per indicizzare e cercare dati. OpenSearch OpenSearch Serverless supporta i provider che utilizzano lo standard SAML 2.0, come IAM Identity Center, Okta, Keycloak, Active Directory Federation Services (AD FS) e Auth0. Puoi configurare IAM Identity Center per sincronizzare utenti e gruppi da altre fonti di identità come Okta e Microsoft Entra ID. OneLogin Per un elenco delle fonti di identità supportate da IAM Identity Center e i passaggi per configurarle, consulta i tutorial introduttivi nella Guida per l'utente di IAM Identity Center.

> **Note**
>
> L'autenticazione SAML serve solo per accedere alle OpenSearch dashboard tramite un browser web. Gli utenti autenticati possono effettuare richieste alle operazioni OpenSearch API solo tramite Dev Tools in Dashboards. OpenSearch Le tue credenziali SAML non ti consentono di effettuare richieste HTTP dirette alle operazioni API. OpenSearch

Per configurare l'autenticazione SAML, è necessario configurare prima un provider di identità (IdP) SAML. Quindi includi uno o più utenti di quell'IdP in una policy di accesso ai dati. Questa policy gli concede determinate autorizzazioni per le raccolte e/o gli indici. Un utente può quindi accedere alle OpenSearch dashboard ed eseguire le azioni consentite nella politica di accesso ai dati.



Argomenti

- Considerazioni
- Autorizzazioni richieste
- Creazione di provider SAML (console)
- Accesso ai pannelli OpenSearch di controllo
- Concessione alle identità SAML dell'accesso ai dati della raccolta
- Creazione di provider SAML (AWS CLI)
- Visualizzazione di provider SAML

- Aggiornamento dei provider SAML
- Eliminazione di provider SAML

Considerazioni

Durante la configurazione dell'autenticazione SAML tieni presente quanto segue:

- Le richieste firmate e crittografate non sono supportate.
- Le asserzioni crittografate non sono supportate.
- L'autenticazione e la disconnessione avviate dal'IdP non sono supportate.

Autorizzazioni richieste

L'autenticazione SAML per OpenSearch Serverless utilizza le seguenti autorizzazioni AWS Identity and Access Management (IAM):

- `aoss:CreateSecurityConfig`: crea un provider SAML.
- `aoss:ListSecurityConfig`: elenca tutti i provider SAML nell'account corrente.
- `aoss:GetSecurityConfig`: visualizza le informazioni sul provider SAML.
- `aoss:UpdateSecurityConfig`: modifica una determinata configurazione del provider SAML, inclusi i metadati XML.
- `aoss:DeleteSecurityConfig`: elimina un provider SAML.

La seguente policy di accesso basata sull'identità consente a un utente di gestire tutte le configurazioni dell'IdP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:CreateSecurityConfig",
                "aoss:DeleteSecurityConfig",
                "aoss:GetSecurityConfig",
                "aoss:UpdateSecurityConfig",
                "aoss:ListSecurityConfigs"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Nota bene: l'elemento `Resource` deve essere un carattere jolly.

Creazione di provider SAML (console)

Queste fasi spiegano come creare provider SAML. Ciò consente l'autenticazione SAML con l'autenticazione avviata dal provider di servizi (SP) per le dashboard. OpenSearch L'autenticazione avviata dall'IdP non è supportata.

Per abilitare l'autenticazione SAML per le dashboard OpenSearch

1. Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel pannello di navigazione a sinistra, espandi Serverless e scegli SAML authentication (Autenticazione SAML).
3. Scegli Add SAML provider (Aggiungi provider SAML).
4. Fornisci un nome e una descrizione per il provider.

   > **Note**
   >
   > Il nome specificato è accessibile pubblicamente e verrà visualizzato in un menu a discesa quando gli utenti accedono alle OpenSearch dashboard. Assicurati che il nome sia facilmente riconoscibile e non riveli informazioni sensibili sul tuo provider di identità.

5. In Configure your IdP (Configura il tuo IdP), copia l'URL Assertion consumer service (ACS).
6. Utilizza l'URL ACS che hai appena copiato per configurare il provider di identità. La terminologia e le fasi variano in base al provider. Consultare la documentazione del provider.

   In Okta, ad esempio, crei una "applicazione Web SAML 2.0" e specifichi l'URL ACS come l'URL di Single Sign-On, l'URL del destinatario e l'URL di destinazione. Per Auth0, lo specifichi negli URL di callback consentiti.
7. Se il tuo IdP prevede un campo apposito, fornisci la restrizione per il pubblico. La restrizione per il pubblico è un valore all'interno dell'asserzione SAML che specifica a chi è destinata

l'asserzione. Per OpenSearch Serverless, specifica. `aws:opensearch:<aws account id>` Ad esempio, `aws:opensearch:123456789012`.

Il nome del campo della restrizione per il pubblico varia in base al provider. Per Okta è l'URI del pubblico (ID entità SP). Per IAM Identity Center è il pubblico SAML dell'applicazione.

8. Se si utilizza IAM Identity Center, è necessario anche specificare la seguente mappatura degli attributi: `Subject=${user:name}`, con un formato `unspecified`.
9. Dopo aver configurato il provider di identità, viene generato un file di metadati IdP. Questo file XML contiene informazioni sul provider, ad esempio un certificato TLS, endpoint Single Sign-On e l'ID entità del provider di identità.

   Copia il testo nel file di metadati dell'IdP e incollalo nel campo Provide metadata from your IdP (Fornisci metadati dal tuo IdP). In alternativa, scegliere Importa da file XML e caricare il file. Il file dei metadati dovrebbe avere un aspetto simile al seguente:

```
<?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. Mantieni vuoto il campo dell'attributo ID utente personalizzato per utilizzare l'`NameID`elemento dell'asserzione SAML per il nome utente. Se l'asserzione non utilizza questo elemento standard e include invece il nome utente come attributo personalizzato, specificare tale attributo qui. Gli

attributi rispettano la distinzione tra maiuscole e minuscole. È supportato solo un singolo attributo dell'utente.

L'esempio seguente mostra un attributo di sovrascrizione per `NameID` nell'asserzione 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. (Facoltativo) Specifica un attributo personalizzato nel campo Group attribute (Attributo del gruppo), ad esempio `role` o `group`. È supportato solo un singolo attributo del gruppo. Non esiste un attributo del gruppo predefinito. Se non ne specifichi uno, le policy di accesso ai dati possono contenere solo utenti principali.

    L'esempio seguente mostra un attributo del gruppo nell'asserzione SAML:

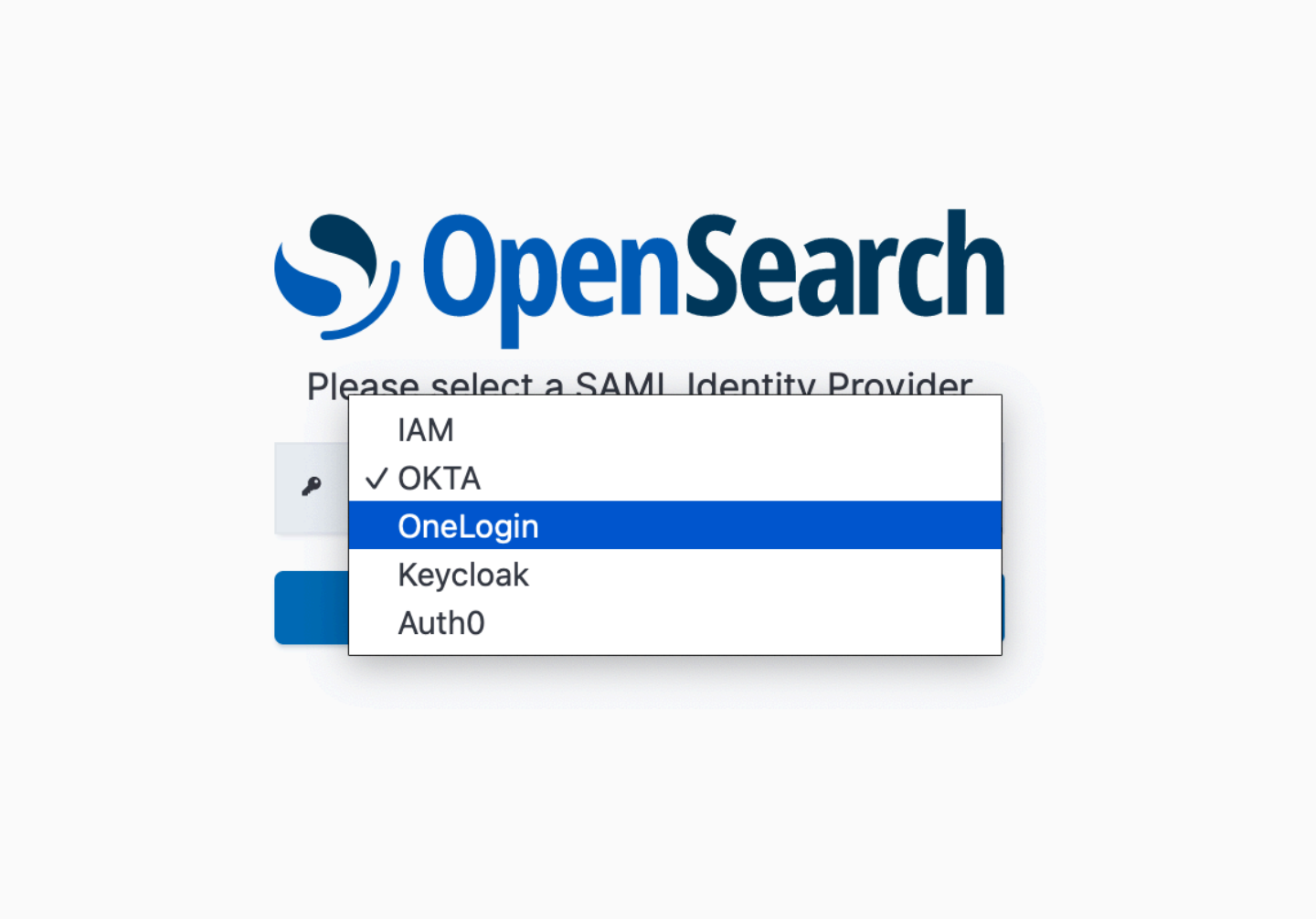
    ```
    <saml2:Attribute Name="department"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">finance</saml2:AttributeValue>
    </saml2:Attribute>
    ```

12. Per impostazione predefinita, OpenSearch Dashboards disconnette gli utenti dopo 24 ore. Puoi configurare questo valore su qualsiasi numero compreso tra 1 e 12 ore (15 e 720 minuti) specificando il timeout del OpenSearch pannello di controllo. Se tenti di impostare il timeout uguale o inferiore a 15 minuti, la sessione verrà reimpostata a un'ora.
13. Scegli Create SAML provider (Crea provider SAML).

Accesso ai pannelli OpenSearch di controllo

Dopo aver configurato un provider SAML, tutti gli utenti e i gruppi associati a tale provider possono accedere all'endpoint OpenSearch Dashboards. L'URL Dashboards ha il formato *collection-endpoint/_dashboards/* per tutte le raccolte.

Se hai abilitato SAML, selezionando il link in basso verrai AWS Management Console indirizzato alla pagina di selezione IdP, dove puoi accedere utilizzando le tue credenziali SAML. Innanzitutto, utilizza il menu a discesa per selezionare un provider di identità:



Quindi accedi utilizzando le tue credenziali IdP.

Se non hai abilitato SAML, selezionando il link nelle AWS Management Console istruzioni potrai accedere come utente o ruolo IAM, senza alcuna opzione per SAML.

Concessione alle identità SAML dell'accesso ai dati della raccolta

Dopo aver creato un provider SAML, è comunque necessario concedere agli utenti e ai gruppi sottostanti l'accesso ai dati all'interno delle raccolte. L'accesso viene concesso tramite le policy di accesso ai dati. Finché non fornisci l'accesso agli utenti, questi non saranno in grado di leggere, scrivere o eliminare alcun dato contenuto nelle raccolte.

Per concedere l'accesso, crea una policy di accesso ai dati e specifica gli ID utente e/o di gruppo SAML nell'istruzione `Principal`:

```
[
   {
      "Rules":[
       ...
      ],
      "Principal":[
         "saml/987654321098/myprovider/user/Shaheen",
         "saml/987654321098/myprovider/group/finance"
      ]
   }
]
```

Puoi concedere l'accesso a raccolte, a indici o a entrambi. Se desideri che utenti diversi dispongano di autorizzazioni diverse, crea più regole. Per un elenco di autorizzazioni disponibili, consulta la sezione Supported policy permissions (Autorizzazioni di policy supportate). Per ulteriori informazioni sul formato di una policy di accesso, consulta la sezione Policy syntax (Sintassi della policy).

Creazione di provider SAML (AWS CLI)

Per creare un provider SAML utilizzando l'API OpenSearch Serverless, invia una richiesta: CreateSecurityConfig

```
aws opensearchserverless create-security-config \
    --name myprovider \
    --type saml \
    --saml-options file://saml-auth0.json
```

Specifica `saml-options`, inclusi i metadati XML, come una mappa chiave-valore all'interno di un file .json. I metadati XML devono essere codificati come stringa con escape JSON.

```
{
   "sessionTimeout": 70,
   "groupAttribute": "department",
   "userAttribute": "userid",
   "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>"
}
```

Visualizzazione di provider SAML

La seguente ListSecurityConfigsrichiesta elenca tutti i provider SAML presenti nel tuo account:

```
aws opensearchserverless list-security-configs --type saml
```

La richiesta restituisce informazioni su tutti i provider SAML esistenti, inclusi i metadati completi dell'IdP generati dal provider di identità:

```
{
   "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"
         }
      }
   ]
}
```

Per visualizzare i dettagli su un provider specifico, inclusa la `configVersion` per gli aggiornamenti futuri, invia una richiesta `GetSecurityConfig`.

Aggiornamento dei provider SAML

Per aggiornare un provider SAML utilizzando la console OpenSearch Serverless, scegli l'autenticazione SAML, seleziona il tuo provider di identità e scegli Modifica. Puoi modificare tutti i campi, inclusi i metadati e gli attributi personalizzati.

Per aggiornare un provider tramite l'API OpenSearch Serverless, invia una UpdateSecurityConfigrichiesta e includi l'identificatore della politica da aggiornare. Inoltre, è necessario includere una versione di configurazione, che è possibile recuperare utilizzando i

comandi `ListSecurityConfigs` o `GetSecurityConfig`. L'inclusione della versione più recente garantisce di non sovrascrivere inavvertitamente una modifica apportata da qualcun altro.

La seguente richiesta aggiorna le opzioni SAML per un provider:

```
aws opensearchserverless update-security-config \
    --id saml/123456789012/myprovider \
    --type saml \
    --saml-options file://saml-auth0.json \
    --config-version MTY2NDA1MjY4NDQ5M18x
```

Specifica le opzioni di configurazione SAML come mappa chiave-valore all'interno di un file .json.

> **Important**
>
> Gli aggiornamenti alle opzioni SAML non sono incrementali. Se non si specifica un valore per un parametro nell'oggetto `SAMLOptions` quando si effettua un aggiornamento, i valori esistenti verranno sostituiti da valori vuoti. Ad esempio, se la configurazione corrente contiene un valore per `userAttribute`, e poi si effettua un aggiornamento e non lo si include, il valore viene rimosso dalla configurazione. Prima di effettuare un aggiornamento, assicurati di conoscere i valori esistenti richiamando l'operazione `GetSecurityConfig`.

Eliminazione di provider SAML

Quando elimini un provider SAML, qualsiasi riferimento a utenti e gruppi associati nelle policy di accesso ai dati non è più funzionale. Per evitare confusione, nelle policy di accesso ti suggeriamo di rimuovere tutti i riferimenti all'endpoint prima di eliminarlo.

Per eliminare un provider SAML utilizzando la console OpenSearch Serverless, scegli Autenticazione, seleziona il provider e scegli Elimina.

Per eliminare un provider tramite l'API OpenSearch Serverless, invia una richiesta: DeleteSecurityConfig

```
aws opensearchserverless delete-security-config --id saml/123456789012/myprovider
```

Convalida della conformità per Amazon Serverless OpenSearch

Revisori di terze parti valutano la sicurezza e la conformità di Amazon OpenSearch Serverless nell'ambito di diversi programmi di AWS conformità. Questi programmi includono SOC, PCI e HIPAA.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).

- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Assegnazione di tag alle raccolte Amazon OpenSearch Serverless

I tag consentono di assegnare informazioni artibrarie a una raccolta Amazon OpenSearch Serverless in modo da poter categorizzare e filtrare tali informazioni. Un tag è un'etichetta di metadati assegnata dall'utente o da AWS a una risorsa AWS.

Ciascun tag è formato da una chiave e da un valore, Per i tag assegnati da te, puoi definire la chiave e il valore. Ad esempio, potresti definire la chiave come `stage` e il valore di una risorsa come `test`.

Con i tag, puoi effettuare le seguenti operazioni:

- Identificazione e organizzazione delle risorse AWS. Molti servizi AWS supportano l'assegnazione di tag, perciò è possibile assegnare lo stesso tag a risorse di diversi servizi per indicare che queste sono correlate. Ad esempio, è possibile assegnare a una raccolta OpenSearch Serverless lo stesso tag che si assegna a un dominio del servizio OpenSearch di Amazon.
- Tenere traccia dei costi AWS. Questi tag vengono attivati nel pannello di controllo AWS Billing and Cost Management. AWS usa i tag per categorizzare i costi e fornire un report di allocazione dei costi mensili. Per ulteriori informazioni, consulta la pagina sull'utilizzo dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing.

In OpenSearch Serverless, la risorsa principale è una raccolta. È possibile utilizzare la console del servizio OpenSearch, la AWS CLI, le operazioni dell'API OpenSearch Serverless o gli SDK AWS per aggiungere, gestire e rimuovere tag da una raccolta.

Autorizzazioni richieste

OpenSearch Serverless utilizza le seguenti autorizzazioni AWS Identity and Access Management Access Analyzer (IAM) per applicare tag alle raccolte:

- `aoss:TagResource`
- `aoss:ListTagsForResource`
- `aoss:UntagResource`

Utilizzo dei tag (console)

La console è il modo più semplice per assegnare un tag a una raccolta.

Per creare un tag (console)

1. Accedi alla console del servizio OpenSearch di Amazon all'indirizzo https://console.aws.amazon.com/aos/home.
2. Espandi Serverless nel pannello di navigazione a sinistra e scegli Collections (Raccolte).
3. Seleziona la raccolta a cui aggiungere i tag e passa alla scheda Tag.
4. Scegli Gestisci, quindi seleziona Aggiungi nuovo tag.
5. Inserire una chiave di tag e un valore facoltativo.
6. Seleziona Salva.

Per eliminare un tag, esegui la stessa procedura e scegli Rimuovi nella pagina Gestisci tag.

Per ulteriori informazioni sull'utilizzo della console per il funzionamento con i tag, consulta Editor di tag nella Guida alle operazioni di base della Console di gestione AWS.

Utilizzo dei tag (AWS CLI)

Per assegnare un tag a una raccolta utilizzando la AWS CLI, invia una richiesta 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
```

È possibile visualizzare i tag esistenti per una raccolta con il comando ListTagsForResource:

```
aws opensearchserverless list-tags-for-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
```

È possibile rimuovere i tag da una raccolta usando il comando UntagResource:

```
aws opensearchserverless untag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tag-keys service
```

Operazioni e plugin supportati in Amazon Serverless OpenSearch

Amazon OpenSearch Serverless supporta una varietà di OpenSearch plug-in, nonché un sottoinsieme delle operazioni API di indicizzazione, ricerca e metadati disponibili in. OpenSearch Per limitare l'accesso a determinate operazioni è possibile includere le autorizzazioni nella colonna sinistra della tabella all'interno delle policy di accesso ai dati.

Argomenti

- Operazioni e autorizzazioni API supportate OpenSearch
- OpenSearch Plugin supportati

Operazioni e autorizzazioni API supportate OpenSearch

La tabella seguente elenca le operazioni API supportate da OpenSearch Serverless, insieme alle corrispondenti autorizzazioni relative alle politiche di accesso ai dati:

Autorizzazione della policy di accesso ai dati	OpenSearch operazioni API	Descrizione e avvertenze
`aoss:CreateIndex`	PUT <index>	Creazione di indici. Per ulteriori informazioni, consulta la sezione Creazione di indici.

Autorizzazione della policy di accesso ai dati	OpenSearch operazioni API	Descrizione e avvertenze
		Note Questa autorizzazione si applica anche alla creazione di indici con i dati di esempio nei dashboard. OpenSearch
`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> • TESTA <index>	Descrizione di indici. Per ulteriori informazioni, consulta le seguenti risorse: • Ottenimento di un indice • Ottenimento di una mappatura • Ottenimento di impostazioni • L'indice esiste • Indici CAT (la risposta non include `status` i `health` nostri campi).

Autorizzazione della policy di accesso ai dati	OpenSearch operazioni API	Descrizione e avvertenze
`aoss:WriteDocument`	• <index>ELIMINA /_doc/ <id> • POST <index>/_bulk • POST <index>/_create/<id> (for search collection types only) • POST <index>/_doc • POST <index>/_update/<id> (for search collection types only) • POST _bulk • PUT <index>/_create/<id> (for search collection types only) • PUT <index>/_doc/<id> (for search collection types only)	Scrittura e aggiornamento di documenti. Per ulteriori informazioni, consulta le seguenti risorse: • Bulk • Indicizzazione di dati **Note** Alcune operazioni sono consentite solo per raccolte di tipo SEARCH. Per ulteriori informazioni, consulta the section called “Scelta di un tipo di raccolta”.

Autorizzazione della policy di accesso ai dati	OpenSearch operazioni API	Descrizione e avvertenze
`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	Lettura di documenti. Per ulteriori informazioni, consulta le seguenti risorse: • Esecuzione di analisi del testo • Ottenimento di un documento • Conteggio • Query DSL • Valutazione della classifica • Analisi di API • Spiegazione

Autorizzazione della policy di accesso ai dati	OpenSearch operazioni API	Descrizione e avvertenze
`aoss:DeleteIndex`	DELETE <target>	Eliminazione degli indici. Per ulteriori informazioni, consulta la sezione Eliminazione di indici.
`aoss:UpdateIndex`	• POST _mapping • POST <index>/_mapping/ • POST <index>/_mappings/ • POST <index>/_setting • POST <index>/_settings • POST _setting • POST _settings • PUT _mapping • PUT <index>/_mapping • PUT <index>/_mappings/ • PUT <index>/_setting • PUT <index>/_settings • PUT _setting • PUT _settings	Aggiornamento delle impostazioni dell'indice. Per ulteriori informazioni, consulta le seguenti risorse: • Mappatura • Aggiornamento delle impostazioni
`aoss:CreateCollectionItems`	POST _aliases	Creazione di alias dell'indice. Per ulteriori informazioni, consulta la sezione Creazione di alias.

Autorizzazione della policy di accesso ai dati	OpenSearch operazioni API	Descrizione e avvertenze
`aoss:DescribeCollectionItems`	• GET <index>/_alias/<alias> • GET _alias • GET _alias/<alias> • GET _cat/aliases • 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>	Descrizione di alias e modelli di indice. Per ulteriori informazioni, consulta le seguenti risorse: • Gestione di alias • Modelli di indice

Autorizzazione della policy di accesso ai dati	OpenSearch operazioni API	Descrizione e avvertenze
`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>	Aggiornamento di alias e modelli di indice. Per ulteriori informazioni, consulta le seguenti risorse: • Alias di indice • Modelli di indice
`aoss:DeleteCollectionItems`	• DELETE <index>/_alias/<alias> • DELETE _component_template/<component-template> • DELETE _index_template/<index-template> • DELETE <index>/_aliases/<alias>	Eliminazione di alias e modelli di indice. Per ulteriori informazioni, consulta le seguenti risorse: • Eliminazione di alias • Eliminazione di un modello

OpenSearch Plugin supportati

OpenSearch Le raccolte serverless sono preconfezionate con i seguenti plugin della community. OpenSearch Serverless implementa e gestisce automaticamente i plug-in per tuo conto.

Plug-in di analisi

- ICU Analysis
- Japanese (kuromoji) Analysis

- Korean (Nori) Analysis
- Phonetic Analysis
- Smart Chinese Analysis
- Stempel Polish Analysis
- Ukrainian Analysis

Plug-in mapper

- Mapper Size
- Mapper Murmur3
- Mapper Annotated Text

Plug-in di scripting

- Painless
- Expression
- Mustache

Inoltre, OpenSearch Serverless include tutti i plugin forniti come moduli.

Monitoraggio di Amazon OpenSearch Serverless

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon OpenSearch Serverless e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare OpenSearch Serverless, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia.

  Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

- AWS CloudTrail acquisisce chiamate API ed eventi correlati da parte di o per conto del tuo Account AWS. Distribuisce i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno effettuato la chiamata AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la AWS CloudTrail Guida per l'utente.
- Amazon EventBridge offre un flusso quasi in tempo reale di eventi di sistema che descrivono le modifiche nei tuoi domini OpenSearch di servizio. Puoi creare regole che controllano determinati eventi e attivano azioni automatiche in altri Servizi AWS quando si verificano tali eventi. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Monitoraggio OpenSearch serverless con Amazon CloudWatch

Puoi monitorare l'utilizzo di Amazon OpenSearch Serverless CloudWatch, che raccoglie dati grezzi e li elabora in parametri leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web.

È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

OpenSearch Serverless riporta le seguenti metriche nel namespace. `AWS/AOSS`

Parametro	Descrizione
`ActiveCollection`	Indica se una raccolta è attiva. Un valore pari a 1 significa che la raccolta è in uno stato `ACTIVE`. Questo valore viene emesso dopo la corretta creazione di una raccolta e rimane 1 finché non si elimina la raccolta. Il parametro non può avere un valore pari a 0. Statistiche rilevanti: Max (Massimo) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi

Parametro	Descrizione
`DeletedDocuments`	Il numero totale di documenti eliminati. Statistiche rilevanti: Average (Media), Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenza: 60 secondi
`IndexingOCU`	Il numero di unità di OpenSearch calcolo (OCU) utilizzate per importare i dati di raccolta. Questo parametro si applica a livello di account. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId` Frequenza: 60 secondi
`IngestionDataRate`	La velocità di indicizzazione in GiB al secondo di una raccolta o di un indice. Questo parametro si applica solo alle richieste di indicizzazione in blocco. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenza: 60 secondi

Parametro	Descrizione
`IngestionDocumentErrors`	Il numero totale di errori del documento durante l'importazione di una raccolta o di un indice. Dopo che una richiesta di indicizzazione in blocco è riuscita, le istanze di scrittura elaborano la richiesta e generano errori per tutti i documenti non riusciti all'interno della richiesta. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenza: 60 secondi
`IngestionDocumentRate`	La frequenza al secondo con cui i documenti vengono inseriti in una raccolta o in un indice. Questo parametro si applica solo alle richieste di indicizzazione in blocco. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenza: 60 secondi
`IngestionRequestErrors`	Il numero totale di errori relativi alle richieste di indicizzazione di massa in una raccolta. OpenSearch Serverless emette questa metrica quando una richiesta di indicizzazione di massa fallisce per qualsiasi motivo, ad esempio un problema di autenticazione o disponibilità. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi

Parametro	Descrizione
`IngestionRequestLatency`	La latenza, in secondi, per le operazioni di scrittura in blocco su una raccolta. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi
`IngestionRequestRate`	Il numero totale di operazioni di scrittura in blocco ricevute da una raccolta. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi
`IngestionRequestSuccess`	Il numero totale di operazioni di indicizzazione riuscite su una raccolta. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi

Parametro	Descrizione
`SearchableDocuments`	Il numero totale di documenti ricercabili in una raccolta o in un indice. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenza: 60 secondi
`SearchRequestErrors`	Il numero totale di errori di query al minuto per una raccolta. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi
`SearchRequestLatency`	Il tempo medio, in millisecondi, impiegato per completare un'operazione di ricerca su una raccolta. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi

Parametro	Descrizione
`SearchOCU`	Il numero di unità di OpenSearch calcolo (OCU) utilizzate per cercare i dati della raccolta. Questo parametro si applica a livello di account. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId` Frequenza: 60 secondi
`SearchRequestRate`	Il numero totale di richieste di ricerca al minuto a una raccolta. Statistiche rilevanti: Average (Media), Maximum (Massimo), Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi
`StorageUsedInS3`	La quantità, in byte, di storage Amazon S3 utilizzata. OpenSearch Serverless archivia i dati indicizzati in Amazon S3. È necessario selezionare il periodo in un minuto per ottenere un valore preciso. Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequenza: 60 secondi

Parametro	Descrizione
`2xx, 3xx, 4xx, 5xx`	Il numero di richieste alla raccolta che hanno prodotto il codice di risposta HTTP specificato (2xx, 3xx, 4xx, 5xx). Statistiche rilevanti: Sum (Somma) Dimensioni: `ClientId`, `CollectionId` , `CollectionName` Frequenza: 60 secondi

Registrazione delle chiamate API OpenSearch Serverless utilizzando AWS CloudTrail

Amazon OpenSearch Serverless è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Serverless.

CloudTrail acquisisce tutte le chiamate API per OpenSearch Serverless come eventi. Le chiamate acquisite includono chiamate dalla sezione Serverless della console di OpenSearch servizio e chiamate in codice alle operazioni dell'API OpenSearch Serverless.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Serverless. OpenSearch Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi.

Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a OpenSearch Serverless, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

OpenSearch Informazioni serverless in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando l'attività si verifica in OpenSearch Serverless, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in. Account AWSPer ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi in tuo Account AWS, inclusi gli eventi per OpenSearch Serverless, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS.

Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni OpenSearch Serverless vengono registrate CloudTrail e documentate nel riferimento all'API OpenSearch Serverless. Ad esempio, le chiamate alle `CreateCollection` `DeleteCollection` azioni e generano voci nei file di registro. `ListCollections` CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di stabilire:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle OpenSearch voci dei file di registro serverless

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro.

Un evento rappresenta una singola richiesta da un'origine. Include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono

una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateCollection`azione.


```
{
   "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"
    }
}
```

Monitoraggio degli eventi OpenSearch serverless tramite Amazon EventBridge

Amazon OpenSearch Service si integra con Amazon EventBridge per informarti di determinati eventi che influiscono sui tuoi domini. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Gli stessi eventi vengono inviati anche ad Amazon CloudWatch Events, il predecessore di Amazon EventBridge. Puoi scrivere regole per indicare quali eventi ti interessano e quali azioni automatiche intraprendere quando un evento corrisponde a una regola. Di seguito sono riportati alcuni esempi di azioni che è possibile attivare automaticamente:

- Invocare una funzione AWS Lambda
- Richiamo di un Run Command di Amazon EC2
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un argomento Amazon SNS o di una coda Amazon SQS

Per ulteriori informazioni, consulta la sezione Guida introduttiva ad Amazon EventBridge nella Amazon EventBridge User Guide.

Configurazione delle notifiche

Puoi utilizzare le notificheAWS utente per ricevere notifiche quando si verifica un evento OpenSearch Serverless. Un evento è un indicatore di un cambiamento nell'ambiente OpenSearch Serverless, ad esempio quando si raggiunge il limite massimo di utilizzo dell'OCU. Amazon EventBridge riceve

l'evento e invia una notifica al Centro AWS Management Console notifiche e ai canali di distribuzione scelti. L'utente riceverà una notifica quando un evento corrisponde a una regola specificata.

OpenSearch eventi Compute Units (OCU)

OpenSearch Serverless invia eventi a EventBridge quando si verifica uno dei seguenti eventi relativi all'OCU.

L'utilizzo dell'OCU si avvicina al limite massimo

OpenSearch Serverless invia questo evento quando l'utilizzo dell'OCU per la ricerca o l'indicizzazione raggiunge il 75% del limite di capacità. L'utilizzo dell'OCU viene calcolato in base al limite di capacità configurato e al consumo attuale dell'OCU.

Esempio

Di seguito è riportato un esempio di evento di questo tipo (cerca OCU):

```
{
  "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."
  }
}
```

Di seguito è riportato un esempio di evento di questo tipo (indice OCU):

```
{
  "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."
  }
```

L'utilizzo dell'OCU ha raggiunto il limite massimo

OpenSearch Serverless invia questo evento quando l'utilizzo dell'OCU per la ricerca o l'indice raggiunge il 100% del limite di capacità. L'utilizzo dell'OCU viene calcolato in base al limite di capacità configurato e al consumo attuale dell'OCU.

Esempio

Di seguito è riportato un esempio di evento di questo tipo (cerca OCU):

```
{
  "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."
  }
}
```

Di seguito è riportato un esempio di evento di questo tipo (indice OCU):

```
{
  "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."
  }
}
```

Creazione e gestione di domini Amazon OpenSearch Service

Questo capitolo descrive come creare e gestire i domini Amazon OpenSearch Service. Un dominio è l'equivalente AWS fornito di un cluster open source. OpenSearch Quando si crea un dominio, si specificano le impostazioni, i tipi di istanza, il numero di istanze e l'allocazione dello storage. Per ulteriori informazioni sui cluster open source, consulta Creazione di un cluster nella OpenSearch documentazione.

A differenza delle istruzioni nel tutorial relativo alle nozioni di base, in questo capitolo sono descritte tutte le opzioni e sono fornite le informazioni di riferimento rilevanti. Puoi completare ogni procedura utilizzando le istruzioni per la console OpenSearch di servizio, AWS Command Line Interface (AWS CLI) o gli AWS SDK.

Creazione di domini OpenSearch di servizio

Questa sezione descrive come creare domini OpenSearch di servizio utilizzando la console di OpenSearch servizio o utilizzando il comando AWS CLI with the`create-domain`.

Creazione OpenSearch di domini di servizio (console)

Utilizzare la procedura seguente per creare un dominio OpenSearch di servizio utilizzando la console.

Per creare un dominio OpenSearch di servizio (console)

1. Passare all'indirizzo https://aws.amazon.com e scegliere Sign In to the Console (Accedi alla console).
2. In Analytics, scegli Amazon OpenSearch Service.
3. Scegli Crea dominio.
4. In Domain name (Nome di dominio), immettere un nome di dominio. Il nome deve soddisfare i seguenti criteri:
   - Unico per il tuo account e Regione AWS
   - Inizia con una lettera minuscola
   - Contiene da 3 a 28 caratteri

- Contiene solo lettere minuscole a - z, i numeri da 0 a 9 e i trattini (-)

5. Per il metodo di creazione del dominio, scegli Creazione standard.
6. Per i modelli, scegli l'opzione più adatta allo scopo del tuo dominio:

   - Domini di produzione per carichi di lavoro che richiedono disponibilità e prestazioni elevate. Questi domini utilizzano Multi-AZ (con o senza standby) e nodi master dedicati per una maggiore disponibilità.
   - Sviluppo/test per lo sviluppo o il test. Questi domini possono utilizzare Multi-AZ (con o senza standby) o una singola zona di disponibilità.

   > **Important**
   >
   > I diversi tipi di distribuzione presentano diverse opzioni su pagine successive. Questi passaggi includono tutte le opzioni.

7. Per le opzioni di distribuzione, scegli Dominio con standby per configurare un dominio 3-AZ, con i nodi in una delle zone riservati come standby. Questa opzione applica una serie di best practice, come il numero di nodi di dati specificato, il conteggio dei nodi principali, il tipo di istanza, il numero di repliche e le impostazioni di aggiornamento software.
8. Per Versione, scegli la versione del OpenSearch sistema operativo Elasticsearch precedente da utilizzare. Ti consigliamo di scegliere la versione più recente di. OpenSearch Per ulteriori informazioni, consulta the section called “Versioni supportate”.

   (Facoltativo) Se hai scelto una OpenSearch versione per il tuo dominio, seleziona Abilita la modalità di compatibilità per OpenSearch segnalare la versione 7.10, che consente a determinati client e plugin OSS di Elasticsearch che controllano la versione prima di connettersi di continuare a utilizzare il servizio.
9. Per Tipo di istanza, scegliere un tipo di istanza per i nodi di dati. Per ulteriori informazioni, consultare the section called “Tipi di istanze supportati”.

   > **Note**
   >
   > Non tutte le zone di disponibilità supportano tutti i tipi di istanze. Se scegli Multi-AZ con o senza Standby, ti consigliamo di scegliere i tipi di istanza della generazione attuale, come R5 o I3.

10. In Number of nodes (Numero di nodi), scegliere il numero di nodi di dati.

Per i valori massimi, consulta Quote di dominio e istanza del servizio. OpenSearch I cluster a nodo singolo sono ideali per lo sviluppo e i test, ma non devono essere utilizzati per i carichi di lavoro di produzione. Per ulteriori linee guida, consulta the section called “Dimensionamento dei domini” e the section called “Configurazione di un dominio Multi-AZ”.

11. Per Tipo di storage, seleziona Amazon EBS. I tipi di volume disponibili nell'elenco dipendono dal tipo di istanza scelta. Per istruzioni su come creare domini di grandi dimensioni, consultare the section called “Scala in petabyte”.
12. Per lo storage EBS, configura le seguenti impostazioni aggiuntive. Alcune impostazioni potrebbero non essere visualizzate a seconda del tipo di volume scelto.

Impostazione	Descrizione
Tipi di volume EBS	Scegli tra Scopo generico (SSD) - gp3 e Scopo generico (SSD) - gp2 o la generazione precedente Capacità di IOPS allocata (SSD) e Magnetico (standard).
Dimensioni dello storage EBS per ogni nodo	Inserisci le dimensioni del volume EBS da collegare a ogni nodo di dati. EBS volume size (Dimensione del volume EBS) è per nodo. È possibile calcolare la dimensione totale del cluster per il dominio del OpenSearch servizio moltiplicando il numero di nodi di dati per la dimensione del volume EBS. Le dimensioni minime e massime di un volume EBS dipendono sia dal tipo di volume EBS specificato sia dal tipo di istanza collegata. Per ulteriori informazioni, consulta Limiti delle dimensioni dei volumi EBS.
IOPS con provisioning	Se hai selezionato un tipo di volume SSD con capacità di IOPS allocata, inserisci il numero di operazioni I/O al secondo (IOPS) supportate dal volume.

13. (Facoltativo) Se hai selezionato un tipo di gp3 volume, espandi le Impostazioni avanzate e specifica IOPS (fino a 16.000 per ogni dimensione di volume da 3 TiB fornita per nodo di dati) e velocità effettiva (fino a 1.000 MIB/s per ogni volume da 3 TiB fornito per nodo di dati) oltre a quanto incluso nel prezzo dello storage, a un costo aggiuntivo. Per ulteriori informazioni, consulta i prezzi OpenSearch di Amazon Service.

14. (Facoltativo) Per abilitare UltraWarm lo storage, scegli Abilita nodi di UltraWarm dati. Ogni tipo di istanza ha una quantità massima di spazio di archiviazione che può indirizzare. Moltiplicare tale importo per il numero di nodi di dati a caldo per l'archiviazione a caldo indirizzabile totale.
15. (Facoltativo) Per abilitare l'archiviazione a freddo, scegliere Abilita archiviazione a freddo. È necessario abilitare UltraWarm per abilitare la conservazione a freddo.
16. Se si utilizza Multi-AZ con Standby, tre nodi master dedicati sono già abilitati. Scegli il tipo di nodi master che desideri. Se hai scelto un dominio Multi-AZ senza Standby, seleziona Abilita nodi master dedicati e scegli il tipo e il numero di nodi master che desideri. I nodi master dedicati aumentano la stabilità del cluster e sono richiesti per domini con un conteggio istanze superiore a 10. Per i domini di produzione consigliamo tre nodi master dedicati.

    > **Note**
    >
    > È possibile scegliere tra tipi di istanze differenti per nodi master dedicati e nodi di dati. Ad esempio, è possibile selezionare istanze generiche o ottimizzate per l'archiviazione per i nodi di dati e scegliere istanze ottimizzate per l'elaborazione per i nodi principali dedicati.

17. (Facoltativo) Per i domini che eseguono OpenSearch Elasticsearch 5.3 e versioni successive, la configurazione Snapshot è irrilevante. Per ulteriori informazioni sugli snapshot automatici, consulta the section called “Creazione di snapshot di indici”.
18. Se si desidera utilizzare un endpoint personalizzato anziché quello standard di `https://search-`*`mydomain`*`-`*`1a2a3a4a5a6a7a8a9a0a9a8a7a`*`.`*`us-east-1`*`.es.amazonaws.com`, scegliere Abilita endpoint personalizzato e fornire un nome e un certificato. Per ulteriori informazioni, consulta the section called “Creazione di un endpoint personalizzato”.
19. In Rete, scegliere Accesso VPC o Accesso pubblico. Se si sceglie Public access (Accesso pubblico), andare al passaggio successivo. Se si sceglie Accesso VPC, è necessario accertarsi di soddisfare tutti i prerequisiti e configurare le seguenti impostazioni:

Impostazione	Descrizione
VPC	Scegli l'ID per il cloud privato virtuale (VPC) da utilizzare. Il VPC e il dominio devono essere uguali Regione AWS ed è necessario seleziona re un VPC con tenancy impostata su Default. OpenSearch Il servizio non supporta ancora i VPC che utilizzano una locazione dedicata.

Impostazione	Descrizione
Sottorete	Scegli una sottorete. Se hai abilitato Multi-AZ, devi scegliere due o tre sottoreti. OpenSearch Il servizio inserirà un endpoint VPC e interfacce di rete elastiche nelle sottoreti. È necessario riservare un numero sufficiente di indirizzi IP per le interfacc e di rete nelle sottoreti. Per ulteriori informazioni, consultare Prenotazione di indirizzi IP in una sottorete VPC.
Gruppi di sicurezza	Scegli uno o più gruppi di sicurezza VPC che consentano all'applicazione richiesta di raggiungere il dominio del OpenSearch servizio sulle porte (80 o 443) e sui protocolli (HTTP o HTTPS) esposti dal dominio. Per ulteriori informazioni, consulta the section called “Supporto per VPC”.
Ruolo IAM	Mantieni il ruolo predefinito. OpenSearch Il servizio utilizza questo ruolo predefinito (noto anche come ruolo collegato al servizio) per accedere al VPC e posizionare un endpoint VPC e interfacce di rete nella sottorete del VPC. Per ulteriori informazioni, consultare Ruolo collegato ai servizi per l'accesso VPC.
Tipo di indirizzo IP	Scegli dual stack o IPv4 come tipo di indirizzo IP. Il dual stack consente di condividere le risorse del dominio tra i tipi di indirizzi IPv4 e IPv6 ed è l'opzione consigliata. Se imposti il tipo di indirizzo IP su dual stack, non puoi modificare il tipo di indirizzo in un secondo momento.

20. Abilitare o disabilitare il controllo granulare degli accessi:

    - Se si desidera utilizzare IAM per la gestione degli utenti, scegliere Imposta ARN IAM come utente principale e specificare l'ARN per un ruolo IAM.
    - Se desideri utilizzare il database utenti interno, scegli Crea utente principale e specifica un nome utente e una password.

    Indipendentemente dall'opzione scelta, l'utente master può accedere a tutti gli indici del cluster e a tutte le API. OpenSearch Per informazioni su quale opzione scegliere, vedere the section called “Concetti chiave”.

Se si disattiva il controllo granulare degli accessi, è comunque possibile controllare l'accesso al dominio inserendolo in un VPC, applicando una policy di accesso restrittivo o entrambi. È necessario abilitare la node-to-node crittografia e la crittografia a riposo per utilizzare un controllo granulare degli accessi.

> **Note**
>
> Si consiglia fortemente di abilitare il controllo granulare degli accessi per proteggere i dati sul dominio. Il controllo granulare degli accessi fornisce protezione a livello di cluster, indice, documento e campo.

21. (Facoltativo) Se desideri utilizzare l'autenticazione SAML per le OpenSearch dashboard, scegli Abilita l'autenticazione SAML e configura le opzioni SAML per il dominio. Per istruzioni, consulta the section called “Autenticazione SAML per dashboard OpenSearch ”.
22. (Facoltativo) Se desideri utilizzare l'autenticazione Amazon Cognito per OpenSearch dashboard, scegli Abilita l'autenticazione Amazon Cognito. Quindi scegli il pool di utenti e il pool di identità di Amazon Cognito che desideri utilizzare per l'autenticazione di OpenSearch Dashboards. Per ulteriori informazioni sulla creazione di queste risorse, consultare the section called “Autenticazione Amazon Cognito per dashboard OpenSearch ”.
23. Per la policy di accesso, scegli una policy di accesso o configurane una personalizzata. Se si sceglie di creare una policy personalizzata, è possibile configurarla manualmente o importarne una da un altro dominio. Per ulteriori informazioni, consultare the section called “Identity and Access Management”.

> **Note**
>
> Se è stato abilitato l'accesso VPC, non è possibile utilizzare policy basate su IP. Invece è possibile utilizzare i gruppi di sicurezza per controllare gli indirizzi IP che possono accedere al dominio. Per ulteriori informazioni, consultare the section called “Informazioni sulle policy d'accesso nei domini VPC”.

24. (Facoltativo) Per richiedere che tutte le richieste al dominio arrivino tramite HTTPS, selezionare Richiedi HTTPS per tutto il traffico verso il dominio. Per abilitare node-to-node la crittografia, seleziona ode-to-nodeCrittografia N. Per ulteriori informazioni, consulta the section called “Nessuna ode-to-node crittografia”. Per abilitare la crittografia dei dati inattivi, seleziona Abilita

la crittografia dei dati inattivi. Queste opzioni sono preselezionate se hai scelto l'opzione di implementazione Multi-AZ with Standby.

25. (Facoltativo) Seleziona Usa chiave AWS proprietaria per fare in modo che OpenSearch Service crei una chiave di AWS KMS crittografia per tuo conto (o utilizzi quella che ha già creato). In caso contrario, scegliere la propria chiave KMS. Per ulteriori informazioni, consulta the section called “Crittografia a riposo”.
26. Per la finestra non di punta, seleziona un orario di inizio per pianificare gli aggiornamenti del software di servizio e le ottimizzazioni Auto-Tune che richiedono un'implementazione blu/verde. Gli aggiornamenti non di punta aiutano a ridurre al minimo il carico sui nodi master dedicati di un cluster durante i periodi di traffico elevato.
27. Per Auto-Tune, scegli se consentire al OpenSearch Servizio di suggerire modifiche alla configurazione relative alla memoria del tuo dominio per migliorare la velocità e la stabilità. Per ulteriori informazioni, consulta the section called “Regolazione automatica”.

    (Facoltativo) Seleziona Finestra Off-peak per pianificare una finestra ricorrente durante la quale Auto-Tune aggiorna il dominio.
28. (Facoltativo) Seleziona Aggiornamento software automatico per abilitare gli aggiornamenti software automatici.
29. (Facoltativo) Aggiungere i tag per descrivere il dominio in modo da poter categorizzare e filtrare in base a tali informazioni. Per ulteriori informazioni, consultare the section called “Assegnazione di tag ai domini”.
30. (Facoltativo) Espandi e configura Impostazioni avanzate del cluster. Per un riepilogo di queste opzioni, vedere the section called “Impostazioni avanzate del cluster”.
31. Scegli Crea.

Creazione OpenSearch di domini di servizio ()AWS CLI

Invece di creare un dominio di OpenSearch servizio utilizzando la console, è possibile utilizzare il AWS CLI. Per la sintassi, consulta Amazon OpenSearch Service nel riferimento ai comandi AWS CLI a.

Comandi di esempio

Questo primo esempio dimostra la seguente configurazione del dominio di OpenSearch servizio:

- Crea un dominio OpenSearch di servizio denominato mylogs con la versione 1.2 OpenSearch

- Popola il dominio con due istanze del tipo `r6g.large.search`
- Utilizza un volume EBS a scopo generico (SSD) gp3 da 100 GiB per lo storage di ogni nodo di dati
- Consente l'accesso anonimo, ma solo da un solo indirizzo 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"]}}}]}'
```

L'esempio successivo mostra la seguente configurazione del dominio di OpenSearch servizio:

- Crea un dominio di OpenSearch servizio denominato mylogs con Elasticsearch versione 7.10
- Popola il dominio con sei istanze del tipo `r6g.large.search`
- Utilizza un volume EBS a scopo generico (SSD) gp2 da 100 GiB per lo storage di ogni nodo di dati
- Limita l'accesso al servizio a un singolo utente, identificato dall'ID dell'utente: 5555 Account AWS
- Distribuisce istanze in tre zone di disponibilità

```
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/*" } ] }'
```

L'esempio successivo mostra la seguente configurazione del dominio di OpenSearch servizio:

- Crea un dominio OpenSearch di servizio denominato mylogs con la versione 1.0 OpenSearch
- Popola il dominio con dieci istanze del tipo `r6g.xlarge.search`

- Popola il dominio con tre istanze del tipo `r6g.large.search` per fungere come nodi master dedicati
- Utilizza un volume EBS con capacità di IOPS allocata di 100 GiB per lo storage, configurato con prestazioni di base di 1.000 IOPS per ogni nodo di dati
- Limita l'accesso a un singolo utente e a una sola subresource, l'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**
>
> Se si tenta di creare un dominio di OpenSearch servizio ed esiste già un dominio con lo stesso nome, la CLI non riporta alcun errore. Restituisce invece i dettagli per il dominio esistente.

Creazione OpenSearch di domini di servizio (SDK)AWS

Gli AWS SDK (eccetto gli SDK per Android e iOS) supportano tutte le azioni definite nell'Amazon OpenSearch Service API Reference, tra cui. `CreateDomain` Per il codice di esempio, consulta the section called “Uso degli SDK AWS”. Per ulteriori informazioni sull'installazione e l'utilizzo degli AWS SDK, consulta AWS Software Development Kits.

Creazione di domini OpenSearch di servizio ()AWS CloudFormation

OpenSearch Il servizio è integrato con AWS CloudFormation, un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive il OpenSearch dominio che desideri creare e CloudFormation predispone e configura il dominio per te. Per ulteriori informazioni, inclusi esempi

di modelli JSON e YAML per OpenSearch domini, consulta il riferimento ai tipi di risorse di Amazon OpenSearch Service nella Guida per l'utente.AWS CloudFormation

Configurazione delle policy di accesso

Amazon OpenSearch Service offre diversi modi per configurare l'accesso ai tuoi domini OpenSearch di servizio. Per ulteriori informazioni, consultare the section called “Identity and Access Management” e the section called “Controllo granulare degli accessi”.

La console offre le policy d'accesso preconfigurate che è possibile personalizzare per le esigenze specifiche del dominio. Puoi anche importare politiche di accesso da altri domini OpenSearch di servizio. Per informazioni su come queste policy d'accesso interagiscono con l'accesso VPC, consulta the section called “Informazioni sulle policy d'accesso nei domini VPC”.

Per configurare le policy d'accesso (console)

1. Andare all'indirizzo https://aws.amazon.com e quindi scegliere Sign In to the Console (Accedi alla console).
2. In Analytics, scegli Amazon OpenSearch Service.
3. Nel pannello di navigazione, in Domini, scegli il dominio che desideri aggiornare.
4. Scegli Operazioni, quindi Modifica configurazione di sicurezza.
5. Modifica il JSON della policy di accesso o importa un'opzione preconfigurata.
6. Seleziona Salvataggio delle modifiche.

Impostazioni avanzate del cluster

Utilizzare le opzioni avanzate per configurare:

Indici nei corpi delle richieste

Specifica se i riferimenti espliciti agli indici sono permessi all'interno del corpo delle richieste HTTP. L'impostazione di questa proprietà su `false` impedisce agli utenti di aggirare il controllo degli accessi per le risorse secondarie. Per impostazione predefinita, il valore è `true`. Per ulteriori informazioni, consultare the section called “Opzioni avanzate e considerazioni sulle API”.

Allocazione della cache dei dati di campo

Specifica la percentuale di spazio heap Java allocata ai dati del campo. Per impostazione predefinita, questa impostazione è il 20% dell'heap JVM.

> **Note**
>
> Molte query dei clienti effettuano la rotazione degli indici giornalieri. È consigliabile iniziare i test di benchmark con `indices.fielddata.cache.size` configurato al 40% dell'heap JVM per la maggior parte dei casi d'uso. Tuttavia, se si dispone di indici di grandi dimensioni, potrebbe essere necessaria una cache dei dati del campo di grandi dimensioni.

Numero massimo di clausole

Specifica il numero massimo di clausole permesse in una query booleana Lucene. Il valore di default è 1.024. Le query con un numero di clausole superiore a quello permesso generano un errore `TooManyClauses`. Per ulteriori informazioni, consultare la documentazione di Lucene.

Apportare modifiche alla configurazione in Amazon OpenSearch Service

Amazon OpenSearch Service utilizza un processo di distribuzione blu/verde per l'aggiornamento dei domini. Una distribuzione blu/verde crea un ambiente inattivo per gli aggiornamenti del dominio che copia l'ambiente di produzione e indirizza gli utenti al nuovo ambiente una volta completati gli aggiornamenti. In un'implementazione blu/verde, l'ambiente blu è l'ambiente di produzione corrente. L'ambiente verde è l'ambiente inattivo.

I dati vengono migrati dall'ambiente blu all'ambiente verde. Quando il nuovo ambiente è pronto, OpenSearch Service passa da un ambiente all'altro per far sì che l'ambiente verde diventi il nuovo ambiente di produzione. Il passaggio avviene senza perdita di dati. Questa pratica riduce al minimo i tempi di inattività e mantiene l'ambiente originale nel caso in cui l'implementazione nel nuovo ambiente non abbia esito positivo.

Argomenti

- Modifiche che di solito causano implementazioni blu/verde

Modifiche che di solito causano implementazioni blu/verde

Le seguenti operazioni causano distribuzioni blu/verde:

- Modifica del tipo di istanza
- Abilitazione del controllo granulare degli accessi
- Esecuzione degli aggiornamenti software del servizio
- Abilitazione o disabilitazione di nodi master dedicati
- Abilitazione o disabilitazione di Multi-AZ senza Standby
- Modifica del tipo di archiviazione, del tipo di volume o della dimensione del volume
- Scelta di sottoreti VPC diverse
- Aggiunta o rimozione di gruppi di sicurezza VPC
- Abilitazione o disabilitazione dell'autenticazione Amazon Cognito per dashboard OpenSearch
- Scelta di un bacino d'utenza o pool di identità di Amazon Cognito differente
- Modifica delle impostazioni avanzate
- Aggiornamento a una nuova OpenSearch versione (le OpenSearch dashboard potrebbero non essere disponibili durante tutto o in parte l'aggiornamento)
- Attivazione della crittografia dei dati archiviati o della crittografia node-to-node
- Attivazione UltraWarm o disabilitazione della conservazione a freddo
- Disabilitazione della regolazione automatica e rollback delle sue modifiche
- Associazione di un plug-in opzionale a un dominio e dissociazione di un plug-in opzionale da un dominio
- Aumento del numero di nodi master dedicati per i domini Multi-AZ con due nodi master dedicati

- Riduzione della dimensione del volume EBS
- Modifica delle dimensioni, degli IOPS o del throughput del volume EBS, se l'ultima modifica apportata è in corso o è avvenuta meno di 6 ore fa
- Attivazione della pubblicazione dei registri di controllo su. CloudWatch

Per i domini Multi-AZ con standby, è possibile effettuare solo una richiesta di modifica alla volta. Se è già in corso una modifica, la nuova richiesta viene rifiutata. Puoi controllare lo stato della modifica corrente con l'`DescribeDomainChangeProgress`API.

Modifiche che di solito non causano implementazioni blu/verde

Nella maggior parte dei casi, le seguenti operazioni non causano distribuzioni blu/verdi:

- Modifica della politica di accesso
- Modifica dell'endpoint personalizzato
- Modifica della politica Transport Layer Security (TLS)
- Modifica dell'orario di uno snapshot automatico
- Abilitazione o disabilitazione di Require HTTPS (Richiedi HTTPS)
- Abilitazione della regolazione automatica senza il rollback delle sue modifiche
- Se il tuo dominio dispone di nodi master dedicati, modifica del nodo di dati o del numero di UltraWarm nodi
- Se il dominio dispone di nodi master dedicati, modifica del tipo o del numero di istanze master dedicate (ad eccezione dei domini Multi-AZ con due nodi master dedicati)
- Abilitazione o disabilitazione della pubblicazione dei log degli errori o degli slow log su CloudWatch
- Disattivazione della pubblicazione dei registri di controllo su CloudWatch
- Aumento della dimensione del volume fino a 3 TiB per nodo di dati, modifica del tipo di volume, degli IOPS o della velocità effettiva
- Aggiunta e rimozione di tag

> **Note**
>
> Esistono alcune eccezioni a seconda della versione del software di servizio. Se vuoi essere sicuro che una modifica non provochi una distribuzione blu/verde, esegui un'operazione a secco prima di aggiornare il dominio, se questa opzione è disponibile. Alcune modifiche non

offrono l'opzione dry run. In genere consigliamo di apportare modifiche al cluster al di fuori delle ore di traffico di punta.

Determinazione se una modifica causerà una implementazione blu/verde

Puoi testare alcuni tipi di modifiche alla configurazione pianificate per determinare se causeranno una distribuzione blu/verde, senza doverti impegnare ad apportare tali modifiche. Prima di avviare una modifica della configurazione, utilizza la console o un'API per eseguire un controllo di convalida per garantire che il dominio sia idoneo per un aggiornamento.

Console

Per convalidare una modifica alla configurazione

1. Accedi alla console di Amazon OpenSearch Service all'indirizzohttps://console.aws.amazon.com/aos/.
2. Nel riquadro di navigazione a sinistra, scegli Domains (Domini).
3. Seleziona il dominio per cui desideri avviare una modifica della configurazione. Si apre la pagina dei dettagli del dominio. Seleziona il menu a discesa Actions (Operazioni), quindi scegli Edit cluster configuration (Modifica configurazione cluster).
4. Nella pagina Edit cluster configuration (Modifica configurazione cluster), è possibile apportare modifiche al tipo di istanza, al numero di nodi e a qualsiasi altra configurazione. Dopo aver confermato le modifiche nel pannello di riepilogo, scegli Run (Esegui).
5. Una volta completato il test, i risultati vengono visualizzati automaticamente nella parte inferiore della pagina, insieme a un ID di test. Questi risultati indicano in quale categoria rientra la modifica:

   - Avvia una implementazione blu/verde
   - Non richiede un'implementazione blu/verde
   - Contiene errori di convalida che è necessario correggere prima di poter salvare le modifiche

   Tieni presente che ogni test sovrascrive quello precedente. Per cercare i dettagli di ogni test in un secondo momento, assicurati di salvare il tuo ID test. Ogni test è disponibile per 90 giorni o fino a quando non si effettua un aggiornamento della configurazione.

6. Per procedere con l'aggiornamento della configurazione, scegli Save changes (Salva modifiche). Altrimenti, scegli Cancel (Annulla). Entrambe le opzioni riportano alla scheda Cluster configuration (Configurazione del cluster). In questa scheda, puoi scegliere Dry run details (Dettagli del test) per visualizzare i dettagli del tuo ultimo test. Questa pagina include anche un side-by-side confronto tra la configurazione prima del funzionamento a secco e la configurazione del funzionamento a secco.

API

È possibile eseguire la convalida del test di analisi anche tramite l'API di configurazione. Per testare le modifiche con l'API, imposta `DryRun` su `true` e `DryRunMode` su `Verbose`. La modalità verbosa esegue un controllo di convalida oltre a determinare se la modifica avvierà una implementazione blu/verde. Ad esempio, questa UpdateDomainConfigrichiesta verifica il tipo di distribuzione risultante dall'attivazione di 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 richiesta esegue un controllo di convalida e restituisce il tipo di implementazione che sarà causata dalla modifica ma non esegue effettivamente l'aggiornamento:

```
{
   "ClusterConfig": {
     ...
    },
   "DryRunResults": {
      "DeploymentType": "Blue/Green",
      "Message": "This change will require a blue/green deployment."
    }
}
```

I possibili tipi di implementazione sono:

- `Blue/Green`: la modifica causerà una implementazione blu/verde.
- `DynamicUpdate`: la modifica non causerà una implementazione blu/verde.
- `Undetermined`: il dominio è ancora in stato di elaborazione, quindi non è possibile determinare il tipo di implementazione.
- `None`: nessuna modifica alla configurazione.

Se la convalida non riesce, viene restituito un elenco di errori di convalida.

```
{
   "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."
         }
      ]
   }
}
```

Se lo stato è fisso`pending`, puoi utilizzare l'ID dry run nella UpdateDomainConfig risposta alle DescribeDryRunProgresschiamate successive per verificare lo stato della convalida.

```
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."
    }
}
```

Per eseguire un test senza un controllo di convalida, imposta `DryRunMode` su `Basic` quando usi l'API di configurazione.

Python

Il seguente codice Python utilizza l'UpdateDomainConfigAPI per eseguire un controllo di convalida dell'esecuzione a secco e, se il controllo ha esito positivo, chiama la stessa API senza esecuzione a secco per avviare l'aggiornamento. Se il controllo fallisce, lo script stampa l'errore e si interrompe.

```
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)
```

Avvio e monitoraggio di una modifica alla configurazione

> **Note**
>
> È possibile richiedere una modifica alla configurazione alla volta. Puoi anche raggruppare più modifiche alla configurazione in un'unica richiesta. Attendi che diventi lo stato del tuo dominio `Active` prima di richiedere ulteriori modifiche alla configurazione.

Puoi visualizzare i campi Domain Processing Status e Config Change Status nella console di Amazon OpenSearch Service per tenere traccia delle modifiche al dominio e alla configurazione. Puoi anche tenere traccia delle modifiche al dominio e alla configurazione tramite i `ConfigChangeStatus` parametri `DomainProcessingStatus` e nelle risposte API. Per ulteriori informazioni, consulta il tipo di DomainStatusdati nel riferimento all'API di OpenSearch servizio.

Visibilità dello stato di elaborazione del dominio: è possibile determinare facilmente lo stato di configurazione di un dominio esaminando il campo Domain Processing Status nella console. Allo

stesso modo, il parametro `DomainProcessingStatus` API può essere utilizzato per identificare lo stato. I seguenti valori rappresentano gli stati di elaborazione per un dominio:

- `Active`: non è in corso alcuna modifica alla configurazione. È possibile inviare una nuova richiesta di modifica della configurazione.
- `Creating`: Il dominio è in fase di creazione.
- `Modifying`: sono in corso modifiche alla configurazione, come l'aggiunta di nuovi nodi di dati, EBS, gp3, il provisioning IOPS o la configurazione di chiavi KMS.

  > **Note**
  >
  > Potresti vedere lo stato come `Modifying` in situazioni in cui un dominio richiede lo spostamento degli shard per completare le modifiche alla configurazione. Per motivi di compatibilità con le versioni precedenti, il comportamento del `Processing` parametro viene mantenuto invariato nelle risposte dell'API e viene impostato su false non appena vengono completate le modifiche alla configurazione di base, senza attendere il completamento del movimento dello shard.

- `Upgrading Engine Version`: è in corso un aggiornamento della versione del motore.
- `Updating Service Software`: è in corso un aggiornamento del software di servizio.
- `Deleting`: Il dominio viene eliminato.
- `Isolated`: il dominio è sospeso.

Visibilità dello stato della configurazione: le modifiche alla configurazione possono essere avviate dall'operatore (ad esempio aggiunta di nuovi nodi dati, modifica del tipo di istanza) o dal servizio (ad esempio Auto-Tune e aggiornamenti nelle ore non di punta). Puoi trovare lo stato delle ultime modifiche alla configurazione nel campo Configuration Change Status della console di Amazon OpenSearch Service e nella risposta dell'`ConfigChangeStatus`API. I seguenti valori indicano lo stato di configurazione di un dominio:

- `Pending`: è stata inviata una richiesta di modifica della configurazione.
- `Initializing`: Il servizio sta inizializzando una richiesta di modifica della configurazione.
- `Validating`: Il servizio sta convalidando le modifiche richieste e le risorse richieste.
- `Awaiting user inputs`: Si applica quando l'operatore prevede che alcune modifiche alla configurazione, ad esempio la modifica del tipo di istanza, procedano ulteriormente. È possibile modificare le modifiche alla configurazione.

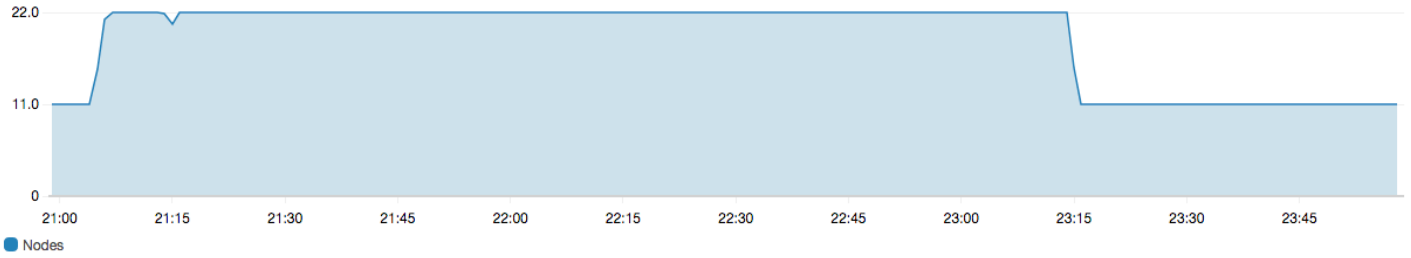
- `Applying changes`: Il servizio sta applicando le modifiche di configurazione richieste.
- `Cancelled`: la modifica della configurazione viene annullata. Se ricevi lo stato di convalida non riuscita, puoi fare clic su Annulla nella console o chiamare l'operazione `CancelDomainConfigChange` API. Se si esegue questa operazione, tutte le modifiche applicate vengono ripristinate.
- `Completed`: le modifiche alla configurazione richieste sono state completate con successo.
- `Validation Failed`: la convalida delle modifiche richieste non è riuscita. Non viene applicata alcuna modifica alla configurazione.

> **Note**
>
> Gli errori di convalida potrebbero essere il risultato di indici rossi presenti nel dominio, dell'indisponibilità di un tipo di istanza scelto o di uno spazio su disco insufficiente. Per un elenco degli errori di convalida, consulta. the section called “Risoluzione degli errori di convalida” Durante un evento di errore di convalida, è possibile annullare, riprovare o modificare le modifiche alla configurazione.

Riepilogo dell'API: è possibile utilizzare le operazioni `DescribeDomainDescribeDomainChangeProgress`, e `DescribeDomainConfig` API per ottenere stati dettagliati di aggiornamento della configurazione. Inoltre, è possibile utilizzare `CancelDomainConfigChange` per annullare gli aggiornamenti in caso di errori di convalida. Per ulteriori informazioni, consulta la documentazione dell'API OpenSearch di servizio

Una volta completate le modifiche alla configurazione, lo stato del dominio torna a`Active`.

Puoi esaminare lo stato del cluster e i CloudWatch parametri di Amazon e vedere che il numero di nodi nel cluster aumenta temporaneamente, spesso raddoppiando, durante l'aggiornamento del dominio. L'illustrazione seguente mostra il numero di nodi che raddoppia da 11 a 22 durante una modifica di configurazione e torna a 11 al termine dell'aggiornamento.



Questo aumento temporaneo può gravare sui nodi master dedicati del cluster, che improvvisamente devono gestire molti più nodi. Può anche aumentare le latenze di ricerca e indicizzazione poiché OpenSearch Service copia i dati dal vecchio cluster a quello nuovo. È importante mantenere una capacità sufficiente sul cluster per gestire il carico di lavoro aggiuntivo associato alle implementazioni blu/verde.

> **Important**
>
> Le modifiche di configurazione e manutenzione del servizio non comportano costi aggiuntivi. Ti viene fatturato solo il numero di nodi richiesti per il cluster. Per le specifiche, consulta the section called “Costi per le modifiche di configurazione”.

Per evitare il sovraccarico dei nodi master dedicati, puoi monitorare l'utilizzo con i parametri di Amazon CloudWatch . Per scoprire i valori massimi consigliati, consulta the section called “Allarmi consigliati CloudWatch ”.

Fasi di una modifica della configurazione

Dopo aver avviato una modifica alla configurazione, OpenSearch Service esegue una serie di passaggi per aggiornare il dominio. È possibile visualizzare lo stato di avanzamento della modifica della configurazione in Stato di modifica della configurazione nella console. I passaggi esatti eseguiti da un aggiornamento dipendono dal tipo di modifica che stai apportando.
È inoltre possibile monitorare una modifica della configurazione utilizzando l'operazione DescribeDomainChangeProgressAPI.

Di seguito sono riportate le fasi possibili che un aggiornamento può passare durante una modifica della configurazione:

Nome fase	Descrizione
Validation	Convalida che il dominio è idoneo per un aggiornamento e fa emergere problemi di

Nome fase	Descrizione
	convalida se necessario.
Creazione di un nuovo ambiente	Completamento dei prerequisiti necessari e creazione delle risorse necessarie per avviare l'implementazione blu/verde.
Provisioning di nuovi nodi	Creazione di una nuova istanza database nell'ambiente di anteprima.
Routing del traffico su nuovi nodi	Reindirizzamento del traffico ai nodi dati appena creati.
Routing del traffico sui vecchi nodi	Disabilitazione del traffico sui vecchi nodi dati.

Nome fase	Descrizione
Preparazione dei nodi per la rimozione	Preparazione alla rimozione dei nodi. Questo passaggio si verifica solo quando si esegue il downscaling del dominio (ad esempio, da 8 nodi a 6 nodi).
Copia di partizioni su nuovi nodi	Spostamento di partizioni dai vecchi nodi ai nuovi nodi.
Terminazione dei nodi	Terminare ed eliminare i vecchi nodi dopo la rimozione delle partizioni.
Eliminazione delle risorse meno recenti	Eliminazione di risorse associate al vecchio ambiente (ad esempio il load balancer).

Nome fase	Descrizione
Aggiornamento dinamico	Viene visualizzato quando l'aggiornamento non richiede un'implementazione blu/verde e può essere applicato dinamicamente.
Applicazione di modifiche dedicate relative al master	Visualizzato quando si modifica il tipo o il conteggio dell'istanza principale dedicata.
Applicazione delle modifiche relative al volume	Viene visualizzato quando le dimensioni, il tipo, gli IOPS e la velocità effettiva del volume vengono modificati.

Impatto sulle prestazioni delle implementazioni blu/green

Durante la distribuzione blu/green, il tuo cluster di OpenSearch servizi Amazon è disponibile per le richieste di ricerca e indicizzazione in entrata. Tuttavia, potresti riscontrare i seguenti problemi di prestazioni:

- Aumento temporaneo dell'utilizzo sui nodi leader poiché i cluster hanno più nodi da gestire.
- Maggiore latenza di ricerca e indicizzazione poiché il OpenSearch servizio copia i dati dai vecchi nodi ai nuovi nodi.
- Aumento dei rifiuti per le richieste in entrata all'aumentare del carico del cluster durante le implementazioni blu/verdi.
- Per evitare problemi di latenza e il rifiuto delle richieste, è consigliabile eseguire distribuzioni blu/verdi quando il cluster è integro e il traffico di rete è scarso.

Costi per le modifiche di configurazione

Se si modifica la configurazione di un dominio, OpenSearch Service crea un nuovo cluster come descritto in. the section called “Modifiche di configurazione” Durante la migrazione dal vecchio al nuovo, saranno calcolate le spese seguenti:

- Se si modifica il tipo di istanza, saranno addebitate le spese sia per i cluster che per la prima ora. Dopo la prima ora, l'addebito è relativo solo al nuovo cluster. I volumi EBS non vengono addebitati due volte perché fanno parte del cluster, quindi la loro fatturazione segue la fatturazione delle istanze.

  Esempio: la configurazione viene modificata passando da tre istanze `m3.xlarge` a quattro istanze `m4.large`. Per la prima ora, ti viene addebitato il costo per entrambi i cluster (3 * `m3.xlarge` + 4 * `m4.large`). Dopo la prima ora, ti viene addebitato solo il nuovo cluster (4 * `m4.large`).
- Se non modifichi il tipo di istanza, ti saranno addebitate solo le spese per il cluster più grande per la prima ora. Dopo la prima ora, l'addebito è relativo solo al nuovo cluster.

  Esempio: la configurazione viene modificata passando da sei istanze `m3.xlarge` a tre istanze `m3.xlarge`. Per la prima ora, ti viene addebitato il cluster più grande (6 * `m3.xlarge`). Dopo la prima ora, ti viene addebitato solo il nuovo cluster (3 * `m3.xlarge`).

Risoluzione degli errori di convalida

Quando avvii una modifica alla configurazione o esegui un OpenSearch aggiornamento della versione di Elasticsearch, OpenSearch Service esegue innanzitutto una serie di controlli di convalida per garantire che il tuo dominio sia idoneo per un aggiornamento. Se uno di questi controlli non riesce, si riceve una notifica nella console contenente i problemi specifici che è necessario correggere prima di aggiornare il dominio. La tabella seguente elenca i possibili problemi di dominio che il OpenSearch Servizio potrebbe riscontrare e i passaggi per risolverli.

Problema	Codice di errore	Fasi per la risoluzione dei problemi
Gruppo di sicurezza non trovato	`SecurityGroupNotFound`	Il gruppo di sicurezza associato al dominio di OpenSearch servizio non esiste. Per risolvere questo problema, crea un gruppo di sicurezza con il nome specificato.
Sottorete non trovata	`SubnetNotFound`	La sottorete associata al dominio OpenSearch di servizio non esiste. Per risolvere questo problema, crea una sottorete nel VPC.
Ruolo collegato al servizio non configurato	`SLRNotConfigured`	Il ruolo collegato al servizio per OpenSearch Service non è configura to. Il ruolo collegato al servizio è predefinito da OpenSearch Service e include tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per conto dell'utente. AWS Se il ruolo non esiste, potresti aver bisogno della Creazione manuale.
Indirizzi IP insufficienti	`InsufficientFreeIPsForSubnets`	Una o più sottoreti VPC non dispongono di indirizzi IP sufficienti per aggiornare il dominio. Per calcolare quanti indirizzi IP sono necessari, vedere the section called “Prenotazione di indirizzi IP in una sottorete VPC”.
Il pool di utenti di Cognito non esiste	`CognitoUserPoolNotFound`	OpenSearch Il servizio non riesce a trovare il pool di utenti di Amazon Cognito. Conferma di averne creato uno e di avere l'ID corretto. Per trovare l'ID, è possibile usare la console Amazon Cognito o il seguente comando della AWS CLI : `aws cognito-idp list-user-pools --max-results 60 --region us-east-1`

Problema	Codice di errore	Fasi per la risoluzione dei problemi
Il pool di identità di Cognito non esiste	`CognitoIdentityPoolNotFound`	OpenSearch Il servizio non riesce a trovare il pool di identità di Cognito. Conferma di averne creato uno e di avere l'ID corretto. Per trovare l'ID, è possibile usare la console Amazon Cognito o il seguente comando della AWS CLI : `aws cognito-identity list-identity-pools --max-results 60 --region us-east-1`
Dominio di Cognito non trovato per il pool di utenti	`CognitoDomainNotFound`	Il pool di utenti non ha un nome di dominio. Puoi configurarne uno utilizzando la console Amazon Cognito o il seguente AWS CLI comando: `aws cognito-idp create-user-pool-domain --domain my-domain --user-pool-id id`
Ruolo Cognito non configurato	`CognitoRoleNotConfigured`	Il ruolo IAM che concede l'autorizzazione al OpenSearch Servizio per configurare i pool di utenti e identità di Amazon Cognito e utilizzarli per l'autenticazione, non è configurato. Configura il ruolo con un set di autorizzazioni e una relazione di trust appropriati. Puoi utilizzare la console, che crea il CognitoAccessForAmazonOpenSearchruolo predefinito per te, oppure puoi configurare manualmente un ruolo utilizzando l'SDK AWS CLI o l' AWS SDK.
Impossibile descrivere il pool di utenti	`UserPoolNotDescribable`	Il ruolo Amazon Cognito specificato non dispone dell'autorizzazione per descrivere il pool di utenti associato al tuo dominio. Assicurarsi che la policy delle autorizzazioni dei ruoli consenta l'operazione `cognito-identity:DescribeUserPool` . Consulta the section called “Informazioni sul ruolo CognitoAccessForAmazonOpenSearch” per la policy completa delle autorizzazioni.

Problema	Codice di errore	Fasi per la risoluzione dei problemi
Impossibile descrivere il pool di identità	`IdentityPoolNotDescribable`	Il ruolo Amazon Cognito specificato non dispone dell'autorizzazione per descrivere il pool di identità associato al tuo dominio. Assicurarsi che la policy delle autorizzazioni dei ruoli consenta l'operazione `cognito-identity:DescribeIdentityPool`. Consulta the section called “Informazioni sul ruolo CognitoAccessForAmazonOpenSearch” per la policy completa delle autorizzazioni.
Impossibile descrivere il pool utente e il pool di identità	`CognitoPoolsNotDescribable`	Il ruolo Amazon Cognito specificato non dispone dell'autorizzazione per descrivere i pool di identità e utente associati al tuo dominio. Assicurarsi che la policy delle autorizzazioni dei ruoli consenta le operazioni `cognito-identity:DescribeIdentityPool` e `cognito-identity:DescribeUserPool`. Consulta the section called “Informazioni sul ruolo CognitoAccessForAmazonOpenSearch” per la policy completa delle autorizzazioni.
Chiave KMS non è abilitata	`KMSKeyNotEnabled`	La chiave AWS Key Management Service (AWS KMS) utilizzata per crittografare il dominio è disabilitata. Riattiva la chiave immediatamente.
Certificato personalizzato non in stato EMESSO	`InvalidCertificate`	Se il tuo dominio utilizza un endpoint personalizzato, lo proteggi generando un certificato SSL in AWS Certificate Manager (ACM) o importandone uno tuo. Lo stato del certificato deve essere Emesso. Se viene visualizzato questo errore, verificare lo stato del certificato nella console ACM. Se lo stato è Scaduto, Non riuscito, Inattivo o In attesa di convalida, consulta ka documentazione per la risoluzione dei problemi di ACM per risolvere il problema.
Capacità insufficiente per avviare il tipo di istanza scelto	`InsufficientInstanceCapacity`	La capacità del tipo di istanza richiesta non è disponibile. Ad esempio, potresti aver richiesto cinque `i3.16xlarge.search` nodi, ma OpenSearch Service non dispone di abbastanza `i3.16xlarge.search` host disponibili, quindi la richiesta non può essere soddisfatta. Controlla i tipi di istanza supportati in OpenSearch Service e scegli un tipo di istanza diverso.

Problema	Codice di errore	Fasi per la risoluzione dei problemi
Indici rossi nel cluster	`RedCluster`	Uno o più indici del cluster hanno uno stato rosso, che porta a uno stato generale del cluster rosso. Per risolvere il problema e risolvere questo problema, vedere the section called “Cluster in stato rosso”.
Interruttore automatico di memoria, troppe richieste	`TooManyRequests`	Ci sono troppe richieste di ricerca e scrittura sul tuo dominio, quindi OpenSearch Service non può aggiornarne la configurazione. Puoi ridurre il numero di richieste, scalare le istanze verticalmente fino a 64 GiB di RAM o scalare orizzontalmente aggiungendo le istanze.
La nuova configurazione non può contenere dati (spazio su disco insufficiente)	`InsufficientStorageCapacity`	Le dimensioni di archiviazione configurate non possono contenere tutti i dati del tuo dominio. Per risolvere questo problema, scegli un volume più grande, elimina gli indici inutilizzati o aumenta il numero di nodi nel cluster per liberare immediatamente spazio su disco.

Problema	Codice di errore	Fasi per la risoluzione dei problemi

Partizioni fissate a nodi specifici	`ShardMovementBlocked`	Uno o più indici nel tuo dominio sono collegati a nodi specifici e non possono essere riassegnati. Ciò è probabilmente accaduto perché è stato configurato il filtro di allocazione delle partizioni, che consente di specificare quali nodi sono autorizzati a ospitare le partizioni di un determinato indice.
		
		Per risolvere questo problema, rimuovere i filtri di allocazione delle partizioni da tutti gli indici interessati:
		
		`PUT my-index/_settings`
		`{`
		`  "settings": {`
		`  "index.routing.allocation.require._name": null`
		`  }`
		`}`

La nuova configurazione non può contenere tutte le partizioni (numero di partizioni)	`TooManyShards`	Il numero di shard sul tuo dominio è troppo alto, il che impedisce a OpenSearch Service di spostarli nella nuova configurazione. Per risolvere questo problema, ridimensiona il tuo dominio orizzontalmente aggiungendo nodi dello stesso tipo di configurazione dei nodi del cluster corrente. Nota che la dimensione massima dei volumi EBS dipende dal tipo di istanza del nodo. Per evitare questo problema in futuro, vedere the section called “Scelta del numero di partizioni” e definire una strategia di partizione appropriata per il tuo caso d'uso.

Problema	Codice di errore	Fasi per la risoluzione dei problemi
La sottorete associata al tuo dominio non supporta gli indirizzi IPv4	`ResultCodeIPv4BlockNotExists`	Per risolvere questo problema, crea una sottorete o aggiorna la sottorete esistente nel tuo VPC in base al tipo di indirizzo IP configurato del dominio. Se il tuo dominio utilizza un tipo di indirizzo solo IPv4, utilizza una sottorete solo IPv4. Se il tuo dominio utilizza la modalità Dual-stack, utilizza una sottorete dual-stack.
La sottorete associata al tuo dominio non supporta gli indirizzi IPv6	`ResultCodeIPv6BlockNotExists`	Per risolvere questo problema, crea una sottorete o aggiorna la sottorete esistente nel tuo VPC in base al tipo di indirizzo IP configurato del dominio. Se il tuo dominio utilizza un tipo di indirizzo solo IPv4, utilizza una sottorete solo IPv4. Se il tuo dominio utilizza la modalità Dual-stack, utilizza una sottorete dual-stack.

Aggiornamenti del software di servizio in Amazon OpenSearch Service

> **Note**
>
> Per le spiegazioni delle modifiche e delle aggiunte apportate in ogni aggiornamento principale del software del servizio (senza patch), consulta le note di rilascio.

Amazon OpenSearch Service rilascia regolarmente aggiornamenti del software di servizio che aggiungono funzionalità o migliorano in altro modo i tuoi domini. Il pannello Notifications (Notifiche) nella console è il modo più semplice per verificare se è disponibile un aggiornamento o controllare lo stato di un aggiornamento. Ogni notifica include dettagli sull'aggiornamento del software del servizio.

Tutti gli aggiornamenti del software di servizio utilizzano implementazioni blu/verdi per ridurre al minimo i tempi di inattività.

Gli aggiornamenti del software di servizio differiscono dagli aggiornamenti di versione. OpenSearch Per informazioni sull'aggiornamento a una versione successiva di OpenSearch, vedere. the section called “Aggiornamento dei domini”

Argomenti

Aggiornamenti facoltativi e aggiornamenti obbligatori

OpenSearch Il servizio prevede due ampie categorie di aggiornamenti software di servizio:

Aggiornamenti opzionali

Gli aggiornamenti opzionali del software di servizio generalmente includono miglioramenti e supporto per nuove caratteristiche o funzionalità. Gli aggiornamenti opzionali non vengono applicati ai tuoi domini e non è prevista una scadenza fissa per installarli. La disponibilità dell'aggiornamento viene comunicata tramite e-mail e una notifica della console. Puoi scegliere di applicare l'aggiornamento immediatamente o riprogrammarlo per una data e un'ora più appropriate. Puoi anche programmarlo durante la finestra non di punta del dominio. La maggior parte degli aggiornamenti software è facoltativa.

Indipendentemente dal fatto che pianifichi o meno un aggiornamento, se apporti una modifica al dominio che causa una distribuzione blu/verde, OpenSearch Service aggiorna automaticamente il software di servizio per te.

Puoi configurare il tuo dominio per applicare automaticamente gli aggiornamenti opzionali durante le ore non di punta. Quando questa opzione è attivata, il OpenSearch Servizio attende almeno 13 giorni dalla data in cui è disponibile un aggiornamento opzionale e quindi pianifica l'aggiornamento dopo

72 ore (tre giorni). Riceverai una notifica sulla console quando l'aggiornamento è pianificato e puoi scegliere di riprogrammarlo per una data successiva.

Per attivare gli aggiornamenti software automatici, seleziona Abilita l'aggiornamento automatico del software quando crei o aggiorni il tuo dominio. Per configurare la stessa impostazione utilizzando AWS CLI, imposta su `--software-update-options true` quando crei o aggiorni il dominio.

Aggiornamenti richiesti

Gli aggiornamenti software di servizio richiesti generalmente includono correzioni di sicurezza critiche o altri aggiornamenti obbligatori per garantire l'integrità e la funzionalità continue del dominio. Esempi di aggiornamenti richiesti sono Log4j Common Vulnerabilities and Exposures (CVE) e l'applicazione di Instance Metadata Service Version 2 (IMDSv2). Il numero di aggiornamenti obbligatori in un anno è in genere inferiore a tre.

OpenSearch Il servizio pianifica automaticamente questi aggiornamenti e avvisa l'utente 72 ore (tre giorni) prima dell'aggiornamento pianificato tramite e-mail e una notifica della console. Puoi scegliere di applicare l'aggiornamento immediatamente o riprogrammarlo per una data e un'ora più appropriate entro il periodo di tempo consentito. Puoi anche programmarlo durante la prossima finestra non di punta del dominio. Se non intraprendi alcuna azione su un aggiornamento richiesto e non apporti modifiche al dominio che causino una distribuzione blu/verde, OpenSearch Service può avviare l'aggiornamento in qualsiasi momento oltre la scadenza specificata (in genere 14 giorni dalla disponibilità), entro la finestra non di punta del dominio.

Indipendentemente da quando è pianificato l'aggiornamento, se apporti una modifica al dominio che causa una distribuzione blu/verde, il OpenSearch Servizio aggiorna automaticamente il dominio per te.

Aggiornamenti delle patch

Versioni software di servizio che terminano con "-P" e un numero, come R20211203-*P4*, sono versioni di patch. È probabile che le patch includano miglioramenti delle prestazioni, correzioni di bug minori e correzioni di sicurezza o miglioramenti della posizione. Le versioni delle patch non includono nuove funzionalità o modifiche sostanziali e in genere non hanno un impatto diretto o evidente sugli utenti. La notifica del software di servizio indica se il rilascio di una patch è facoltativo o obbligatorio.

Considerazioni

Per stabilire se aggiornare il dominio, considerare quando segue:

- L'aggiornamento manuale del dominio consente di sfruttare più rapidamente le nuove funzionalità. Quando scegli Aggiorna, il OpenSearch servizio mette la richiesta in coda e avvia l'aggiornamento quando è disponibile.
- Quando si avvia un aggiornamento del software di servizio, OpenSearch Service invia una notifica quando l'aggiornamento inizia e quando viene completato.
- Gli aggiornamenti software utilizzano implementazioni blu/verde per ridurre al minimo i tempi di inattività. Gli aggiornamenti possono sovraccaricare temporaneamente i nodi principali dedicati di un cluster, quindi assicurarsi di mantenere una capacità sufficiente per gestire il sovraccarico associato.
- Gli aggiornamenti vengono generalmente completati in pochi minuti, ma possono richiedere anche diverse ore o addirittura giorni se il sistema subisce un carico pesante. Valuta la possibilità di aggiornare il dominio durante la finestra configurata non di punta per evitare lunghi periodi di aggiornamento.

Avvio di un aggiornamento del software di servizio

Puoi richiedere un aggiornamento del software di OpenSearch servizio tramite la console di servizio AWS CLI, o uno degli SDK.

Console

Per richiedere un aggiornamento del software di servizio

1. Apri la console OpenSearch di Amazon Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Seleziona il nome di dominio per aprirne la configurazione.
3. Scegli Azioni, Aggiorna e seleziona una delle seguenti opzioni:

    - Applica l'aggiornamento ora: pianifica immediatamente l'azione in modo che venga eseguita nell'ora corrente, se c'è capacità disponibile. Se la capacità non è disponibile, forniamo altre fasce orarie disponibili tra cui scegliere.
    - Pianificalo in una finestra non di punta: disponibile solo se la finestra non di punta è abilitata per il dominio. Pianifica l'aggiornamento in modo che avvenga durante la finestra non di punta configurata del dominio. Non è garantito che l'aggiornamento avvenga nella finestra immediata successiva. A seconda della capacità, potrebbe verificarsi nei giorni successivi. Per ulteriori informazioni, consulta the section called “Finestre non di punta”.

- Pianifica per data e ora specifiche: pianifica l'aggiornamento in modo che avvenga in una data e un'ora specifiche. Se l'ora specificata non è disponibile per motivi di capacità, puoi selezionare una fascia oraria diversa.

Se pianifichi l'aggiornamento per una data successiva (all'interno o all'esterno della finestra non di punta del dominio), puoi riprogrammarlo in qualsiasi momento. Per istruzioni, consulta the section called “Riprogrammazione delle azioni”.

4. Scegli Conferma.

AWS CLI

Invia una start-service-software-update AWS CLI richiesta per avviare un aggiornamento del software di servizio. Questo esempio aggiunge immediatamente l'aggiornamento alla coda:

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "NOW"
```

Risposta:

```
{
    "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

Dopo aver richiesto un aggiornamento, hai a disposizione una finestra di tempo ristretta per annullarlo. La durata di questo `PENDING_UPDATE` stato può variare notevolmente e dipende dall'utente Regione AWS e dal numero di aggiornamenti simultanei eseguiti

dal OpenSearch Servizio. Per annullare un aggiornamento, usa la console o il `cancel-service-software-update` AWS CLI comando.

Se la richiesta ha esito negativo con un`BaseException`, significa che l'ora specificata non è disponibile per motivi di capacità e devi specificare un'ora diversa. OpenSearch Il servizio fornisce suggerimenti alternativi sugli slot disponibili nella risposta.

AWS SDK

Questo script Python di esempio utilizza i metodi describe_domain e start_service_software_update di per verificare se un dominio è idoneo AWS SDK for Python (Boto3) per un aggiornamento del software di servizio e, in tal caso, avvia l'aggiornamento. È necessario fornire un valore per `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)
```

Pianificazione degli aggiornamenti software durante le finestre non di punta

Ogni dominio OpenSearch di servizio creato dopo il 16 febbraio 2023 ha una finestra giornaliera di 10 ore tra le 22:00 e le 8:00 ora locale, periodo considerato non di punta. OpenSearch Il servizio utilizza questa finestra per pianificare gli aggiornamenti del software di servizio per il dominio. Gli aggiornamenti non di punta aiutano a ridurre al minimo l'affaticamento sui nodi master dedicati di un cluster durante i periodi di traffico più intenso. OpenSearch Il servizio non può avviare aggiornamenti al di fuori di questa finestra di 10 ore senza il tuo consenso.

- Per gli aggiornamenti opzionali, il OpenSearch Servizio notifica all'utente la disponibilità dell'aggiornamento e richiede all'utente di pianificare l'aggiornamento durante una finestra non di punta imminente.
- Per gli aggiornamenti richiesti, il OpenSearch Servizio pianifica automaticamente l'aggiornamento durante una prossima finestra non di punta e invia una notifica all'utente con tre giorni di anticipo. Puoi riprogrammare l'aggiornamento (all'interno o all'esterno della finestra non di punta), ma solo entro il periodo di tempo richiesto per il completamento dell'aggiornamento.

Per ogni dominio, puoi scegliere di sostituire l'ora di inizio predefinita delle 22:00 con un'ora personalizzata. Per istruzioni, consulta the section called “Configurazione di una finestra personalizzata non di punta”.

Console

Per pianificare un aggiornamento durante una prossima finestra non di punta

1. Apri la console OpenSearch di Amazon Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Seleziona il nome di dominio per aprirne la configurazione.
3. Scegli Operazioni, Aggiorna.
4. Seleziona Pianificalo in una finestra non di punta.
5. Scegli Conferma.

Puoi visualizzare l'azione pianificata nella scheda della finestra Non di punta e riprogrammarla in qualsiasi momento. Per informazioni, consulta the section called “Visualizzazione delle azioni pianificate”.

CLI

Per pianificare un aggiornamento durante una prossima finestra non di punta utilizzando il AWS CLI, invia una StartServiceSoftwareUpdaterichiesta e specifica il parametro: `OFF_PEAK_WINDOW` `--schedule-at`

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "OFF_PEAK_WINDOW"
```

Aggiornamenti del software del servizio di monitoraggio

OpenSearch Il servizio invia una notifica quando un aggiornamento del software di servizio è disponibile, richiesto, avviato, completato o non riuscito. È possibile visualizzare queste notifiche nel pannello Notifiche della console di OpenSearch servizio. La gravità della notifica è `Informational` se l'aggiornamento è facoltativo e `High` se invece è obbligatorio.

OpenSearch Il servizio invia anche eventi software di servizio ad Amazon EventBridge. Puoi utilizzarlo EventBridge per configurare regole che inviano un'e-mail o eseguono un'azione specifica quando viene ricevuto un evento. Per un esempio di procedura guidata, consulta the section called “Tutorial: Invio di avvisi SNS per gli aggiornamenti disponibili”.

Per vedere il formato di ogni evento software di servizio inviato ad Amazon EventBridge, consultathe section called “Eventi di aggiornamento del software di servizio”.

Quando i domini non sono idonei per un aggiornamento

Il dominio potrebbe non essere idoneo all'aggiornamento del software del servizio se si trova in uno degli stati riportati di seguito:

Stato	Descrizione
Dominio in elaborazione	Il dominio è nel mezzo di una modifica di configurazione. Controlla l'idoneità dell'aggiornamento al termine dell'operazione.
Cluster in stato rosso	Uno o più indici nel cluster sono in stato rosso. Per la risoluzione dei problemi, consulta the section called “Cluster in stato rosso”.
Elevata percentuale di errori	Il OpenSearch cluster restituisce un numero elevato di 5 xx errori quando tenta di elaborare le richieste. Questo problema è in genere il risultato di un numero eccessivo di richieste di lettura o scrittura simultanee. Valuta la possibilità di ridurre il traffico verso il cluster o di eseguire il dimensionamento del dominio.
Split brain	Il cervello diviso significa che il OpenSearch cluster ha più di un nodo master ed è suddiviso in due cluster che non si ricongiungeranno mai da soli. Puoi evitare lo split brain utilizzando il numero consigliato di nodi master dedicati. Per risolvere un problema di split brain, contatta AWS Support.

Stato	Descrizione
Problema di integrazione di Amazon Cognito	Il tuo dominio utilizza l'autenticazione per OpenSearch le dashboard e OpenSearch Service non riesce a trovare una o più risorse Amazon Cognito. Questo problema in genere si verifica se manca il bacino d'utenza di Amazon Cognito. Per correggere il problema, ricrea la risorsa mancante e configura il dominio del OpenSearch servizio per utilizzarla.
Altro problema del servizio	Problemi relativi al OpenSearch Servizio stesso potrebbero far sì che il dominio venga visualizzato come non idoneo per un aggiornamento. Se nessuna delle condizioni precedenti si applica al dominio e il problema persiste per più di un giorno, contatta AWS Support.

Definizione delle finestre non di punta per Amazon Service OpenSearch

Quando crei un dominio Amazon OpenSearch Service, definisci una finestra giornaliera di 10 ore considerata non di punta. OpenSearch Il servizio utilizza questa finestra per pianificare gli aggiornamenti del software di servizio e le ottimizzazioni Auto-Tune che richiedono un'implementazione blu/verde durante periodi di traffico relativamente inferiori, quando possibile. Il colore blu/verde si riferisce al processo di creazione di un nuovo ambiente per gli aggiornamenti del dominio e di indirizzamento degli utenti verso il nuovo ambiente dopo il completamento di tali aggiornamenti.

Sebbene le implementazioni blu/verde non comportino interruzioni, per ridurre al minimo qualsiasi potenziale impatto sulle prestazioni durante il consumo di risorse per una distribuzione blu/verde, si consiglia di pianificare queste distribuzioni durante la finestra non di picco configurata per il dominio. Gli aggiornamenti, come le sostituzioni dei nodi o quelli che devono essere implementati immediatamente nel dominio, non utilizzano la finestra non di punta.

È possibile modificare l'ora di inizio della finestra non di punta, ma non la lunghezza della finestra.

> **Note**
>
> Le finestre non di punta sono state introdotte il 16 febbraio 2023. Per impostazione predefinita, per tutti i domini creati prima di questa data la finestra non di punta è disattivata. È necessario abilitare e configurare manualmente la finestra non di punta per questi

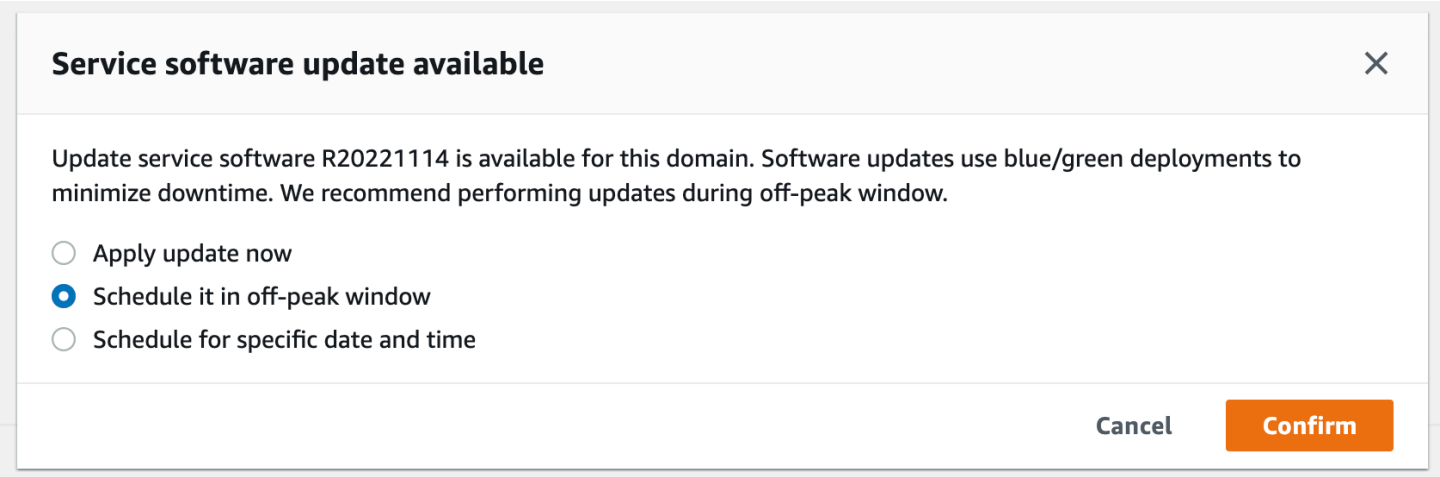
domini. Per tutti i domini creati dopo questa data, la finestra non di punta sarà abilitata per impostazione predefinita. Non puoi disabilitare la finestra non di punta per un dominio dopo che è stata abilitata.

Argomenti

Aggiornamenti software di servizio non di punta

OpenSearch Il servizio prevede due ampie categorie di aggiornamenti del software di servizio: facoltativi e obbligatori. Entrambi i tipi richiedono implementazioni blu/verdi. Gli aggiornamenti opzionali non vengono applicati ai tuoi domini, mentre gli aggiornamenti richiesti vengono installati automaticamente se non intraprendi alcuna azione prima della scadenza specificata (in genere due settimane dalla disponibilità). Per ulteriori informazioni, consulta the section called “Aggiornamenti facoltativi e aggiornamenti obbligatori”.

Quando avvii un aggiornamento facoltativo, puoi scegliere di applicarlo immediatamente, pianificarlo per una finestra successiva non di punta o specificare una data e un'ora personalizzate per applicarlo.



Per gli aggiornamenti richiesti, il OpenSearch Servizio pianifica automaticamente una data e un'ora durante le ore non di punta per eseguire l'aggiornamento. Riceverai una notifica tre giorni prima dell'aggiornamento pianificato e puoi scegliere di riprogrammarlo per una data e un'ora successive entro il periodo di distribuzione richiesto. Per istruzioni, consulta the section called "Riprogrammazione delle azioni".

Ottimizzazioni Auto-Tune in caso di picco

In precedenza, Auto-Tune utilizzava finestre di manutenzione per pianificare le modifiche che richiedevano un'implementazione blu/verde. I domini che avevano già Auto-Tune e le finestre di manutenzione abilitate prima dell'introduzione delle finestre non di punta continueranno a utilizzare le finestre di manutenzione per questi aggiornamenti, a meno che non si effettui la migrazione per utilizzare la finestra non di punta.

Ti consigliamo di migrare i domini per utilizzare la finestra non di punta, poiché viene utilizzata per pianificare altre attività sul dominio, come gli aggiornamenti del software di servizio. Per istruzioni, consulta the section called "Migrazione dalle finestre di manutenzione di Auto-Tune". Non puoi tornare a utilizzare le finestre di manutenzione dopo aver migrato il dominio alla finestra non di punta.

Tutti i domini creati dopo il 16 febbraio 2023 utilizzeranno la finestra non di punta, anziché le finestre di manutenzione precedenti, per pianificare le distribuzioni blu/verdi. Non puoi disabilitare la finestra non di punta per un dominio. Per un elenco delle ottimizzazioni Auto-Tune che richiedono implementazioni blu/verdi, consulta. the section called "Tipi di modifiche"

Attivazione della finestra non di punta

Per tutti i domini creati prima del 16 febbraio 2023 (quando sono state introdotte le finestre non di punta) la funzionalità è disattivata per impostazione predefinita. È necessario abilitarla manualmente per questi domini. Non puoi disabilitare la finestra non di punta dopo averla abilitata.

Console

Per abilitare la finestra non di punta per un dominio

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Seleziona il nome del dominio per aprirne la configurazione.
3. Vai alla scheda della finestra Off-peak e scegli Modifica.
4. Specificate un'ora di inizio personalizzata in UTC (Coordinated Universal Time). Ad esempio, per configurare l'ora di inizio delle 23:30 nella regione Stati Uniti occidentali (Oregon), specificare 07:30.
5. Seleziona Salvataggio delle modifiche.

CLI

Per modificare la finestra non di punta utilizzando il, invia una richiesta: AWS CLI UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'Enabled=true,
 OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Se non specifichi un'ora di inizio della finestra personalizzata, il valore predefinito è 00:00 UTC.

Configurazione di una finestra personalizzata non di punta

Specifichi una finestra non di punta personalizzata per il tuo dominio in UTC (Coordinated Universal Time). Ad esempio, se desideri che la finestra non di punta inizi alle 23:00 per un dominio nella regione Stati Uniti orientali (Virginia settentrionale), devi specificare le 04:00 UTC.

Console

Per modificare la finestra non di punta per un dominio

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Seleziona il nome del dominio per aprirne la configurazione.
3. Vai alla scheda della finestra Off-peak. Puoi visualizzare la finestra configurata non di punta e un elenco delle azioni pianificate imminenti per il dominio.
4. Scegli Modifica e specifica una nuova ora di inizio in UTC. Ad esempio, per configurare l'ora di inizio delle 21:00 nella regione Stati Uniti orientali (Virginia settentrionale), specifica 02:00 UCT.
5. Seleziona Salvataggio delle modifiche.

CLI

Per configurare una finestra non di punta personalizzata utilizzandoAWS CLI, invia una UpdateDomainConfigrichiesta e specifica l'ora e il minuto nel formato orario di 24 ore.

Ad esempio, la seguente richiesta modifica l'ora di inizio della finestra alle 2:00 UTC:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Se non specifichi l'ora di inizio della finestra, l'impostazione predefinita è alle 22:00 ora locale in cui è stato creato il Regione AWS dominio.

Visualizzazione delle azioni pianificate

Puoi visualizzare tutte le azioni attualmente pianificate, in corso o in sospeso per ciascuno dei tuoi domini. Le azioni possono avere una gravità di `HIGH`, `MEDIUM`, e. `LOW`

Le azioni possono avere i seguenti stati:

- `Pending update`— L'azione è in coda per essere elaborata.
- `In progress`— L'azione è attualmente in corso.
- `Failed`— L'azione non è stata completata.

- `Completed`— L'azione è stata completata con successo.
- `Not eligible`— Solo per gli aggiornamenti del software di servizio. L'aggiornamento non può procedere perché lo stato del cluster non è integro.
- `Eligible`— Solo per gli aggiornamenti del software di servizio. Il dominio è idoneo per un aggiornamento.

Console

La console OpenSearch di servizio mostra tutte le azioni pianificate all'interno della configurazione del dominio, insieme alla gravità e allo stato corrente di ciascuna azione.

Per visualizzare le azioni pianificate per un dominio

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Seleziona il nome del dominio per aprirne la configurazione.
3. Vai alla scheda della finestra Off-peak.
4. In Azioni pianificate, visualizza tutte le azioni attualmente pianificate, in corso o in sospeso per il dominio.

CLI

Per visualizzare le azioni pianificate utilizzandoAWS CLI, invia una ListScheduledActionsrichiesta:

```
aws opensearch list-scheduled-actions \
  --domain-name my-domain
```

Risposta:

```
{
    "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",
        }
    ]
}
```

Riprogrammazione delle azioni

OpenSearch Il servizio notifica all'utente gli aggiornamenti programmati del software di servizio e le ottimizzazioni di Auto-Tune. Puoi scegliere di applicare la modifica immediatamente o riprogrammarla per una data e un'ora successive.

> **Note**
>
> OpenSearch Il servizio può pianificare l'azione entro un'ora dall'orario selezionato. Ad esempio, se scegli di applicare un aggiornamento alle 17:00, puoi applicarlo tra le 17:00 e le 18:00.

Console

Per riprogrammare un'azione

1. Apri la console Amazon OpenSearch Service all'[indirizzo https://console.aws.amazon.com/aos/home](https://console.aws.amazon.com/aos/home).
2. Seleziona il nome del dominio per aprirne la configurazione.
3. Vai alla scheda della finestra Off-peak.

4. In Azioni pianificate, seleziona l'azione e scegli Riprogramma.
5. Selezionare una delle seguenti opzioni:

   - Applica l'aggiornamento ora: pianifica immediatamente l'azione in modo che venga eseguita nell'ora corrente, se c'è capacità disponibile. Se la capacità non è disponibile, forniamo altre fasce orarie disponibili tra cui scegliere.
   - Pianificalo in una finestra non di punta: contrassegna l'azione da riprendere durante una prossima finestra non di punta. Non c'è alcuna garanzia che la modifica venga implementata nella finestra immediatamente successiva. A seconda della capacità, potrebbe verificarsi nei giorni successivi.
   - Riprogramma questo aggiornamento: consente di specificare una data e un'ora personalizzate per applicare la modifica. Se l'ora specificata non è disponibile per motivi di capacità, è possibile selezionare una fascia oraria diversa.
   - Annulla aggiornamento pianificato: annulla l'aggiornamento. Questa opzione è disponibile solo per gli aggiornamenti opzionali del software di servizio. Non è disponibile per le azioni Auto-Tune o gli aggiornamenti software obbligatori.
6. Seleziona Salvataggio delle modifiche.

CLI

Per riprogrammare un'azione utilizzando ilAWS CLI, invia una richiesta. UpdateScheduledAction Per recuperare l'ID dell'azione, invia una richiesta. `ListScheduledActions`

La richiesta seguente riprogramma un aggiornamento del software di servizio per una data e un'ora specifiche:

```
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
```

Risposta:

```
{
   "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"
   }
}
```

Se la richiesta ha esito negativo con un`SlotNotAvailableException`, significa che l'ora specificata non è disponibile per motivi di capacità ed è necessario specificare un'ora diversa. OpenSearch Il servizio fornisce suggerimenti alternativi sugli slot disponibili nella risposta.

Migrazione dalle finestre di manutenzione di Auto-Tune

Se un dominio è stato creato prima del 16 febbraio 2023, potrebbe utilizzare le finestre di manutenzione per pianificare le ottimizzazioni di Auto-Tune che richiedono una distribuzione blu/verde. Puoi migrare i domini Auto-Tune esistenti per utilizzare invece la finestra non di punta.

> **Note**
>
> Non puoi tornare a utilizzare le finestre di manutenzione dopo aver migrato il dominio per utilizzare le finestre non di punta.

Console

Per migrare un dominio per utilizzare la finestra non di punta

1. Nella console di Amazon OpenSearch Service, seleziona il nome del dominio per aprirne la configurazione.
2. Vai alla scheda Auto-Tune e scegli Modifica.
3. Seleziona Migra alla finestra non di punta.
4. Per Ora di inizio (UTC), fornisci un'ora di inizio giornaliera per la finestra non di punta dell'Universal Coordinated Time (UTC).
5. Seleziona Salvataggio delle modifiche.

CLI

Per migrare da una finestra di manutenzione di Auto-Tune a una finestra non di punta utilizzando il, invia una richiesta: AWS CLI UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=[]
```

La finestra di manutenzione di Auto-Tune deve essere attivata per poter migrare un dominio dalla finestra di manutenzione di Auto-Tune a quella non di punta. È possibile abilitare la finestra non di punta in una richiesta separata o nella stessa richiesta. Per istruzioni, consultare the section called "Attivazione della finestra non di punta".

Notifiche in Amazon OpenSearch Service

Le notifiche in Amazon OpenSearch Service contengono informazioni importanti sulle prestazioni e sullo stato dei tuoi domini. OpenSearch Il servizio ti avvisa sugli aggiornamenti del software di servizio, sui miglioramenti di Auto-Tune, sugli eventi relativi allo stato di salute del cluster e sugli errori del dominio. Le notifiche sono disponibili per tutte le versioni di Elasticsearch OSS. OpenSearch

È possibile visualizzare le notifiche nel pannello Notifiche della console di OpenSearch servizio. Tutte le notifiche per OpenSearch il Servizio vengono visualizzate anche in Amazon EventBridge. Per un elenco completo delle notifiche e degli eventi di esempio, consulta la sezione the section called "Monitoraggio degli eventi".

Argomenti

- Nozioni di base sulle notifiche
- Gravità delle notifiche
- Evento di esempio EventBridge

Nozioni di base sulle notifiche

Le notifiche vengono attivate automaticamente quando si crea un dominio. Vai al pannello Notifiche della console di OpenSearch servizio per monitorare e confermare le notifiche. Ogni notifica include

informazioni quali l'ora in cui è stata pubblicata, il dominio a cui si riferisce, il livello di gravità e di stato e una breve spiegazione. È possibile visualizzare le notifiche cronologiche fino a 90 giorni prima nella console.

Dopo aver effettuato l'accesso al pannello Notifiche o confermando una notifica, è possibile che venga visualizzato un messaggio di errore che indica che non si dispone di autorizzazioni per l'esecuzione di `es:ListNotifications` o `es:UpdateNotificationStatus`. Per risolvere questo problema, assegna all'utente o al ruolo le seguenti autorizzazioni in IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "es:UpdateNotificationStatus",
      "es:ListNotifications"
    ],
    "Resource": "arn:aws:es:*:123456789012:domain/*"
  }]
}
```

La console IAM genera un errore ("IAM non riconosce una o più azioni") che può essere ignorato in modo sicuro. È inoltre possibile limitare l'operazione `es:UpdateNotificationStatus` per determinati domini. Per ulteriori informazioni, vedi the section called “Riferimenti agli elementi della policy”.

Gravità delle notifiche

Le notifiche nel OpenSearch Servizio possono essere informative, che si riferiscono a qualsiasi azione già intrapresa o alle operazioni del dominio, oppure utilizzabili, che richiedono l'adozione di azioni specifiche, come l'applicazione di una patch di sicurezza obbligatoria. A ogni notifica è associata una gravità, che può essere `Informational`, `Low`, `Medium`, `High` o `Critical`. Nella seguente tabella sono riepilogate le varie gravità:

Gravità	Descrizione	Esempi
`Informational`	Informazioni relative al funzionamento del tuo dominio.	• Aggiornamento del software di servizio disponibile • Regolazione automatica avviata

Gravità	Descrizione	Esempi
`Low`	Un'azione consigliata, ma senza alcun impatto negativo sulla disponibilità o sulle prestazioni del dominio se non viene eseguita.	• Regolazione automatica annullata • Avviso di conteggio di partizioni elevate
`Medium`	Un impatto è possibile se l'azione consigliata non viene intrapresa, ma viene fornita con una finestra temporale estesa per l'azione da intraprendere.	• Aggiornamento del software di servizio non riuscito • Superamento del limite del numero di partizioni
`High`	È necessaria un'azione urgente per evitare effetti avversi.	• Aggiornamento del software di servizio richiesto • Chiave KMS inaccessibile
`Critical`	È necessaria un'azione immediata per evitare impatti negativi o per riprendersi da questi impatti.	Nessuna attualmente disponibile

Evento di esempio EventBridge

L'esempio seguente mostra un evento OpenSearch di notifica del servizio inviato ad Amazon EventBridge. La notifica corrispondente ha una gravità pari a `Informational` perché l'aggiornamento è facoltativo:

```
{
  "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."
  }
}
```

Configurazione di un dominio Multi-AZ in Amazon Service OpenSearch

Per prevenire la perdita di dati e ridurre al minimo i tempi di inattività del cluster Amazon OpenSearch Service in caso di interruzione del servizio, puoi distribuire i nodi su due o tre zone di disponibilità nella stessa regione, una configurazione nota come Multi-AZ. Le zone di disponibilità sono località isolate all'interno di ciascuna regione. AWS

Per i domini che eseguono carichi di lavoro di produzione, consigliamo l'opzione di implementazione Multi-AZ with Standby, che crea la seguente configurazione:

- Il dominio è distribuito su tre zone.
- Tipi di istanze di ultima generazione per nodi master e nodi dati dedicati.
- Tre nodi master dedicati e tre (o più di tre) nodi dati.
- Almeno due repliche per ogni indice del dominio o un multiplo di tre copie di dati (inclusi sia i nodi primari che le repliche).

Il resto di questa sezione fornisce spiegazioni e contesto su queste configurazioni.

Multi-AZ con Standby

Multi-AZ with Standby è un'opzione di implementazione per i domini Amazon OpenSearch Service che offre una disponibilità del 99,99%, prestazioni costanti per i carichi di lavoro di produzione e configurazione e gestione semplificate dei domini. Quando utilizzi Multi-AZ con Standby, i domini sono resilienti ai guasti dell'infrastruttura, senza alcun impatto sulle prestazioni o sulla disponibilità. Questa opzione di implementazione raggiunge questo standard imponendo una serie di best practice,

come il numero di nodi di dati specificato, il conteggio dei nodi principali, il tipo di istanze, il numero di repliche, le impostazioni di aggiornamento del software e l'attivazione di Auto-Tune.

Quando si utilizza Multi-AZ con Standby, OpenSearch Service crea un dominio in tre zone di disponibilità, ognuna delle quali contiene una copia completa dei dati e i dati vengono distribuiti equamente in ciascuna delle zone. Il tuo dominio riserva i nodi in una di queste zone come standby, il che significa che non soddisfano le richieste di ricerca. Quando OpenSearch Service rileva un guasto nell'infrastruttura sottostante, attiva automaticamente i nodi di standby in meno di un minuto. Il dominio continua a servire le richieste di indicizzazione e ricerca e qualsiasi impatto è limitato al tempo necessario per eseguire il failover. Non vi è alcuna ridistribuzione di dati o risorse, il che si traduce in prestazioni del cluster inalterate e nessun rischio di riduzione della disponibilità. Multi-AZ con Standby è disponibile senza costi aggiuntivi.

Sono disponibili due opzioni per creare un dominio con standby su. AWS Management Console Innanzitutto, puoi creare un dominio con il metodo di creazione Easy create e OpenSearch Service utilizzerà automaticamente una configurazione predeterminata, che include quanto segue:

- Tre zone di disponibilità, una delle quali funge da standby
- Tre nodi master e nodi dati dedicati
- Auto-Tune abilitato sul dominio
- Storage GP3 per i nodi di dati

Puoi anche scegliere il metodo di creazione standard e selezionare Dominio con standby come opzione di distribuzione. Ciò consente di personalizzare il dominio pur mantenendo obbligatorie le funzionalità chiave di standby, come tre zone e tre nodi master. Ti consigliamo di scegliere un numero di nodi dati che sia un multiplo di tre (il numero di zone di disponibilità).

Dopo aver creato il dominio, puoi accedere alle pagine dei dettagli del dominio e, nella scheda Configurazione del cluster, confermare che 3-AZ con standby sia visualizzato sotto Zone di disponibilità.

In caso di problemi durante la migrazione di un dominio esistente a Multi-AZ con Standby, consulta Errore durante la migrazione a Multi-AZ con Standby nella guida alla risoluzione dei problemi.

Limitazioni

Quando configuri un dominio con Multi-AZ with Standby, considera le seguenti limitazioni:

- Il numero totale di shard su un nodo non può superare 1000, il numero totale di shard su un cluster non può superare 75000 e la dimensione di un singolo shard non può superare i 65 GB.
- Multi-AZ con Standby funziona solo con i tipi di `m5` istanza,`c5`, `r5r6g`, `c6g` e. `m6g` `r6gd` `i3` Per ulteriori informazioni sulle istanze supportate, consulta Tipi di istanze supportati.
- È possibile utilizzare solo Provisioned IOPS SSD, General Purpose SSD (GP3) o storage supportato da istanze con standby.
- Se si abilita UltraWarmsu un dominio Multi-AZ con Standby, il numero di nodi caldi deve essere un multiplo del numero di zone di disponibilità utilizzate.

Multi-AZ senza Standby

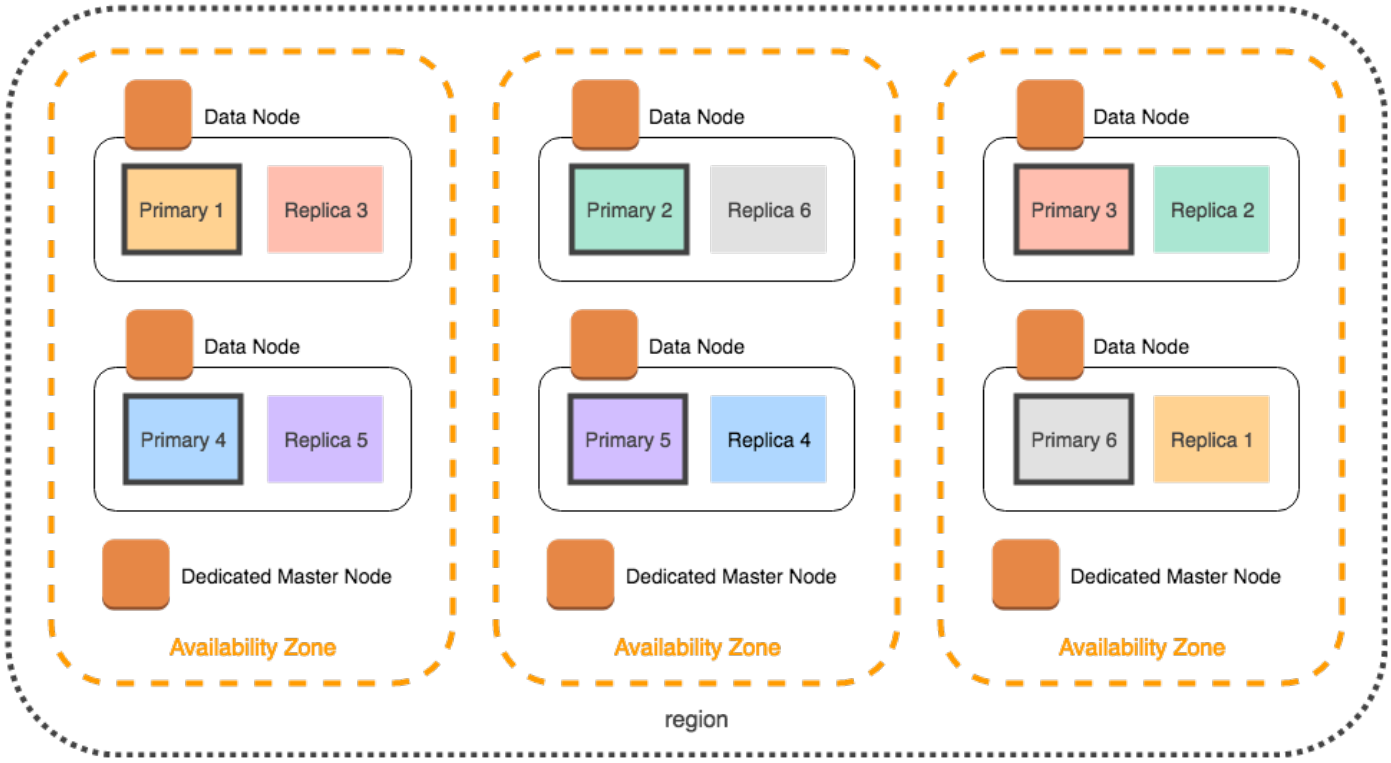
OpenSearch Il servizio supporta ancora Multi-AZ senza Standby, che offre una disponibilità del 99,9%. I nodi sono distribuiti tra le zone di disponibilità e la disponibilità dipende dal numero di zone di disponibilità e dalle copie dei dati. Mentre con lo standby è necessario configurare il dominio secondo le migliori pratiche, senza standby è possibile scegliere il numero di zone di disponibilità, nodi e repliche. Non consigliamo questa opzione a meno che non disponiate di flussi di lavoro esistenti che verrebbero interrotti dalla creazione di domini con modalità di standby.

Se scegli questa opzione, ti consigliamo comunque di selezionare tre zone di disponibilità per rimanere resiliente ai guasti di nodi, dischi e Single-AZ. Quando si verifica un errore, il cluster ridistribuisce i dati tra le risorse rimanenti per mantenere la disponibilità e la ridondanza. Questo spostamento dei dati aumenta l'utilizzo delle risorse nel cluster e può avere un impatto sulle prestazioni. Se il cluster non è dimensionato correttamente, può subire una riduzione della disponibilità, il che vanifica in gran parte lo scopo di Multi-AZ.

L'unico modo per configurare un dominio senza standby su AWS Management Console è scegliere il metodo di creazione Standard create e selezionare Domain without standby come opzione di distribuzione.

Distribuzione di partizioni

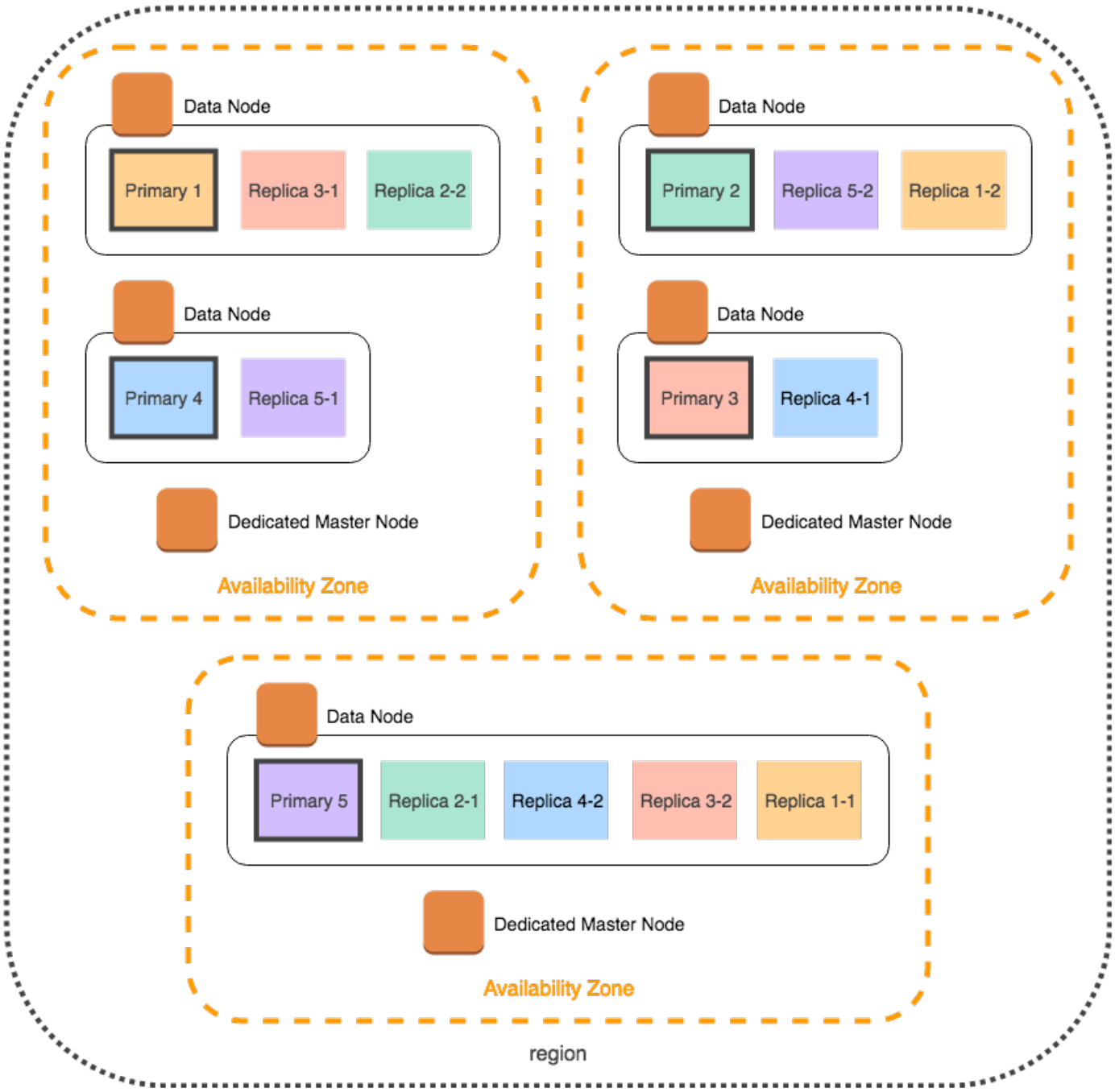
Se abiliti Multi-AZ without Standby, devi creare almeno una replica per ogni indice del cluster. Senza repliche, OpenSearch Service non può distribuire copie dei dati in altre zone di disponibilità. Fortunatamente, la configurazione predefinita per qualsiasi indice prevede un conteggio di repliche pari a 1. Come illustrato nel diagramma seguente, OpenSearch Service fa del suo meglio per distribuire gli shard primari e i corrispondenti shard di replica in zone diverse.



Oltre a distribuire gli shard per zona di disponibilità, OpenSearch Service li distribuisce per nodo. Tuttavia, alcune configurazioni di dominio possono portare a conteggi di partizioni squilibrati. Considerare il dominio seguente:

- 5 nodi di dati
- 5 partizioni primarie
- 2 repliche
- 3 zone di disponibilità

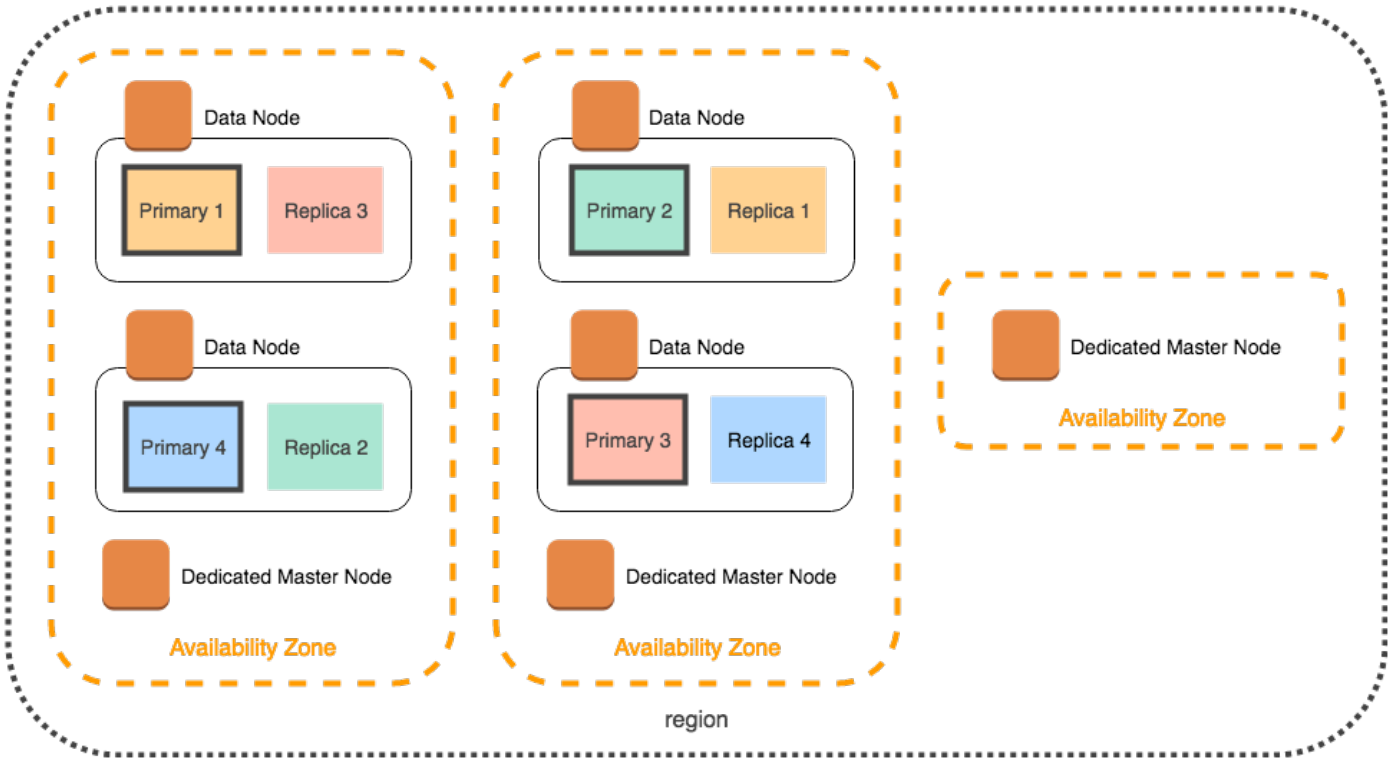
In questa situazione, OpenSearch Service deve sovraccaricare un nodo per distribuire gli shard primari e di replica tra le zone, come illustrato nel diagramma seguente.



Per evitare questo tipo di situazioni, che possono mettere a dura prova i singoli nodi e compromettere le prestazioni, si consiglia di scegliere Multi-AZ con Standby oppure di scegliere un numero di istanze multiplo di tre se si prevede di avere due o più repliche per indice.

Distribuzione dei nodi principali dedicati

Anche se si selezionano due zone di disponibilità durante la configurazione del dominio, OpenSearch Service distribuisce automaticamente i nodi master dedicati su tre zone di disponibilità. Questa distribuzione consente di evitare tempi di inattività dei cluster se in una zona si verifica un'interruzione del servizio. Se si utilizzano i tre nodi master dedicati consigliati e una zona di disponibilità è inutilizzabile, il cluster ha ancora un quorum (2) di nodi master dedicati e può eleggere un nuovo nodo master. Il seguente diagramma mostra questa configurazione.



Se si sceglie un tipo di istanza della generazione precedente che non è disponibile nelle tre zone di disponibilità, si verifica lo scenario seguente:

- Se hai scelto tre zone di disponibilità per il dominio, OpenSearch Service genera un errore. Scegliere un tipo di istanza diverso e riprovare.
- Se hai scelto due zone di disponibilità per il dominio, OpenSearch Service distribuisce i nodi master dedicati su due zone.

Interruzioni delle zone di disponibilità

I tempi di inattività per le zone di disponibilità sono rari, ma si verificano. La tabella seguente elenca diverse configurazioni con Multi-AZ e comportamenti durante i tempi di inattività. L'ultima riga della tabella si riferisce a Multi-AZ con Standby, mentre tutte le altre righe hanno configurazioni che si applicano solo a Multi-AZ senza Standby.

Numero di zone di disponibilità in una regione	Numero delle zone di disponibilità scelte	Numero di nodi principali dedicati	Comportamento nel caso in cui una zona di disponibilità subisca un'interruzione
2 o più	2	0	Tempo di inattività. Il cluster perde metà dei propri nodi di dati e deve sostituirne almeno uno nella zona di disponibilità rimanente prima di poter eleggere un nodo master.
2	2	3	50/50 possibilità di tempi di inattività. OpenSearch Il servizio distribuisce due nodi master dedicati in una zona di disponibilità e uno nell'altra: • Se la zona di disponibilità con un nodo master dedicato subisce un'interruzione, i due nodi master dedicati nella zona di disponibilità rimanente possono scegliere un nodo master. • Se la zona di disponibilità con due nodi master dedicati subisce un'interruzione, il cluster non è disponibile fino a quando la zona di disponibilità rimanente viene ripristin ata.
3 o più	2	3	Nessun tempo di inattività. OpenSearch Il servizio distribuisce automaticamente i nodi master dedicati su tre zone di disponibilità, in

Numero di zone di disponibilità in una regione	Numero delle zone di disponibilità scelte	Numero di nodi principali dedicati	Comportamento nel caso in cui una zona di disponibilità subisca un'interruzione
			modo che i restanti due nodi master dedicati possano eleggere un master.
3 o più	3	0	Nessun tempo di inattività. Circa due terzi dei nodi di dati sono ancora disponibili per eleggere un nodo master.
3 o più	3	3	Nessun tempo di inattività. I restanti due nodi master dedicati possono scegliere un nodo master.

In tutte le configurazioni, indipendentemente dalla causa, i guasti dei nodi possono causare un periodo di carico maggiore sui nodi di dati rimanenti del cluster, mentre OpenSearch Service configura automaticamente i nuovi nodi per sostituire quelli ora mancanti.

Ad esempio, nel caso in cui si verificasse l'interruzione di una zona di disponibilità in una configurazione a tre zone, due terzi dei nodi dei dati devono elaborare tutte le richieste al cluster. Mentre elaborano queste richieste, i nodi rimanenti cercano di replicare le partizioni sui nuovi nodi non appena sono disponibili online, con un ulteriore impatto sulle prestazioni. Se la disponibilità è fondamentale per il carico di lavoro, considerare l'aggiunta di risorse al cluster per alleviare questa preoccupazione.

> **Note**
>
> OpenSearch Il servizio gestisce i domini Multi-AZ in modo trasparente, quindi non è possibile simulare manualmente le interruzioni delle zone di disponibilità.

Avvio dei domini Amazon OpenSearch Service all'interno di un VPC

Puoi lanciare AWS risorse, come i domini Amazon OpenSearch Service, in un cloud privato virtuale (VPC). Un VPC è una rete virtuale dedicata a te. Account AWSIl VPC è isolato a livello logico dalle altre reti virtuali del cloud AWS . L'inserimento di un dominio di OpenSearch servizio all'interno di un VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno del VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS

> **Note**
>
> Se inserisci il tuo dominio OpenSearch di servizio all'interno di un VPC, il computer deve essere in grado di connettersi al VPC. Questa connessione spesso avviene tramite una VPN, un gateway di transito, una rete gestita o un server proxy. Non è possibile accedere direttamente ai domini dall'esterno del VPC.

Argomenti

VPC e domini pubblici

Di seguito sono riportati alcuni dei modi in cui i domini in VPC differiscono dai domini pubblici. Ogni differenza è descritta più avanti in modo più dettagliato.

- Grazie a loro isolamento logico, i domini che si trovano all'interno di un VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici.
- Mentre i domini pubblici sono accessibili da qualsiasi dispositivo connesso a Internet, i domini in VPC richiedono una qualche forma di VPN o proxy.
- Rispetto ai domini pubblici, i domini VPC visualizzano meno informazioni nella console . In particolare, la scheda Integrità del cluster non include le informazioni sulle partizioni e la scheda Indici non è presente.

- Gli endpoint del dominio assumono forme diverse (`https://search-domain-name` e `https://vpc-domain-name`).
- Poiché i gruppi di sicurezza applicano già le policy di accesso basate su IP, non è possibile applicare policy d'accesso basate su IP ai domini che si trovano all'interno di un VPC.

Limitazioni

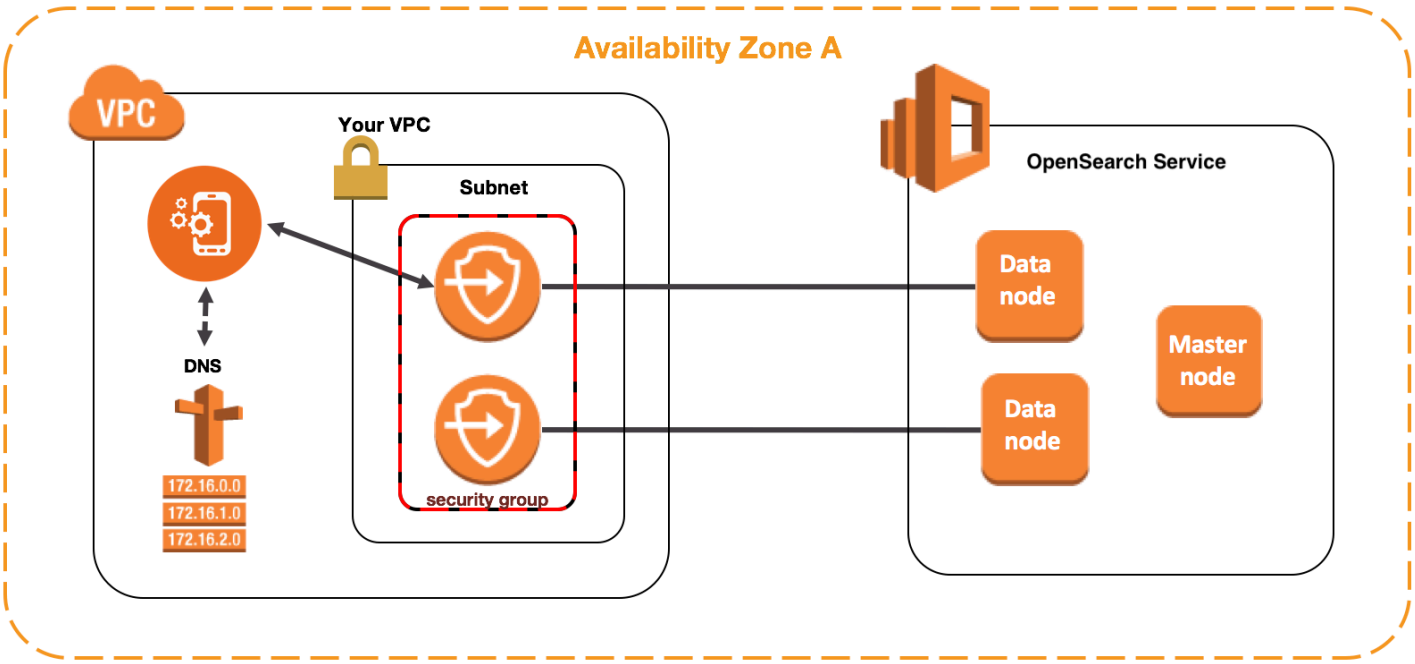
La gestione di un dominio di OpenSearch servizio all'interno di un VPC presenta le seguenti limitazioni:

- Se avvii un nuovo dominio all'interno di un VPC, successivamente non puoi passare all'uso di un endpoint pubblico. Lo stesso vale al contrario: se crei un dominio con un endpoint pubblico, successivamente non puoi inserirlo in un VPC. Devi invece creare un nuovo dominio ed eseguire la migrazione dei dati.
- È possibile avviare il dominio all'interno di un VPC oppure usare un endpoint pubblico, ma non è possibile eseguire entrambe le operazioni. Al momento della creazione di un dominio, devi scegliere una delle due opzioni.
- Non è possibile avviare il dominio in un VPC che usa la tenancy dedicata. Devi usare un VPC con tenancy impostata su Default (Predefinita).
- Dopo aver inserito un dominio all'interno di un VPC, non è possibile spostarlo in un VPC diverso, ma è possibile modificare le sottoreti e le impostazioni del gruppo di sicurezza.
- Per accedere all'installazione predefinita di OpenSearch dashboard per un dominio che risiede all'interno di un VPC, gli utenti devono avere accesso al VPC. Questo processo varia in base alla configurazione di rete, ma generalmente prevede la connessione a una VPN o una rete gestita o l'uso di un server proxy o di un gateway di transito. Per ulteriori informazioni, consultare the section called “Informazioni sulle policy d'accesso nei domini VPC”, la Guida per l'utente di Amazon VPC e the section called “Controllo dell'accesso ai dashboard OpenSearch ”.

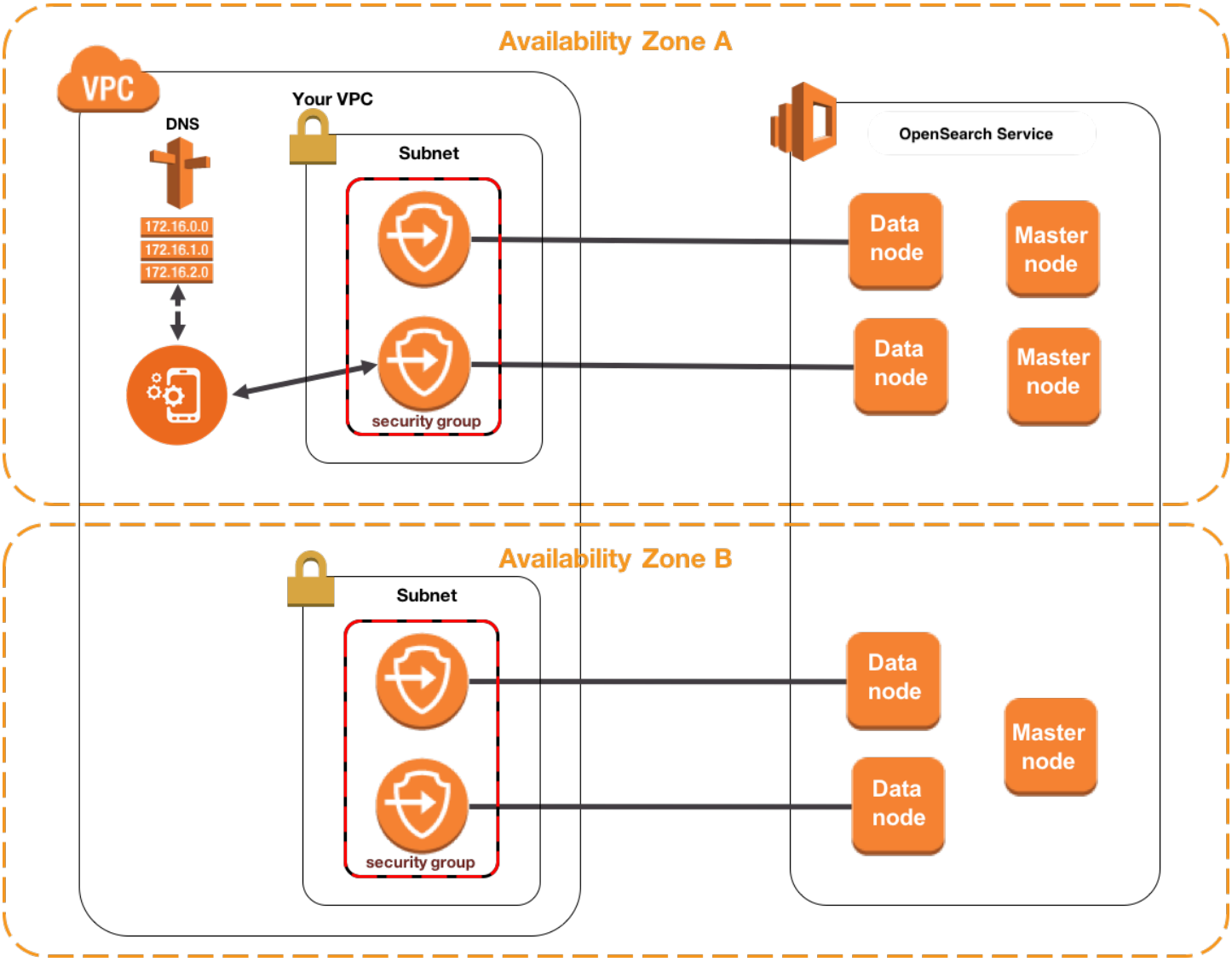
Architettura

Per supportare i VPC, OpenSearch Service colloca un endpoint in una, due o tre sottoreti del tuo VPC. Se si attivano più zone di disponibilità per il dominio, ogni sottorete deve trovarsi in una zona di disponibilità diversa nella stessa area. Se si utilizza una sola zona di disponibilità, OpenSearch Service colloca un endpoint in una sola sottorete.

La figura seguente mostra l'architettura del VPC per una zona di disponibilità.



La figura seguente mostra l'architettura del VPC per due zone di disponibilità.



OpenSearch Il servizio inserisce anche un'interfaccia di rete elastica (ENI) nel VPC per ciascuno dei nodi di dati. OpenSearch Il servizio assegna a ciascun ENI un indirizzo IP privato dall'intervallo di indirizzi IPv4 della sottorete. Il servizio, inoltre, assegna un nome host DNS pubblico (che è l'endpoint del dominio) per gli indirizzi IP. È necessario usare un servizio DNS pubblico per risolvere l'endpoint (che è un nome host DNS) negli indirizzi IP appropriati per i nodi di dati:

- Se il tuo VPC utilizza il server DNS fornito da Amazon impostando l'`enableDnsSupport`opzione su `true` (il valore predefinito), la risoluzione per l'endpoint del OpenSearch servizio avrà esito positivo.
- Se il tuo VPC utilizza un server DNS privato e il server può raggiungere i server DNS pubblici autorevoli per risolvere i nomi host DNS, anche la risoluzione per l'endpoint del servizio avrà successo. OpenSearch

Poiché gli indirizzi IP possono cambiare, è necessario risolvere l'endpoint del dominio periodicamente, in modo che sia sempre possibile accedere ai nodi di dati corretti. È consigliabile impostare l'intervallo di risoluzione DNS su un minuto. Se usi un client, assicurati anche che la cache DNS nel client venga cancellata.

Migrazione dall'accesso pubblico all'accesso VPC

Quando crei un dominio, specifichi se deve avere un endpoint pubblico o trovarsi all'interno di un VPC. Una volta completata la creazione, non è possibile passare da un'opzione all'altra. Devi invece creare un nuovo dominio e reindicizzare manualmente i dati o eseguirne la migrazione. Gli snapshot offrono una semplice modalità di migrazione dei dati. Per informazioni su come acquisire e ripristinare gli snapshot, consulta the section called “Creazione di snapshot di indici”.

Informazioni sulle policy d'accesso nei domini VPC

L'inserimento OpenSearch del dominio di servizio all'interno di un VPC fornisce un livello di sicurezza intrinseco e robusto. Quando crei un dominio con accesso pubblico, l'endpoint ha il formato seguente:

```
https://search-domain-name-identifier.region.es.amazonaws.com
```

Come suggerisce l'etichetta "pubblico", questo endpoint è accessibile da qualsiasi dispositivo connesso a Internet, anche se è possibile (e necessario) controllare l'accesso. Se accedi all'endpoint in un Web browser, potrebbe venire visualizzato un messaggio `Not Authorized`, ma la richiesta raggiunge il dominio.

Quando crei un dominio con accesso VPC, l'endpoint sembra simile a un endpoint pubblico:

```
https://vpc-domain-name-identifier.region.es.amazonaws.com
```

Se provi ad accedere all'endpoint in un Web browser, tuttavia, si potrebbe verificare il timeout della richiesta. Per eseguire richieste `GET` anche di base, il computer deve essere in grado di connettersi al VPC. Questa connessione spesso avviene tramite una VPN, un gateway di transito, una rete gestita o un server proxy. Per maggiori dettagli sulle varie forme che può avere, consultare Esempi per VPC nella Guida per l'utente di Amazon VPC. Per un esempio relativo allo sviluppo consulta the section called “Test dei domini VPC”.

Oltre a questo requisito di connettività, i VPC permettono di gestire l'accesso al dominio tramite gruppi di sicurezza. Per molti casi d'uso, questa combinazione di caratteristiche di sicurezza è sufficiente e può essere appropriato applicare una policy d'accesso aperta al dominio.

Operare con una politica di accesso aperto non significa che chiunque su Internet possa accedere al dominio del OpenSearch Servizio. Significa piuttosto che se una richiesta raggiunge il dominio del OpenSearch Servizio e i gruppi di sicurezza associati lo consentono, il dominio accetta la richiesta. L'unica eccezione è se si utilizza il controllo granulare degli accessi o una policy di accesso che specifichi i ruoli IAM. In questi casi, affinché il dominio accetti la richiesta, i gruppi di sicurezza devono permettere l'operazione e la richiesta deve essere firmata con credenziali valide.

> **Note**
>
> Poiché i gruppi di sicurezza applicano già criteri di accesso basati su IP, non è possibile applicare criteri di accesso basati su IP ai domini di OpenSearch servizio che risiedono all'interno di un VPC. Se usi l'accesso pubblico, le policy basate su IP sono ancora disponibili.

Prima di iniziare: Prerequisiti per l'accesso al VPC

Prima di poter abilitare una connessione tra un VPC e il nuovo dominio di OpenSearch servizio, devi fare quanto segue:

- Crea un VPC

  Per creare il tuo VPC, puoi utilizzare la console Amazon VPC, la AWS CLI o uno degli SDK. AWS Per ulteriori informazioni, consultare Utilizzo dei VPC nella Guida per l'utente di Amazon VPC. Se hai già un VPC, questa fase può essere ignorata.

- Prenota indirizzi IP

  OpenSearch Il servizio consente la connessione di un VPC a un dominio inserendo le interfacce di rete in una sottorete del VPC. Ogni interfaccia di rete è associata a un indirizzo IP. È necessario riservare un numero sufficiente di indirizzi IP nella sottorete per le interfacce di rete. Per ulteriori informazioni, consultare Prenotazione di indirizzi IP in una sottorete VPC.

Test dei domini VPC

La sicurezza avanzata di un VPC può trasformare la connessione al dominio e l'esecuzione di test di base in una vera sfida. Se disponi già di un dominio OpenSearch Service VPC e preferisci non creare un server VPN, prova la seguente procedura:

1. Per la policy di accesso del dominio, scegli Utilizza solo il controllo granulare degli accessi. È sempre possibile aggiornare questa impostazione dopo aver completato il test.
2. Crea un'istanza Amazon Linux Amazon EC2 nello stesso VPC, sottorete e gruppo di sicurezza del tuo dominio di servizio. OpenSearch

   Poiché questa istanza è a scopo di test e deve fare poco lavoro, scegliere un tipo di istanza poco costoso come `t2.micro`. Assegnare all'istanza un indirizzo IP pubblico e creare una nuova coppia di chiavi o sceglierne una esistente. Se si crea una nuova chiave, scaricarla nella directory `~/.ssh`.

   Per ulteriori informazioni sulla creazione di istanze, consultare Nozioni di base sulle istanze Linux di Amazon EC2.
3. Aggiungere un gateway internet al VPC.
4. Nella tabella di routing per il VPC, aggiungere un nuovo routing. Per Destination (Destinazione), specificare un blocco CIDR che contiene l'indirizzo IP pubblico del computer. In Target (Destinazione), specificare il gateway Internet appena creato.

   Ad esempio, è possibile specificare solo `123.123.123.123/32` per un computer o `123.123.123.0/24` per una serie di computer.
5. Per il gruppo di sicurezza, specificare due regole in entrata:

Type	Protocollo	Intervallo porte	Origine
SSH (22)	TCP (6)	22	*your-cidr-block*
HTTPS (443)	TCP (6)	443	*your-security-group-id*

   La prima regola consente l'SSH nell'istanza EC2. Il secondo consente all'istanza EC2 di comunicare con il dominio OpenSearch Service tramite HTTPS.
6. Dal terminale, esegui il comando seguente:

```
ssh -i ~/.ssh/your-key.pem ec2-user@your-ec2-instance-public-ip -N -L
 9200:vpc-domain-name.region.es.amazonaws.com:443
```

Questo comando crea un tunnel SSH che inoltra le richieste a https://localhost:9200 al dominio del OpenSearch servizio tramite l'istanza EC2. Specificando la porta 9200 nel comando si simula un' OpenSearch installazione locale, ma usa la porta che preferisci. OpenSearch Il servizio accetta solo connessioni tramite la porta 80 (HTTP) o 443 (HTTPS).

Il comando non fornisce alcun feedback e viene eseguito a tempo indeterminato. Per arrestarlo, premere `Ctrl + C`.

7. Vai a https://localhost:9200/_dashboards/ nel tuo browser web. Potrebbe essere necessario riconoscere un'eccezione di sicurezza.

   In alternativa, è possibile inviare le richieste a https://localhost:9200 utilizzando curl, Postman o il linguaggio di programmazione preferito.

   > **Tip**
   >
   > Se si verificano errori di curl a causa di una mancata corrispondenza del certificato prova il flag `--insecure`.

Prenotazione di indirizzi IP in una sottorete VPC

OpenSearch Il servizio connette un dominio a un VPC inserendo le interfacce di rete in una sottorete del VPC (o più sottoreti del VPC se si abilitano più zone di disponibilità). Ogni interfaccia di rete è associata a un indirizzo IP. Prima di creare il dominio di OpenSearch servizio, è necessario disporre di un numero sufficiente di indirizzi IP disponibili in ciascuna sottorete per ospitare le interfacce di rete.

Ecco la formula di base: il numero di indirizzi IP che OpenSearch Service riserva in ogni sottorete è tre volte il numero di nodi di dati, diviso per il numero di zone di disponibilità.

Examples (Esempi)

- Se un dominio ha nove nodi di dati su tre zone di disponibilità, il numero di indirizzi IP per sottorete è pari a 9*3/3 = 9.
- Se un dominio ha otto nodi di dati su due zone di disponibilità, il numero di indirizzi IP per sottorete è pari a 8*3/2 = 12.
- Se un dominio ha sei nodi di dati in una zona di disponibilità, il numero di indirizzi IP per sottorete è pari a 6*3/1 = 18.

Quando crei il dominio, OpenSearch Service riserva gli indirizzi IP, ne utilizza alcuni per il dominio e riserva il resto per le implementazioni blu/verdi. È possibile visualizzare le interfacce di rete e gli indirizzi IP associati nella sezione Interfacce di rete della console Amazon EC2. La colonna Descrizione mostra a quale dominio di OpenSearch servizio è associata l'interfaccia di rete.

> **Tip**
>
> Si consiglia di creare sottoreti dedicate per gli indirizzi IP riservati del OpenSearch servizio. Usando sottoreti dedicate, puoi evitare sovrapposizioni con altri servizi e applicazioni e puoi riservare ulteriori indirizzi IP se è necessario dimensionare il cluster in futuro. Per ulteriori informazioni, consultare Creazione di una sottorete nel VPC.

Ruolo collegato ai servizi per l'accesso VPC

Un ruolo collegato al servizio è un tipo unico di ruolo IAM che delega le autorizzazioni a un servizio in modo che possa creare e gestire risorse per tuo conto. OpenSearch Il servizio richiede un ruolo collegato al servizio per accedere al tuo VPC, creare l'endpoint del dominio e posizionare le interfacce di rete in una sottorete del tuo VPC.

OpenSearch Il servizio crea automaticamente il ruolo quando utilizzi la console di OpenSearch servizio per creare un dominio all'interno di un VPC. Affinché questa operazione di creazione automatica riesca, devi disporre delle autorizzazioni per l'operazione `iam:CreateServiceLinkedRole`. Per ulteriori informazioni, consultare Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Dopo che OpenSearch Service ha creato il ruolo, puoi visualizzarlo (`AWSServiceRoleForAmazonOpenSearchService`) utilizzando la console IAM.

Per informazioni complete sulle autorizzazioni di questo ruolo e su come eliminarlo, consulta the section called “Uso di ruoli collegati ai servizi”.

Creazione di istantanee dell'indice in Amazon Service OpenSearch

Le istantanee in Amazon OpenSearch Service sono backup degli indici e dello stato di un cluster. Lo stato include le impostazioni del cluster, le informazioni sul nodo, le impostazioni degli indici e l'allocazione delle partizioni.

OpenSearch Le istantanee dei servizi sono disponibili nelle seguenti forme:

- Gli snapshot automatici sono solo per il ripristino del cluster. È possibile utilizzarli per ripristinare il dominio in caso di stato rosso del cluster o di perdita di dati. Per ulteriori informazioni, vedere Ripristino delle istantanee di seguito. OpenSearch Il servizio archivia le istantanee automatizzate in un bucket Amazon S3 preconfigurato senza costi aggiuntivi.
- Gli snapshot manuali servono per il ripristino del cluster o lo spostamento di dati da un cluster a un altro. È necessario avviare gli snapshot manuali. Questi snapshot vengono archiviati nel bucket Amazon S3 e vengono applicati i costi standard di S3. Se disponi di un'istantanea da un OpenSearch cluster autogestito, puoi utilizzarla per migrare a un dominio di servizio. OpenSearch Per ulteriori informazioni, consulta Migrazione ad Amazon OpenSearch Service.

Tutti i domini OpenSearch di servizio scattano istantanee automatiche, ma la frequenza varia nei seguenti modi:

- Per i domini che eseguono OpenSearch Elasticsearch 5.3 e versioni successive, OpenSearch Service acquisisce istantanee automatiche ogni ora e ne conserva fino a 336 per 14 giorni. Gli snapshot orari sono meno dirompenti a causa della loro natura incrementale. Forniscono inoltre un punto di ripristino più recente in caso di problemi di dominio.
- Per i domini che eseguono Elasticsearch 5.1 e versioni precedenti, OpenSearch Service acquisisce istantanee automatiche giornaliere nell'ora specificata, ne conserva fino a 14 e non conserva alcun dato sulle istantanee per più di 30 giorni.

Se il cluster entra nello stato rosso, tutti gli snapshot automatici hanno esito negativo mentre lo stato del cluster persiste. Se il problema non viene risolto entro due settimane, è possibile che i dati del cluster vengano persi definitivamente. Per la risoluzione dei problemi, consulta the section called “Cluster in stato rosso”.

Argomenti

- Utilizzo di Curator per gli snapshot

Prerequisiti

Per creare manualmente gli snapshot, è necessario utilizzare IAM e Amazon S3. Verificare che siano soddisfatti i seguenti prerequisiti prima di provare ad acquisire uno snapshot.

Prerequisito	Descrizione
Bucket S3	Crea un bucket S3 per archiviare istantanee manuali per il tuo dominio di servizio. OpenSearch Per le istruzioni, consulta Crea un bucket nella Guida per l'utente di Amazon Simple Storage Service. Ricordare il nome del bucket per utilizzarlo nei seguenti punti: • L'istruzione `Resource` della policy IAM collegata al ruolo IAM • Il client Python utilizzato per registrare un repository di snapshot (se si utilizza questo metodo) **Important** Non applicare la regola del ciclo di vita S3 Glacier a questo bucket. Gli snapshot manuali non supportano la classe di archiviazione S3 Glacier.

Ruolo IAM	Crea un ruolo IAM per delegare le autorizzazioni al servizio. OpenSearch Per le istruzioni, consultare Creazione di un ruolo IAM (console) nella Guida per l'utente di IAM. Nel resto di questo capitolo ci si riferisce a questo ruolo come `TheSnapshotRole` .
	
	Collegamento di una policy IAM
	
	Collegare la seguente policy a `TheSnapshotRole` per consentire l'accesso al bucket S3:
	
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [{`

Prerequisito	Descrizione

```
      "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 /*"
      ]
    }
  ]
}
```

Per istruzioni su come collegare una policy a un ruolo, consultare Aggiunta di autorizzazioni per l'identità IAM nella Guida per l'utente di IAM.

Modifica della relazione di trust

Modifica la relazione di trust di `TheSnapshotRole` per specificare OpenSearch Service nell'`Principal` istruzione, come mostrato nell'esempio seguente:

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

Prerequisito	Descrizione
	} Per le istruzioni su come modificare la relazione di trust, consultare Modifica di una policy di attendibilità del ruolo nella Guida per l'utente di IAM.

Autorizzazioni	Per registrare il repository di snapshot, devi essere in grado di passare `TheSnapshotRole` a OpenSearch Service. Devi inoltre disporre dell'accesso all'operazione `es:ESHttpPut` . Per concedere entrambe queste autorizzazioni, collega la policy seguente al ruolo IAM le cui credenziali vengono utilizzate per firmare la richiesta:
	
	`{ "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 /*" } ] }`
	
	Se l'utente o il ruolo non dispone `iam:PassRole` delle autorizzazioni necessarie per il passaggio`TheSnapshotRole` , è possibile che si verifichi il seguente errore comune quando si tenta di registrare un repository nel passaggio successivo:
	
	`$ 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 "}`

Registrazione di un repository di snapshot manuali

È necessario registrare un archivio di istantanee con OpenSearch Service prima di poter scattare istantanee dell'indice manualmente. Questa operazione unica richiede la firma della AWS richiesta con credenziali a cui è consentito l'accessoTheSnapshotRole, come descritto in. the section called “Prerequisiti”

Passaggio 1: mappare il ruolo dell'istantanea nelle OpenSearch dashboard (se si utilizza un controllo di accesso granulare)

Il controllo granulare degli accessi introduce un passaggio aggiuntivo durante la registrazione di un repository. Anche se si utilizza l'autenticazione di base HTTP per tutti gli altri scopi, è necessario mappare il ruolo `manage_snapshots` al ruolo IAM che dispone delle autorizzazioni `iam:PassRole` per inviare `TheSnapshotRole`.

1. Vai al plug-in OpenSearch Dashboards per il tuo dominio di servizio. OpenSearch Puoi trovare l'endpoint Dashboards nella dashboard del tuo dominio nella OpenSearch console di servizio.
2. Dal menu principale scegliere Sicurezza, Ruoli e selezionare il ruolo manage_snapshots.
3. Scegliere Utenti mappati, Gestisci mappatura.
4. Aggiungi l'ARN del ruolo che dispone delle autorizzazioni per inviare `TheSnapshotRole`. Inserisci gli ARN dei ruoli in Backend roles (Ruoli di back-end).

   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. Selezionare Mappa e confermare che l'utente o il ruolo venga visualizzato in Utenti mappati.

Fase 2: Registrazione di un repository

La seguente scheda Istantanee mostra come registrare una directory di istantanee. Per le opzioni specifiche relative alla crittografia di un'istantanea manuale e alla registrazione di un'istantanea dopo la migrazione a un nuovo dominio, consulta le schede pertinenti.

Snapshots

Per registrare un archivio di snapshot, invia una richiesta PUT all'endpoint del dominio del servizio. OpenSearch Puoi usare curl, il client Python di esempio, Postman o qualche altro metodo per inviare una richiesta firmata per registrare il repository di snapshot. Tieni presente

che non puoi utilizzare una richiesta PUT nella console OpenSearch Dashboards per registrare il repository.

La richiesta ha il seguente 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**
>
> I nomi dei repository non possono iniziare con "cs-". Inoltre, non dovresti scrivere nello stesso repository da più domini. Solo un dominio deve avere accesso in scrittura al repository.

Se il dominio si trova all'interno di un Virtual Private Cloud (VPC), perché la richiesta registri correttamente il repository di snapshot il computer deve essere connesso al VPC. L'accesso a un VPC varia in base alla configurazione della rete, ma prevede con ogni probabilità la connessione a una VPN o a una rete aziendale. Per verificare di poter raggiungere il dominio del OpenSearch servizio, accedi a `https://your-vpc-domain.region.es.amazonaws.com` In un browser Web e verifica di ricevere la risposta JSON predefinita.

Quando il bucket Amazon S3 si trova in un OpenSearch dominio Regione AWS diverso dal tuo, aggiungi il parametro `"endpoint": "s3.amazonaws.com"` alla richiesta.

Encrypted snapshots

Al momento non puoi utilizzare le chiavi AWS Key Management Service (KMS) per crittografare le istantanee manuali, ma puoi proteggerle utilizzando la crittografia lato server (SSE).

Per attivare SSE con chiavi gestite da S3 per il bucket che usi come repository di istantanee, aggiungile al blocco della richiesta PUT. `"server_side_encryption": true` `"settings"` Per maggiori informazioni, consultare Protezione dei dati mediante la crittografia lato server con

chiavi di crittografia gestite da Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

In alternativa, puoi utilizzare AWS KMS le chiavi per la crittografia lato server sul bucket S3 che usi come repository di istantanee. Se utilizzi questo approccio, assicurati di fornire l'`TheSnapshotRole`autorizzazione alla AWS KMS chiave utilizzata per crittografare il bucket S3. Per ulteriori informazioni, consulta Policy delle chiavi in AWS KMS.

Domain migration

La registrazione di un repository di snapshot è un'operazione che viene eseguita una tantum. Tuttavia, per eseguire la migrazione da un dominio a un altro, è necessario registrare lo stesso repository di snapshot sia sul vecchio dominio che sul nuovo. Il nome del repository è arbitrario.

Considerare le seguenti linee guida quando si esegue la migrazione a un nuovo dominio o si registra lo stesso repository con più domini:

- Quando si registra il repository nel nuovo dominio, aggiungere `"readonly": true` al blocco `"settings"` della richiesta PUT. Questa impostazione impedisce di sovrascrivere accidentalmente i dati dal vecchio dominio. Solo un dominio deve avere accesso in scrittura al repository.
- Se stai migrando i dati verso un dominio in un altro (ad esempio Regione AWS, da un vecchio dominio e bucket situato in us-east-2 a un nuovo dominio in us-west-2), `"region": "region"` sostituiscili con nell'istruzione PUT e riprova la richiesta. `"endpoint": "s3.amazonaws.com"`

Utilizzo del client Python di esempio

Il client Python è più facile da automatizzare rispetto a una semplice richiesta HTTP e ha una migliore riusabilità. Se si sceglie di utilizzare questo metodo per registrare un repository di snapshot, salvare il seguente codice Python di esempio come file Python, ad esempio `register-repo.py`. Il client richiede i pacchetti AWS SDK for Python (Boto3), richieste e requests-aws4auth. Il client contiene esempi commentati per altre operazioni con snapshot.

Aggiornare le seguenti variabili nel codice di esempio:`host`, `region`, `path` e `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)
```

Acquisizione di snapshot manuali

Gli snapshot non sono istantanei. Richiedono tempo per essere completati e non rappresentano viste perfette del cluster. point-in-time Mentre è in corso uno snapshot, è comunque possibile indicizzare i documenti ed effettuare altre richieste al cluster, ma i nuovi documenti (e gli aggiornamenti ai documenti esistenti) non saranno generalmente inclusi nello snapshot. L'istantanea include gli shard primari così come esistevano al momento dell' OpenSearch avvio dell'istantanea. A seconda della dimensione del pool di thread dello snapshot, potrebbero essere incluse diverse partizioni nello snapshot in momenti leggermente diversi. Per le best practice relative alle istantanee, consulta. the section called “Migliora le prestazioni delle istantanee”

Archiviazione e prestazioni degli snapshot

OpenSearch le istantanee sono incrementali, il che significa che memorizzano solo i dati modificati dall'ultima istantanea riuscita. Questa natura incrementale significa che la differenza di utilizzo del disco tra snapshot frequenti e infrequenti spesso è minima. In altre parole, effettuando snapshot orarie per una settimana (per un totale di 168 snapshot) potrebbe non essere necessario molto più spazio su disco rispetto a una snapshot singola alla fine della settimana. Inoltre, se la frequenza con cui si prendono le snapshot è alta, minore è il tempo necessario per il completamento del processo. Ad esempio, gli snapshot giornalieri possono richiedere 20-30 minuti per essere completati, mentre gli snapshot orari potrebbero essere completati in pochi minuti. Alcuni OpenSearch utenti scattano istantanee ogni mezz'ora.

Acquisisci uno snapshot

Quando si crea uno snapshot, specificare quanto segue:

- Il nome del repository di snapshot
- Un nome per lo snapshot

Per brevità e comodità, gli esempi illustrati in questo capitolo utilizzano curl, un comune client HTTP. Per passare un nome utente e una password alla tua richiesta curl, consulta il tutorial Getting started.

Se le tue politiche di accesso specificano utenti o ruoli, devi firmare le tue richieste di snapshot. Per curl, puoi usare l'`--aws-sigv4`opzione con la versione 7.75.0 o successiva. Puoi anche usare gli esempi commentati nel client Python di esempio per effettuare richieste HTTP firmate agli stessi endpoint utilizzati dai comandi curl.

Per acquisire uno snapshot manuale, procedere nel seguente modo:

1. Non puoi acquisire uno snapshot se ne è attualmente in esecuzione un altro. Per verificare, esegui il comando seguente:

   ```
   curl -XGET 'domain-endpoint/_snapshot/_status'
   ```

2. Emettere il comando seguente per acquisire manualmente uno snapshot:

   ```
   curl -XPUT 'domain-endpoint/_snapshot/repository-name/snapshot-name'
   ```

Per includere o escludere determinati indici e specificare altre impostazioni, aggiungere un corpo della richiesta. Per la struttura della richiesta, consulta Take snapshots nella documentazione. OpenSearch

> **Note**
>
> Il tempo necessario per scattare un'istantanea aumenta con la dimensione del dominio del OpenSearch servizio. In caso di operazioni di snapshot di lunga durata, talvolta si verifica l'errore `504 GATEWAY_TIMEOUT`. In genere, è possibile ignorare questi errori e attendere il completamento dell'operazione. Utilizzare il comando seguente per verificare lo stato di tutti gli snapshot del dominio:
>
> ```
> curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
> ```

Ripristino di snapshot

Prima di ripristinare un'istantanea, assicurati che il dominio di destinazione non utilizzi Multi-AZ with Standby. Se lo standby è abilitato, l'operazione di ripristino non riesce.

> **Warning**
>
> Se si utilizzano alias di indice, è necessario interrompere le richieste di scrittura su un alias o passare l'alias a un altro indice prima di eliminarne l'indice. Interrompere le richieste di scrittura consente di evitare il seguente scenario:
>
> 1. L'eliminazione di un indice comporta l'eliminazione anche del relativo alias.
> 2. Una richiesta di scrittura all'alias ormai eliminato crea un nuovo indice con lo stesso nome dell'alias.
> 3. Non puoi più utilizzare l'alias a causa di un conflitto di denominazione con il nuovo indice. Se hai passato l'alias a un altro indice, specifica `"include_aliases": false` durante il ripristino da una snapshot.

Per ripristinare una snapshot

1. Identificare lo snapshot che si desidera ripristinare. Assicurati che tutte le impostazioni di questo indice, come i pacchetti di analisi personalizzati o le impostazioni dei requisiti di allocazione, siano compatibili con il dominio. Per vedere tutti i repository di snapshot, esegui il comando seguente:

   ```
   curl -XGET 'domain-endpoint/_snapshot?pretty'
   ```

   Dopo aver identificato il repository, esegui il comando seguente per visualizzare tutte le snapshot:

   ```
   curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
   ```

   > **Note**
   >
   > La maggior parte delle snapshot automatiche viene archiviata nel repository `cs-automated`. Se il dominio prevede la crittografia dei dati a riposo, gli snapshot saranno archiviati nel repository `cs-automated-enc`. Se il repository di snapshot manuali che si sta cercando non viene trovato, verificare di averlo registrato nel dominio.

2. (Facoltativo) Eliminare o rinominare uno o più indici nel dominio del OpenSearch servizio in caso di conflitti di denominazione tra gli indici del cluster e gli indici nell'istantanea. Non è possibile ripristinare un'istantanea degli indici in un cluster che contiene già indici con gli stessi nomi. OpenSearch

   Se sono presenti conflitti di nomi degli indici, sono disponibili le opzioni seguenti:

   - Elimina gli indici nel dominio di OpenSearch servizio esistente e quindi ripristina l'istantanea.
   - Rinominare gli indici mentre vengono ripristinati dallo snapshot e in seguito reindicizzarli. Per informazioni su come rinominare gli indici, consulta questa richiesta di esempio nella documentazione. OpenSearch
   - Ripristina l'istantanea in un dominio di OpenSearch servizio diverso (possibile solo con istantanee manuali).

   Il comando seguente elimina tutti gli indici esistenti in un dominio:

   ```
   curl -XDELETE 'domain-endpoint/_all'
   ```

Tuttavia, se non si prevede di ripristinare tutti gli indici, è possibile eliminarne uno:

```
curl -XDELETE 'domain-endpoint/index-name'
```

3. Esegui il comando seguente per ripristinare una snapshot:

```
curl -XPOST 'domain-endpoint/_snapshot/repository-name/snapshot-name/_restore'
```

A causa delle autorizzazioni speciali sui OpenSearch dashboard e degli indici di controllo degli accessi dettagliati, i tentativi di ripristinare tutti gli indici potrebbero fallire, soprattutto se si tenta di eseguire il ripristino da un'istantanea automatica. Nell'esempio seguente viene ripristinato solo un indice, `my-index`, da `2020-snapshot` nel repository di snapshot `cs-automated`:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "my-index"}' \
-H 'Content-Type: application/json'
```

In alternativa, è possibile ripristinare tutti gli indici tranne gli indici Dashboards e quelli con controllo granulare degli accessi:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "-.kibana*,-.opendistro*"}' \
-H 'Content-Type: application/json'
```

È possibile ripristinare un'istantanea senza eliminarne i dati utilizzando i parametri and. `rename_pattern` `rename_replacement` Per ulteriori informazioni su questi parametri, consulta i campi di richiesta dell'API Restore Snapshot e la richiesta di esempio nella documentazione. OpenSearch

> **Note**
>
> Se non tutte le partizioni principali sono disponibili per le istanze in questione, uno snapshot può avere `state` come `PARTIAL`. Tale valore indica che i dati provenienti da almeno una partizione non sono stati memorizzati. È comunque possibile eseguire il ripristino da una snapshot parziale, ma potrebbe essere necessario utilizzare le snapshot meno recenti per ripristinare gli indici mancanti.

Eliminazione degli snapshot manuali

Per eliminare uno snapshot manuale, emettere il seguente comando:

```
DELETE _snapshot/repository-name/snapshot-name
```

Automatizzazione delle istantanee con Snapshot Management

È possibile impostare una politica di gestione delle istantanee (SM) nelle OpenSearch dashboard per automatizzare la creazione e l'eliminazione periodiche delle istantanee. SM può creare un'istantanea di un gruppo di indici, mentre Index State Management può scattare una sola istantanea per indice. Per utilizzare SM in OpenSearch Service, devi registrare il tuo repository Amazon S3. Per istruzioni sulla registrazione del repository, consulta Registrazione di un repository di snapshot manuale.

Prima di SM, OpenSearch Service offriva una funzionalità di snapshot automatica e gratuita che è ancora attiva per impostazione predefinita. Questa funzionalità invia istantanee nel repository gestito dal servizio`cs-*`. Per disattivare la funzionalità, contatta. AWS Support

Per ulteriori informazioni sulla funzionalità SM, consulta la sezione Gestione delle istantanee nella OpenSearch documentazione.

Attualmente SM non supporta la creazione di istantanee su più tipi di indici. Ad esempio, se provi a creare un'istantanea su più indici con `*` e alcuni indici si trovano nel livello «warm», la creazione dell'istantanea avrà esito negativo. Se è necessario che l'istantanea contenga più tipi di indice, utilizzate l'azione di istantanea ISM finché SM non supporta questa opzione.

Configurazione delle autorizzazioni

Se si esegue l'aggiornamento alla versione 2.5 da una versione precedente del dominio di OpenSearch servizio, è possibile che le autorizzazioni di sicurezza per la gestione delle istantanee non siano definite nel dominio. Gli utenti non amministratori devono essere mappati a questo ruolo per poter utilizzare la gestione delle istantanee sui domini utilizzando un controllo granulare degli accessi. Per creare manualmente il ruolo di gestione delle istantanee, procedi nel seguente modo:

1. In OpenSearch Dashboard, vai su Sicurezza e scegli Autorizzazioni.
2. Scegliere Crea gruppo di operazioni e configurare i seguenti gruppi:

Group name (Nome gruppo)	Autorizzazioni
`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. Scegliere Ruoli, quindi selezionare Crea ruolo.
4. Assegna un nome al ruolo snapshot_management_role.
5. Per le autorizzazioni del cluster, seleziona o. `snapshot_management_full_access` `snapshot_management_read_access`
6. Scegli Crea.
7. Dopo aver creato il ruolo, associalo a qualsiasi ruolo utente o di backend che gestirà le istantanee.

Considerazioni

Quando configuri la gestione delle istantanee, considera quanto segue:

- È consentita una sola policy per repository.
- Sono consentite fino a 400 istantanee per una policy.
- Questa funzionalità non verrà eseguita se il dominio ha uno stato rosso, è sottoposto a una pressione JVM elevata (85% o superiore) o ha una funzione di snapshot bloccata. Quando le

prestazioni complessive di indicizzazione e ricerca del cluster ne risentono, anche SM potrebbe risentirne.

- Un'operazione di istantanea inizia solo al termine dell'operazione precedente, in modo che nessuna operazione di snapshot simultanea venga attivata da una policy.
- Più politiche con la stessa pianificazione possono causare un picco di risorse. Se gli indici istantanei delle policy si sovrappongono, le operazioni di snapshot a livello di shard possono essere eseguite solo in sequenza, il che può causare problemi di prestazioni a cascata. Se le policy condividono un repository, si verificherà un picco di operazioni di scrittura su quel repository.
- Si consiglia di pianificare l'automazione delle operazioni di snapshot su non più di una volta all'ora, a meno che non si tratti di un caso d'uso particolare.

Automazione di snapshot con Index State Management

È possibile utilizzare l'operazione `snapshot` di Index State Management (ISM) per attivare automaticamente gli snapshot di indici in base alle modifiche relative all'età, alle dimensioni o al numero di documenti. ISM è la soluzione migliore quando è necessaria un'istantanea per indice. Se hai bisogno di un'istantanea di un gruppo di indici, vedi. Automatizzazione delle istantanee con Snapshot Management

Per utilizzare SM in OpenSearch Service, devi registrare il tuo repository Amazon S3. Per un esempio di policy ISM che utilizza l'operazione `snapshot`, consultare Policy di esempio.

Utilizzo di Curator per gli snapshot

Se ISM non funziona per la gestione di indici e snapshot, è possibile utilizzare Curator. Offre funzionalità di filtraggio avanzate utili che semplificano le attività di gestione in cluster complessi. Utilizza pip per installare Curator.

```
pip install elasticsearch-curator
```

È possibile utilizzare Curator come interfaccia a riga di comando (CLI) o API Python. Se utilizzi l'API Python, è necessario utilizzare la versione 7.13.4 o precedente del client elasticsearch-py legacy. Non supporta il client opensearch-py.

Se si utilizza l'interfaccia a riga di comando (CLI), esportare le credenziali dalla riga di comando e configurare `curator.yml` come segue:

```
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
```

Aggiornamento dei domini Amazon Service OpenSearch

> **Note**
>
> OpenSearch e gli aggiornamenti di versione di Elasticsearch differiscono dagli aggiornamenti del software di servizio. Per informazioni sull'aggiornamento del software di servizio per il dominio di OpenSearch servizio, consulta. the section called “Aggiornamenti del software del servizio”

Amazon OpenSearch Service offre aggiornamenti sul posto per i domini con versione OpenSearch 1.0 o successiva oppure Elasticsearch 5.1 o versione successiva. Se utilizzi servizi come Amazon Data Firehose o Amazon CloudWatch Logs per lo streaming di dati su OpenSearch Service, verifica che questi servizi supportino la versione più recente di prima della migrazione. OpenSearch

Argomenti

Percorsi di aggiornamento supportati

Attualmente, OpenSearch Service supporta i seguenti percorsi di aggiornamento:

Dalla versione	Alla versione
OpenSearch 1.3 o 2. x	OpenSearch 2. x La versione 2.3 presenta le seguenti modifiche importanti: • Il `type` parametro è stato rimosso da tutti gli endpoint OpenSearch API nella versione 2.0. Per ulteriori informazioni, consulta la sezione modifiche importanti. • Se il tuo dominio contiene indici (caldi o freddi) originariamente creati in Elasticsearch 6.8, tali indici non sono compatibili con la versione 2.3. UltraWarm OpenSearch Prima di eseguire l'aggiornamento alla versione 2.3, è necessario reindicizzare gli indici incompatibili. Per gli indici incompatibili UltraWarm o freddi, esegui la migrazione alla memorizzazione a caldo, reindicizza i dati e quindi esegui nuovamente la migrazione alla memorizzazione a caldo o a freddo. In alternativa, puoi eliminare questi indici se non sono più necessari. Se accidentalmente effettui l'upgrade del tuo dominio alla versione 2.3 senza aver prima eseguito questi passaggi, non sarai in grado di migrare gli indici incompatibili dal livello di archiviazione attuale. La tua unica opzione è quella di eliminarli.
OpenSearch 1. x	OpenSearch 1. x
Elasticsearch 7.x	Ricerca elastica 7. x o 1. OpenSearch x

Dalla versione	Alla versione
	Important OpenSearch 1. x introduce numerose modifiche sostanziali. Per informazioni dettagliate, vedi Ridenominazione del servizio OpenSearch di Amazon.
Elasticsearch 6.8	Elasticsearch 7. x o 1. OpenSearch x **Important** Elasticsearch 7.0 e OpenSearch 1.0 includono numerose modifiche sostanziali. Prima di iniziare un aggiornamento sul posto, consigliamo di scattare un'istantanea manuale del 6. dominio x, ripristinandolo su un test 7. x o OpenSearch 1. dominio x e utilizzo di quel dominio di test per identificare potenziali problemi di aggiornamento. Per informazioni sulle modifiche introdotte nella OpenSearch versione 1.0, vedereRidenominazione del servizio OpenSearch di Amazon. Come Elasticsearch 6.x, gli indici possono contenere un solo tipo di mappatura, ma tale tipo ora deve essere denominato `_doc`. Di conseguenza, alcune API non richiedono più un tipo di mappatura nel corpo della richiesta (ad esempio l'API `_bulk`). Per i nuovi indici, Elasticsearch 7, ospitato autonomamente. OpenSearch x e 1. x ha un numero di frammenti predefinito pari a uno. OpenSearch Domini di servizio su Elasticsearch 7. x e versioni successive mantengono il precedente valore predefinito di cinque.
Elasticsearch 6.x	Elasticsearch 6.x

Dalla versione	Alla versione
Elasticsearch 5.6	Elasticsearch 6.x **Important** Gli indici creati nella versione 6.x non supportano più tipi di mappatura diversi. Gli indici creati nella versione 5.x supportano ancora tipi di mappatura diversi quando sono ripristinati in un cluster 6.x. Controllare che il codice cliente crei un solo tipo di mappatura per indice. Per ridurre al minimo i tempi di inattività durante l'aggiornamento da Elasticsearch 5.6 a 6. x, OpenSearch Service reindicizza l'`.kibana`indice su`.kibana-6` , elimina`.kibana`, crea un alias denominato `.kibana` e associa il nuovo indice al nuovo alias.
Elasticsearch 5.x	Elasticsearch 5.x

Il processo di aggiornamento è costituito da tre fasi:

1. Controlli prima dell'aggiornamento: il OpenSearch servizio verifica la presenza di problemi che possono bloccare un aggiornamento e non procede alla fase successiva a meno che tali controlli non abbiano esito positivo.
2. Istantanea: il OpenSearch servizio scatta un'istantanea del cluster OpenSearch o Elasticsearch e non procede al passaggio successivo a meno che l'istantanea non abbia esito positivo. Se l'aggiornamento non riesce, OpenSearch Service utilizza questa istantanea per ripristinare il cluster allo stato originale. Per ulteriori informazioni, consulta the section called “Impossibile eseguire il downgrade dopo l'aggiornamento”.
3. Aggiornamento: il OpenSearch servizio avvia l'aggiornamento, che può richiedere da 15 minuti a diverse ore per essere completato. OpenSearch I dashboard potrebbero non essere disponibili durante alcuni o tutti gli upgrade.

Avvio di un aggiornamento (console)

Il processo di aggiornamento è irreversibile e non può essere sospeso né annullato. Durante un aggiornamento, non è possibile apportare modifiche di configurazione al dominio. Prima di avviare un aggiornamento, controllare attentamente che si desidera continuare. Puoi usare queste stesse fasi per eseguire il controllo di pre-aggiornamento senza di fatto avviare un aggiornamento.

Se il cluster dispone di nodi master dedicati, OpenSearch gli aggiornamenti vengono completati senza tempi di inattività. In caso contrario, il cluster potrebbe non rispondere per alcuni secondi dopo l'aggiornamento mentre elegge un nodo master.

Per aggiornare un dominio a una versione successiva di Elasticsearch OpenSearch

1. Acquisire uno snapshot manuale del dominio. Questa istantanea funge da backup che puoi ripristinare su un nuovo dominio se desideri tornare a utilizzare la versione precedente. OpenSearch
2. Passare all'indirizzo https://aws.amazon.com e scegliere Sign In to the Console (Accedi alla console).
3. In Analytics, scegli Amazon OpenSearch Service.
4. Nel riquadro di navigazione, scegli il dominio da aggiornare in Domains (Domini).
5. Scegli Operazioni, quindi Aggiorna.
6. Scegli la versione a cui eseguire l'aggiornamento. Se stai effettuando l'aggiornamento a una OpenSearch versione, viene visualizzata l'opzione Abilita la modalità di compatibilità. Se abiliti questa impostazione, OpenSearch riporta la sua versione come 7.10 per consentire ai client OSS e ai plugin Elasticsearch OSS come Logstash di continuare a lavorare con Amazon Service. OpenSearch Puoi disattivare questa operazione in un secondo momento
7. Seleziona Upgrade (Aggiorna).
8. Controlla il campo Stato dominio nel pannello di controllo del dominio per monitorare lo stato dell'aggiornamento.

Avvio di un aggiornamento (CLI)

Puoi utilizzare le seguenti operazioni per identificare la versione corretta di OpenSearch Elasticsearch per il tuo dominio, avviare un aggiornamento sul posto, eseguire il controllo pre-aggiornamento e visualizzare lo stato di avanzamento:

- `get-compatible-versions` (`GetCompatibleVersions`)
- `upgrade-domain` (`UpgradeDomain`)
- `get-upgrade-status` (`GetUpgradeStatus`)
- `get-upgrade-history` (`GetUpgradeHistory`)

Per ulteriori informazioni, consulta il riferimento ai comandiAWS CLI e il riferimento all'API di Amazon OpenSearch Service.

Avvio di un aggiornamento (SDK)

Questo esempio utilizza il client Python di OpenSearchServicebasso livello di AWS SDK for Python (Boto) per verificare se un dominio è idoneo per l'aggiornamento a una versione specifica, lo aggiorna e controlla continuamente lo stato dell'aggiornamento.

```
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()
```

Errori nella risoluzione dei problemi di convalida

Quando avvii un aggiornamento di una versione OpenSearch o di Elasticsearch, OpenSearch Service esegue innanzitutto una serie di controlli di convalida per garantire che il tuo dominio sia idoneo per un aggiornamento. Se uno di questi controlli non riesce, si riceve una notifica contenente i problemi specifici che è necessario correggere prima di aggiornare il dominio. Per un elenco dei potenziali problemi e dei passaggi per risolverli, consulta the section called “Risoluzione degli errori di convalida”.

Risoluzione dei problemi relativi all'aggiornamento

Aggiornamenti locali richiedono domini sani. Il dominio potrebbe essere non idoneo per un aggiornamento o non completare l'aggiornamento per diversi motivi. La tabella riportata di seguito mostra i problemi più comuni.

Problema	Descrizione
Plugin opzionale non supportato	Quando si aggiorna un dominio con plug-in opzionali, OpenSearc h Service aggiorna automaticamente anche i plug-in. Pertanto, la versione di destinazione del dominio deve supportare anche questi plugin opzionali. Se nel dominio è installato un plug-in opzionale che non è disponibile per la versione di destinazione, la richiesta di aggiornamento ha esito negativo.
Troppe partizioni per nodo	OpenSearch, oltre a 7. x versioni di Elasticsearch hanno un'impost azione predefinita di non più di 1.000 shard per nodo. Se un nodo del cluster corrente supera questa impostazione, il OpenSearch servizio non consente l'aggiornamento. Consulta the section called “Limite massimo di partizioni superato” per le opzioni di risoluzione dei problemi.
Dominio in elaborazi one	Il dominio è nel mezzo di una modifica di configurazione. Controlla l'idoneità dell'aggiornamento al termine dell'operazione.
Cluster in stato rosso	Uno o più indici nel cluster sono in stato rosso. Per la risoluzione dei problemi, consulta the section called “Cluster in stato rosso”.
Elevata percentuale di errori	Il cluster restituisce un numero elevato di errori 5xx durante il tentativo di elaborazione delle richieste. Questo problema è in genere il risultato di un numero eccessivo di richieste di lettura o scrittura simultanee. Valuta

Problema	Descrizione
	la possibilità di ridurre il traffico verso il cluster o di eseguire il dimension amento del dominio.
Split brain	Split brain significa che il cluster contiene più nodi principali ed è stato diviso in due cluster che non verranno mai riuniti in modo autonomo. Puoi evitare lo split brain utilizzando il numero consigliato di nodi master dedicati. Per risolvere un problema di split brain, contatta AWS Support.
Impossibile trovare nodo master	OpenSearch Il servizio non riesce a trovare il nodo principale del cluster. Se il dominio utilizza il Multi-AZ, un errore nella zona di disponibilità potrebbe aver causato la perdita del quorum da parte del cluster e la conseguente incapacità di eleggere un nuovo nodo master. Se il problema non si risolve automaticamente, contatta AWS Support.
Troppe attività in sospeso	Il nodo master si trova in condizioni di carico elevato e presenta numerose attività in sospeso. Valuta la possibilità di ridurre il traffico verso il cluster o di eseguire il dimensionamento del dominio.
Volume di archiviaz ione compromesso	Il volume del disco di uno o più nodi non funziona correttamente. Questo problema si verifica spesso insieme ad altri problemi, come un'elevat a percentuale di errori o troppe attività in sospeso. Se si verifica in isolamento e non si risolve automaticamente, contatta AWS Support.
Problema chiave KMS	La chiave KMS utilizzata per crittografare il dominio non è accessibile o manca. Per ulteriori informazioni, consultare the section called “Monitora ggio dei domini che crittografano dati a riposo”.
Snapshot in corso	Il dominio sta attualmente acquisendo una snapshot. Controlla l'idoneit à dell'aggiornamento al termine della snapshot. Verifica anche che puoi elencare repository snapshot manuali, elencare snapshot all'interno di tali repository e acquisire snapshot manuali. Se OpenSearch il Servizio non è in grado di verificare se un'istantanea è in corso, gli aggiornamenti possono avere esito negativo.
Timeout o errore snapshot	Il pre-aggiornamento snapshot richiede troppo tempo o non è riuscito. Verifica l'integrità del cluster e riprova. Se il problema persiste, contatta AWS Support.

Problema	Descrizione
Indici incompatibili	Uno o più indici sono incompatibili con la versione di destinazione. Questo problema può verificarsi se hai migrato gli indici da una versione precedente di Elasticsearch o Elasticsearch. OpenSearch Reindicizzare gli indici e riprovare.
Elevato utilizzo del disco	L'utilizzo del disco per il cluster supera il 90%. Elimina i dati o ricalibra il dominio e riprova.
Elevato utilizzo JVM	L'utilizzo della memoria JVM è superiore al 75%. Riduci il traffico verso il cluster o ricalibra il dominio e riprova.
OpenSearch Problema con gli alias dei dashboard	`.dashboards` è già configurato come alias ed è mappato su un indice incompatibile, probabilmente uno di una versione precedente di Dashboards. OpenSearch Reindicizza e riprova.
Stato rosso di Dashboards	OpenSearch Lo stato del pannello di controllo è rosso. Provare a usare Dashboards al termine dell'aggiornamento. Se lo stato rosso persiste, risolvilo manualmente e riprova.
Compatibilità tra cluster	È possibile eseguire l'aggiornamento solo se viene mantenuta la compatibilità tra cluster tra i domini di origine e di destinazione dopo l'aggiornamento. Durante il processo di aggiornamento, vengono identific ate tutte le connessioni non compatibili. Per procedere, aggiornare il dominio remoto o eliminare le connessioni non compatibili. Tenere presente che se la replica è attiva sul dominio, non è possibile riprenderla dopo aver eliminato la connessione.
Altro problema relativo OpenSearc h al servizio di assistenza	Problemi relativi al OpenSearch Servizio stesso potrebbero far sì che il dominio venga visualizzato come non idoneo per un aggiornamento. Se nessuna delle condizioni precedenti si applica al dominio e il problema persiste per più di un giorno, contatta AWS Support.

Utilizzo di uno snapshot per migrare i dati

Gli aggiornamenti sul posto sono il modo più semplice, veloce e affidabile per aggiornare un dominio a una versione successiva OpenSearch o di Elasticsearch. Gli snapshot sono un'ottima opzione

se occorre migrare da una versione precedente alla 5.1 di Elasticsearch o si desidera migrare a un cluster completamente nuovo.

La tabella seguente mostra come utilizzare le istantanee per migrare i dati verso un dominio che utilizza una versione diversa o di Elasticsearch. OpenSearch Per informazioni su come acquisire e ripristinare gli snapshot, consulta the section called “Creazione di snapshot di indici”.

Dalla versione	Alla versione	Processo di migrazione

OpenSearch 1.3 o 2. x	OpenSearch 2. x	1. Consulta le ultime modifiche apportate alla versione OpenSearch 2.3 per vedere se è necessario apportare modifiche agli indici o alle applicazioni.
		2. Crea un'istantanea manuale della versione 1.3 o 2. dominio x.
		3. Crea un 2. dominio x che è una versione superiore alla versione 1.3 o 2 originale. dominio x.
		4. Ripristina l'istantanea dal dominio originale al 2. dominio x. Durante l'operazione, potrebbe essere necessario ripristinare l'`.opensearch` indice con un nuovo nome:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".opensearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		Quindi è possibile reindicizzare `.backup-opensearch` sul nuovo dominio e configurarlo come alias su `.opensearch` . Tieni presente che la chiamata `_restore` REST non include `include_global_state` perché l'impostazione predefinita in `_restore` è false. Di conseguenza, il dominio di test

Dalla versione	Alla versione	Processo di migrazione
		non includerà alcun modello di indice e non avrà lo stato completo del backup. 5. Se non si ha più bisogno del dominio originale, eliminarlo. In caso contrario, verranno addebitati i costi per il dominio.

OpenSearch 1. x	OpenSearch 1. x	1. Crea un'istantanea manuale del file 1. dominio x.
		2. Crea un 1. dominio x che è una versione superiore a quella originale 1. dominio x.
		3. Ripristina l'istantanea dal dominio originale al nuovo 1. dominio x. Durante l'operazione, potrebbe essere necessario ripristinare l'`.opensearch` indice con un nuovo nome:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".opensearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		Quindi è possibile reindicizzare `.backup-opensearch` sul nuovo dominio e configurarlo come alias su `.opensearch` . Tieni presente che la chiamata `_restore` REST non include `include_global_state` perché l'impostazione predefinita in `_restore` è false. Di conseguenza, il dominio di test non includerà alcun modello di indice e non avrà lo stato completo del backup.
		4. Se non si ha più bisogno del dominio originale, eliminarlo. In caso contrario, verranno addebitati i costi per il dominio.

Dalla versione	Alla versione	Processo di migrazione

Elasticsearch 6.x o 7.x	OpenSearch 1. x	1. Consulta le ultime modifiche apportate alla OpenSearch versione 1.0 per vedere se è necessario apportare modifiche agli indici o alle applicazioni.
		2. Creare uno snapshot manuale del dominio Elasticsearch 7.x o 6.x.
		3. Crea un 1. OpenSearch dominio x.
		4. Ripristina l'istantanea dal dominio Elasticsearch al dominio. OpenSearch Durante l'operazione, potrebbe essere necessario ripristinare l'`.elasticsearch` indice con un nuovo nome:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		Quindi è possibile reindicizzare `.backup-opensearch` sul nuovo dominio e configurarlo come alias su `.elasticsearch` . Tieni presente che la chiamata `_restore` REST non include `include_global_state` perché l'impostazione predefinita in `_restore` è false. Di conseguenza, il dominio di test non includerà alcun modello di indice e non avrà lo stato completo del backup.
		5. Se non si ha più bisogno del dominio originale, eliminarlo. In caso contrario, verranno addebitati i costi per il dominio.

Dalla versione	Alla versione	Processo di migrazione

Elasticsearch 6.x	Elasticsearch 7.x	1. Esaminare le modifiche importanti in 7.0 per vedere se è necessario adeguare gli indici o le applicazioni.
		2. Creare una snapshot manuale del dominio 6.x.
		3. Creare un dominio 7.x.
		4. Ripristinare la snapshot dal dominio originale al dominio 7.x. Durante l'operazione, è probabile che sia necessario ripristinare l'indice `.opensearch` con un nuovo nome:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-elasticsearch"`
		`}`
		Quindi è possibile reindicizzare `.backup-elasticsearch` sul nuovo dominio e configurarlo come alias su `.elasticsearch` . Tieni presente che la chiamata `_restore` REST non include `include_global_state` perché l'impostazione predefinita `_restore` è false. Di conseguenza, il dominio di test non includerà alcun modello di indice e non avrà lo stato completo del backup.
		5. Se non si ha più bisogno del dominio originale, eliminarlo. In caso contrario, verranno addebitati i costi per il dominio.

Dalla versione	Alla versione	Processo di migrazione
Elasticsearch 6.x	Elasticsearch 6.8	1. Creare una snapshot manuale del dominio 6.x. 2. Creare un dominio 6.8. 3. Ripristinare lo snapshot dal dominio originale nel dominio 6.8. 4. Se non si ha più bisogno del dominio originale, eliminarlo. In caso contrario, verranno addebitati i costi per il dominio.
Elasticsearch 5.x	Elasticsearch 6.x	1. Esaminare le modifiche importanti in 6.0 per vedere se è necessario adeguare gli indici o le applicazioni. 2. Creare una snapshot manuale del dominio 5.x. 3. Creare un dominio 6.x. 4. Ripristinare la snapshot dal dominio originale al dominio 6.x. 5. Se non si ha più bisogno del dominio 5.x, eliminarl o. In caso contrario, verranno addebitati i costi per il dominio.
Elasticsearch 5.x	Elasticsearch 5.6	1. Creare una snapshot manuale del dominio 5.x. 2. Creare un dominio 5.6. 3. Ripristinare la snapshot dal dominio originale al dominio 5.6. 4. Se non si ha più bisogno del dominio originale, eliminarlo. In caso contrario, verranno addebitati i costi per il dominio.

Dalla versione	Alla versione	Processo di migrazione
Elasticsearch 2.3	Elasticsearch 6.x	Gli snapshot di Elasticsearch 2.3 non sono compatibili con la versione 6.x. Per migrare i dati direttamente da 2.3 a 6.x, è necessario ricreare manualmente gli indici nel nuovo dominio. In alternativa, è possibile seguire i passaggi da 2.3 a 5.x in questa tabella, eseguire le operazioni `_reindex` nel nuovo dominio 5.x per convertire gli indici 2.3 negli indici 5.x e seguire i passaggi da 5.x a 6.x.
Elasticsearch 2.3	Elasticsearch 5.x	1. Esaminare le modifiche importanti in 5.0 per vedere se è necessario adeguare gli indici o le applicazioni. 2. Creare una snapshot manuale del dominio 2.3. 3. Creare un dominio 5.x. 4. Ripristinare la snapshot dal dominio 2.3 al dominio 5.x. 5. Se non si ha più bisogno del dominio 2.3, eliminarl o. In caso contrario, verranno addebitati i costi per il dominio.
Elasticsearch 1.5	Elasticsearch 5.x	Gli snapshot di Elasticsearch 1.5 non sono compatibi li con la versione 5.x. Per migrare i dati da 1.5 a 5.x, è necessario ricreare manualmente gli indici nel nuovo dominio. **Important** Le istantanee 1.5 sono compatibili con 2.3, ma i domini OpenSearch Service 2.3 non supportan o l'`_reindex`operazione. Poiché non è possibile reindicizzarli, gli indici originati in un dominio 1.5 non riescono a effettuare il ripristino dalle snapshot 2.3 a domini 5.x.

Dalla versione	Alla versione	Processo di migrazione
Elasticsearch 1.5	Elasticsearch 2.3	1. Utilizzare il plugin di migrazione per scoprire se è possibile effettuare direttamente l'upgrade alla versione 2.3. Potrebbe essere necessario modificare i dati prima della migrazione. a. In un browser Web, aprire `http://domain-endpoint /_plugin/migration/` . b. Scegliere Run checks now (Esegui controlli). c. Esaminare i risultati e, se necessario, seguire le istruzioni per modificare i dati. 2. Creare una snapshot manuale del dominio 1.5. 3. Creare un dominio 2.3. 4. Ripristinare la snapshot dal dominio 1.5 al dominio 2.3. 5. Se non si ha più bisogno del dominio 1.5, eliminarlo. In caso contrario, verranno addebitati i costi per il dominio.

Creazione di un endpoint personalizzato per Amazon Service OpenSearch

La creazione di un endpoint personalizzato per il tuo dominio Amazon OpenSearch Service ti semplifica il riferimento agli URL tuoi OpenSearch e di OpenSearch Dashboard. Puoi includere il marchio della tua azienda o semplicemente utilizzare un easier-to-remember endpoint più corto di quello standard.

Se è necessario passare a un nuovo dominio, aggiornare il DNS in modo che punti al nuovo URL e continuare a utilizzare lo stesso endpoint di prima.

Puoi proteggere gli endpoint personalizzati generando un certificato in AWS Certificate Manager (ACM) o importandone uno tuo.

Endpoint personalizzati per nuovi domini

È possibile abilitare un endpoint personalizzato per un nuovo dominio di OpenSearch servizio utilizzando la console di OpenSearch servizio o l'API di configurazione AWS CLI.

Come personalizzare l'endpoint (console)

1. Dalla console OpenSearch di servizio, scegli Crea dominio e fornisci un nome per il dominio.
2. In Endpoint personalizzato, selezionare Abilita endpoint personalizzato.
3. Per Nome host personalizzato, immettere il nome host dell'endpoint personalizzato preferito. Il nome host deve essere un nome di dominio completo (FQDN) come www.tuodominio.com o esempio.tuodominio.com.

   > **Note**
   >
   > Se non si dispone di un certificato jolly, sarà necessario ottenere un nuovo certificato per i domini secondari dell'endpoint personalizzato.

4. Per Certificato AWS , scegliere il certificato SSL che si desidera utilizzare per il dominio. Se non sono disponibili certificati, è possibile importarne uno in ACM o utilizzare ACM per eseguirne il provisioning. Per informazioni su come creare un certificato, consultare Emissione e gestione di certificati nella Guida per l'utente di AWS Certificate Manager.

   > **Note**
   >
   > Il certificato deve avere il nome dell'endpoint personalizzato e appartenere allo stesso account del dominio OpenSearch di servizio. Lo stato del certificato deve essere EMESSO.

   - Completa la procedura per creare il dominio e scegli Crea.
   - Al termine dell'elaborazione selezionare il dominio per visualizzare l'endpoint personalizzato.

   Per utilizzare la CLI o l'API di configurazione, utilizzare le operazioni `CreateDomain` e `UpdateDomainConfig`. Per ulteriori informazioni, consulta AWS CLI Command Reference e Amazon OpenSearch Service API Reference.

Endpoint personalizzati per domini esistenti

Per aggiungere un endpoint personalizzato a un dominio di OpenSearch servizio esistente, scegli Modifica ed esegui i passaggi da 2 a 4 precedenti.

Passaggi successivi

Dopo aver abilitato un endpoint personalizzato per il tuo dominio di OpenSearch servizio, puoi creare una mappatura CNAME in Amazon Route 53 (o nel tuo provider di servizi DNS preferito). La creazione di una mappatura CNAME ti consentirà di indirizzare il traffico verso il tuo endpoint personalizzato e i relativi sottodomini. Senza questa mappatura, non sarai in grado di indirizzare il traffico verso il tuo endpoint personalizzato. Per i passaggi per creare questa mappatura in Route 53, vedi Configurazione del routing DNS per un nuovo dominio e Creazione di una nuova zona ospitata per un sottodominio. Per altri provider, consultare la relativa documentazione.

Crea un record CNAME che punti l'endpoint personalizzato all'endpoint del dominio generato automaticamente. Se il tuo dominio è dual stack, puoi indirizzare il record CNAME verso uno dei due endpoint generati dal servizio. La funzionalità dual stack dell'endpoint personalizzato dipende dall'endpoint generato dal servizio a cui punti il record CNAME. Il nome host dell'endpoint personalizzato è il nome del record CNAME e il nome host dell'endpoint del dominio è il valore del record CNAME.

Se utilizzi l'autenticazione SAML per le OpenSearch dashboard, devi aggiornare il tuo IdP con il nuovo URL SSO.

Puoi usare Amazon Route 53 per creare un tipo di record alias per indirizzare l'endpoint personalizzato del tuo dominio verso un endpoint di ricerca dual stack. Per creare un tipo di record alias, devi configurare il tuo dominio per utilizzare il tipo di indirizzo IP dual stack. Puoi farlo utilizzando l'API Route 53.

Per creare un tipo di record di alias utilizzando l'API Route 53, specifica la destinazione dell'alias del tuo dominio. Puoi trovare l'alias target del tuo dominio nel campo Hosted Zone (dual stack) nella sezione degli endpoint personalizzati della console di OpenSearch servizio oppure utilizzando l'`DescribeDomain`API e copiando il valore di. `DomainEndpointV2HostedZoneId`

Auto-Tune per Amazon Service OpenSearch

Auto-Tune in Amazon OpenSearch Service utilizza i parametri di prestazioni e utilizzo del OpenSearch cluster per suggerire modifiche alla configurazione relative alla memoria, tra cui le

dimensioni della coda e della cache e le impostazioni della macchina virtuale Java (JVM) sui nodi. Queste modifiche facoltative migliorano la velocità e la stabilità del cluster.

Alcune modifiche vengono implementate immediatamente, mentre altre sono pianificate durante la finestra non di punta del dominio. Puoi ripristinare le impostazioni predefinite del OpenSearch servizio in qualsiasi momento. Man mano che Auto-Tune raccoglie e analizza le metriche delle prestazioni per il tuo dominio, puoi visualizzarne i consigli nella console di OpenSearch servizio nella pagina Notifiche.

Auto-Tune è disponibile in commercio Regioni AWS su domini che eseguono qualsiasi OpenSearch versione o Elasticsearch 6.7 o versione successiva, con un tipo di istanza supportato.

Argomenti

Tipi di modifiche

La regolazione automatica ha due grandi categorie di modifiche:

- Modifiche senza interruzioni che applica durante l'esecuzione del cluster.
- Modifiche che richiedono una distribuzione blu/verde, da applicare durante la finestra non di punta del dominio.

In base ai parametri delle prestazioni del dominio, la regolazione automatica può suggerire regolazioni alle seguenti impostazioni:

Tipo di modifica	Categoria	Descrizione
Dimensioni heap JVM	Blu/verde	Per impostazione predefinita, OpenSearch Service utilizza il 50% della RAM di un'istanza per l'heap JVM, fino a una dimensione dell'heap di 32 GiB.

Tipo di modifica	Categoria	Descrizione
		L'aumento di questa percentuale offre OpenSearch più memoria, ma ne lascia meno per il sistema operativo e altri processi. Valori maggiori possono ridurre il numero di interruzioni di garbage collection, ma aumentare la lunghezza di tali interruzioni.
Impostazioni JVM di nuova generazione	Blu/verde	Le impostazioni di "nuova generazione" di JVM influenzano la frequenza delle garbage collection minori. Le raccolte minori più frequenti possono diminuire il numero di raccolte principali e interruzioni.
Dimensioni della coda	Senza interruzioni	Per impostazione predefinita, la dimensione della coda di ricerca è `1000` e la dimensione della coda di scrittura è`10000`. La regolazione automatica dimensiona automaticamente le code di ricerca e scrittura se è disponibile un heap aggiuntivo per gestire le richieste.
Dimensioni della cache	Senza interruzioni	La cache dei campi monitora le strutture dati on-heap, quindi è importante monitorare l'utilizzo della cache. La regolazione automatica dimensiona la dimensione della cache dei dati sul campo per evitare problemi di memoria esaurita e di interruttore. La cache di richieste delle partizioni viene gestita a livello di nodo e ha una dimensione massima di default pari all'1% dell'heap. La regolazione automatica dimensiona la dimensione della cache delle richieste delle partizioni per accettare più richieste di ricerca e indice rispetto a quelle gestite dal cluster configurato.

Tipo di modifica	Categoria	Descrizione
Dimensione richiesta	Senza interruzioni	Per impostazione predefinita, quando la dimensione aggregata delle richieste in corso supera il 10% del totale della JVM (2% per i tipi di `t2` istanze e 1% per`t3.small`), limita tutte OpenSearch le richieste nuove `_search` e `_bulk` fino al completamento delle richieste esistenti. Auto-Tune regola automaticamente questa soglia, tipicamente tra il 5-15%, in base alla quantità di JVM attualmente occupata nel sistema. Ad esempio, se la pressione della memoria JVM è elevata, Auto-Tune potrebbe ridurre la soglia al 5%, a quel punto si potrebbero vedere più rifiuti fino a quando il cluster non si stabilizza e la soglia aumenta.

Abilitazione o disabilitazione della regolazione automatica

OpenSearch Il servizio abilita Auto-Tune per impostazione predefinita sui nuovi domini. Per abilitare o disabilitare Auto-Tune sui domini esistenti, consigliamo di utilizzare la console, che semplifica il processo. L'abilitazione della regolazione automatica non causa una implementazione blu/verde.

Al momento non è possibile abilitare o disabilitare l'ottimizzazione automatica tramite AWS CloudFormation.

Console

Per abilitare Auto-Tune su un dominio esistente

1. Apri la console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel riquadro di navigazione, in Domini, scegli il nome di dominio per aprire la configurazione del cluster.
3. Scegli Attiva se Auto-Tune non è già abilitato.
4. Facoltativamente, seleziona la finestra Off-peak per pianificare le ottimizzazioni che richiedono una distribuzione blu/verde durante la finestra non di picco configurata del dominio. Per ulteriori informazioni, consulta the section called “Pianificazione dei miglioramenti di Auto-Tune”.

5. Seleziona Save changes (Salva modifiche).

CLI

Per abilitare Auto-Tune utilizzando il, invia una richiesta: AWS CLI UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options DesiredState=ENABLED
```

Pianificazione dei miglioramenti di Auto-Tune

Prima del 16 febbraio 2023, Auto-Tune utilizzava le finestre di manutenzione per pianificare le modifiche che richiedevano un'implementazione blu/verde. Le finestre di manutenzione sono ora obsolete a favore delle finestre non di punta, che sono blocchi di tempo giornalieri di 10 ore durante i quali il traffico sul dominio è generalmente ridotto. Puoi modificare l'ora di inizio predefinita per la finestra non di punta, ma non puoi modificare la lunghezza.

Tutti i domini che avevano le finestre di manutenzione Auto-Tune abilitate prima dell'introduzione delle finestre non di punta il 16 febbraio 2023 possono continuare a utilizzare le finestre di manutenzione precedenti senza interruzioni. Tuttavia, ti consigliamo di migrare i domini esistenti per utilizzare invece la finestra non di punta per la manutenzione del dominio. Per istruzioni, consulta the section called “Migrazione dalle finestre di manutenzione di Auto-Tune”.

Console

Per pianificare le azioni di Auto-Tune, la finestra non di punta

1. Apri la console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nel riquadro di navigazione, in Domini, scegli il nome di dominio per aprire la configurazione del cluster.
3. Vai alla scheda Auto-Tune e scegli Modifica.
4. Scegli Attiva se Auto-Tune non è già abilitato.
5. In Pianifica le ottimizzazioni durante le finestre non di punta, seleziona Finestra non di punta.
6. Sceglie Save changes (Salva modifiche).

CLI

Per configurare il tuo dominio in modo da pianificare le azioni di Auto-Tune durante la finestra configurata non di punta, includi nella richiesta: `UseOffPeakWindow` UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=null
```

Monitoraggio delle modifiche Auto-Tune

È possibile monitorare le statistiche di Auto-Tune in. Amazon CloudWatch Per un elenco completo di parametri, consulta the section called “Metriche Auto-Tune”.

OpenSearch Il servizio invia eventi Auto-Tune ad Amazon. EventBridge Puoi utilizzarlo EventBridge per configurare regole che inviano un'e-mail o eseguono un'azione specifica quando viene ricevuto un evento. Per vedere il formato di ogni evento Auto-Tune inviato a EventBridge, vedithe section called “Eventi di regolazione automatica”.

Taggare i domini Amazon OpenSearch Service

I tag ti consentono di assegnare informazioni arbitrarie a un dominio Amazon OpenSearch Service in modo da poterle classificare e filtrare in base a tali informazioni. Un tag è una coppia chiave-valore che definisci e associ a un dominio di servizio. OpenSearch Puoi utilizzare questi tag per tenere traccia dei costi raggruppando le spese per risorse con tag simili. AWS non applica alcun significato semantico ai tag. I tag sono interpretati prettamente come stringhe di caratteri. Tutti i tag includono gli elementi seguenti:

Elemento del tag	Descrizione	Richiesto
Chiave tag	La chiave di tag corrisponde al nome del tag. La chiave deve essere unica per il dominio del OpenSearch servizio a cui è collegata. Per un elenco di restrizioni di base su chiavi e valori dei tag, consulta la sezione relativa alle restrizioni per i tag definiti dall'utente.	Sì
Valore tag	Il valore di tag è un valore di stringa del tag. I valori dei tag possono essere `null` e non devono necessariamente essere univoci in un set	No

Elemento del tag	Descrizione	Richiesto
	di tag. Ad esempio, può esserci una coppia chiave-valore in un set di tag project/Trinity e in cost-center/Trinity. Per un elenco di restrizioni di base su chiavi e valori dei tag, consulta la sezione relativa alle restrizioni per i tag definiti dall'utente.	

Ogni dominio OpenSearch di servizio ha un set di tag, che contiene tutti i tag assegnati a quel dominio OpenSearch di servizio. AWS non assegna automaticamente alcun tag ai domini di OpenSearch servizio. Un set di tag può contenere tra 0 e 50 tag. Se si aggiunge un tag a un dominio con la stessa chiave di un tag esistente, il nuovo valore sovrascrive il vecchio valore.

Esempi di assegnazione di tag

È possibile utilizzare una chiave di tag per definire una categoria e il valore del tag potrebbe essere un elemento di tale categoria. Ad esempio, è possibile definire una chiave di tag `project` e un valore di tag di`Salix`, che indicano che il dominio OpenSearch Service è assegnato al progetto Salix. È inoltre possibile utilizzare i tag per designare i domini di OpenSearch servizio da utilizzare per il test o la produzione utilizzando una chiave come o. `environment=test` `environment=production` Prova a utilizzare un set coerente di chiavi di tag per semplificare il monitoraggio dei metadati associati OpenSearch ai domini di servizio.

Puoi anche utilizzare i tag per organizzare la AWS fattura in modo che rifletta la tua struttura dei costi. A tale scopo, registrati per ricevere la Account AWS fattura con i valori chiave dell'etichetta inclusi. Quindi, per visualizzare il costo delle risorse combinate, puoi organizzare le informazioni di fatturazione in base alle risorse con gli stessi valori di chiave di tag. Ad esempio, puoi taggare diversi domini di OpenSearch servizio con coppie chiave-valore e quindi organizzare i dati di fatturazione per visualizzare il costo totale di ogni dominio per diversi servizi. Per ulteriori informazioni, consultare la sezione relativa all'utilizzo dei tag per l'allocazione dei costi nella documentazione relativa a gestione di costi e fatturazioneAWS .

> **Note**
>
> I tag sono memorizzati nella cache a fini di autorizzazione. Per questo motivo, le aggiunte e gli aggiornamenti ai tag sui domini di OpenSearch servizio potrebbero richiedere alcuni minuti prima che siano disponibili.

Utilizzo dei tag (console)

La console è il modo più semplice per assegnare un tag a un dominio.

Per creare un tag (console)

1. Andare all'indirizzo https://aws.amazon.com e quindi scegliere Sign In to the Console (Accedi alla console).
2. In Analytics, scegli Amazon OpenSearch Service.
3. Seleziona il dominio a cui aggiungere i tag e passa alla scheda Tag.
4. Scegli Gestisci, quindi seleziona Aggiungi nuovo tag.
5. Inserire una chiave di tag e un valore facoltativo.
6. Selezionare Salva.

Per eliminare un tag, esegui la stessa procedura e scegli Rimuovi nella pagina Gestisci tag.

Per ulteriori informazioni sull'utilizzo della console per il funzionamento con i tag, consulta Editor di tag nella Guida alle operazioni di base della Console di gestioneAWS .

Utilizzo dei tag (AWS CLI)

Puoi creare tag di risorse usando il --add-tags comando AWS CLI with the.

Sintassi

```
add-tags --arn=<domain_arn> --tag-list Key=<key>,Value=<value>
```

Parametro	Descrizione
`--arn`	Nome della risorsa Amazon per il dominio di OpenSearch servizio a cui è associato il tag.
`--tag-list`	Insieme di coppie chiave-valore separate da spazi nel seguente formato: `Key=<key>,Value=<value>`

Esempio

Nell'esempio seguente vengono creati due tag per il dominio logs:

```
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
```

Puoi rimuovere i tag da un dominio OpenSearch di servizio utilizzando il --remove-tags comando.

Sintassi

```
remove-tags --arn=<domain_arn> --tag-keys Key=<key>,Value=<value>
```

Parametro	Descrizione
`--arn`	Amazon Resource Name (ARN) per il dominio OpenSearch di servizio a cui è associato il tag.
`--tag-keys`	Set di coppie chiave-valore separate da spazi che desideri rimuovere dal dominio del servizio. OpenSearch

Esempio

Nell'esempio seguente, i due tag creati nell'esempio precedente vengono rimossi dal dominio logs:

```
aws opensearch remove-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-
keys service instances
```

È possibile visualizzare i tag esistenti per un dominio di OpenSearch servizio con il comando: --list-tags

Sintassi

```
list-tags --arn=<domain_arn>
```

Parametro	Descrizione
`--arn`	Amazon Resource Name (ARN) per il dominio di OpenSearch servizio a cui sono allegati i tag.

Esempio

Nell'esempio seguente vengono elencati tutti i tag di risorsa per il dominio logs:

```
aws opensearch list-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs
```

Lavorare con i tag (AWS SDK)

Gli AWS SDK (ad eccezione degli SDK per Android e iOS) supportano tutte le azioni definite nell'Amazon OpenSearch Service API Reference, tra cui `AddTags`, `ListTags`, e `RemoveTags` le operazioni. Per ulteriori informazioni sull'installazione e l'utilizzo degli AWS SDK, consulta AWS Software Development Kits.

Python

Questo esempio utilizza il client Python di OpenSearchServicebasso livello dell'SDK AWS per Python (Boto) per aggiungere un tag a un dominio, elencare il tag associato al dominio e rimuovere un tag dal dominio. È necessario fornire valori per `DOMAIN_ARN`, `TAG_KEY` e `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
```

Esecuzione di azioni amministrative sui domini Amazon OpenSearch Service

Amazon OpenSearch Service offre diverse opzioni amministrative che forniscono un controllo granulare se devi risolvere problemi con il tuo dominio. Queste opzioni includono la possibilità di riavviare il OpenSearch processo su un nodo di dati e la possibilità di riavviare un nodo di dati.

OpenSearch Il servizio monitora i parametri di integrità dei nodi e, in caso di anomalie, intraprende azioni correttive per mantenere stabili i domini. Con le opzioni amministrative per riavviare il OpenSearch processo su un nodo e riavviare un nodo stesso, hai il controllo su alcune di queste azioni di mitigazione.

È possibile utilizzare AWS Management Console AWS CLI, o l' AWS SDK per eseguire queste azioni. Le seguenti sezioni spiegano come eseguire queste azioni con la console.

Riavvia il OpenSearch processo su un nodo

Per riavviare il OpenSearch processo su un nodo

1. Accedi alla console OpenSearch di servizio all'indirizzohttps://console.aws.amazon.com/aos/.
2. Nel riquadro di navigazione a sinistra, scegli Domains (Domini). Scegli il nome del dominio con cui vuoi lavorare.
3. Dopo l'apertura della pagina dei dettagli del dominio, vai alla scheda Integrità dell'istanza.

4. In Nodi di dati, seleziona il pulsante accanto al nodo su cui desideri riavviare il processo.
5. Seleziona il menu a discesa Azioni e scegli Riavvia il processo OpenSearch /Elasticsearch.
6. Scegli Conferma nella modalità modale.
7. Per vedere lo stato dell'azione che hai avviato, seleziona il nome del nodo. Dopo l'apertura della pagina dei dettagli del nodo, scegli la scheda Eventi sotto il nome del nodo per visualizzare un elenco di eventi associati a quel nodo.

Riavvia un nodo di dati

Per riavviare un nodo di dati

1. Accedi alla console di OpenSearch servizio all'indirizzohttps://console.aws.amazon.com/aos/.
2. Nel riquadro di navigazione a sinistra, scegli Domains (Domini). Scegli il nome del dominio con cui vuoi lavorare.
3. Dopo l'apertura della pagina dei dettagli del dominio, vai alla scheda Integrità dell'istanza.
4. In Nodi di dati, seleziona il pulsante accanto al nodo su cui desideri riavviare il processo.
5. Seleziona il menu a discesa Azioni e scegli il nodo Riavvia.
6. Scegli Conferma nella modalità modale.
7. Per vedere lo stato dell'azione che hai avviato, seleziona il nome del nodo. Dopo l'apertura della pagina dei dettagli del nodo, scegli la scheda Eventi sotto il nome del nodo per visualizzare un elenco di eventi associati a quel nodo.

Riavvia la Dashboard o il processo Kibana su un nodo

Per riavviare la Dashboard o il processo Kibana su un nodo

1. Vai alla console di OpenSearch servizio all'indirizzo. https://console.aws.amazon.com/aos/
2. Nel riquadro di navigazione a sinistra, scegli Domains (Domini). Scegli il nome del dominio con cui vuoi lavorare.
3. Dopo l'apertura della pagina dei dettagli del dominio, vai alla scheda Integrità dell'istanza.
4. In Nodi di dati, seleziona il pulsante accanto al nodo su cui desideri riavviare il processo.
5. Seleziona il menu a discesa Azioni e scegli Riavvia il processo Dashboard/Kibana.
6. Scegli Conferma nella modalità modale.

7. Per vedere lo stato dell'azione che hai avviato, seleziona il nome del nodo. Dopo l'apertura della pagina dei dettagli del nodo, scegli la scheda Eventi sotto il nome del nodo per visualizzare un elenco di eventi associati a quel nodo.

Limitazioni

Le opzioni amministrative presentano le seguenti limitazioni:

- Le opzioni amministrative sono supportate nelle versioni 7.x e successive di Elasticsearch.
- Le opzioni amministrative non supportano i domini con Multi-AZ con Standby abilitato.
- Il OpenSearch riavvio del processo di Elasticsearch e il riavvio del nodo dati sono supportati nei domini con tre o più nodi di dati.
- Il supporto dei processi Dashboards e Kibana è supportato su domini con due o più nodi di dati.
- Per riavviare il OpenSearch processo su un nodo o riavviare un nodo, il dominio non deve essere in rosso e tutti gli indici devono avere delle repliche configurate.

Utilizzo delle query dirette OpenSearch di Amazon Service con Amazon S3

Puoi utilizzare le query dirette OpenSearch di Amazon Service per interrogare i dati in Amazon S3. Amazon OpenSearch Service offre un'integrazione diretta delle query con Amazon S3 per analizzare i log operativi in Amazon S3 e i data lake basati su Amazon S3 senza dover passare da un servizio all'altro. Ora puoi analizzare i dati negli archivi di oggetti cloud e utilizzare contemporaneamente le analisi operative e le visualizzazioni di Service. OpenSearch

Con le query dirette con Amazon S3, non è più necessario creare pipeline ETL complesse o sostenere le spese per la duplicazione dei dati sia nello storage Service che in Amazon S3. OpenSearch Puoi anche installare integrazioni di modelli di log più diffusi che includono dashboard predefiniti e configurare accelerazioni dei dati su misura per quel tipo di registro. I modelli includono log di flusso VPC, log e AWS CloudTrail log Amazon S3. Le accelerazioni includono indici che saltano, viste materializzate e indici coperti.

Argomenti

Prezzi

Paghi per le risorse esistenti di OpenSearch Service e Amazon S3 utilizzate per creare ed elaborare query dirette. Le query inviate ad Amazon S3 utilizzano elaborazione fatturabile e vengono visualizzate OpenSearch come unità di calcolo (OCU) all'ora.

Le query dirette con Amazon S3 sono di due tipi: interattive e con accelerazioni. Le query interattive eseguono analisi sui dati in Amazon S3. Quando esegui una nuova query, OpenSearch Service avvia una nuova sessione che dura almeno tre minuti. OpenSearch Il servizio mantiene attiva la sessione per garantire che le query successive vengano eseguite rapidamente. Le query di accelerazione utilizzano l'elaborazione per mantenere gli indici nel Servizio. OpenSearch Queste query in genere richiedono più tempo perché inseriscono una quantità variabile di dati nel OpenSearch Servizio per velocizzare l'esecuzione delle query interattive.

Per ulteriori informazioni, consulta la pagina dei prezzi OpenSearch di Amazon Service.

Limitazioni

Le seguenti limitazioni si applicano alle query OpenSearch Service Direct con Amazon S3.

- Il tuo OpenSearch dominio deve essere la versione 2.13 o successiva per supportare le query dirette di OpenSearch Service.
- Non disponibile su Serverless. OpenSearch
- Il tuo OpenSearch dominio AWS Glue Data Catalog deve appartenere allo stesso Account AWS. Il tuo bucket Amazon S3 può trovarsi in un account diverso (richiede l'aggiunta di una condizione alla tua policy IAM), ma deve appartenere allo Regione AWS stesso dominio.
- Alcuni tipi di dati non sono supportati. I tipi di dati supportati sono limitati a Parquet, CSV e JSON.
- OpenSearch Le query dirette al servizio con Amazon S3 supportano solo le tabelle Spark generate da Query Workbench. Le tabelle generate all'interno di AWS Glue Data Catalog o Athena non sono supportate dallo streaming Spark, necessario per mantenere le accelerazioni e mantenere aggiornati gli indici.
- I dati devono essere appiattiti prima dell'interrogazione oppure è necessario utilizzare SQL in OpenSearch Service per modificare le colonne annidate in colonne dedicate.
- Le colonne mancanti possono richiedere l'utilizzo della funzione `COALESCE` SQL per restituire i risultati.
- Se la struttura dei dati cambia, sono necessari aggiornamenti per la AWS Glue tabella e le accelerazioni esistenti.
- OpenSearch i tipi di istanza hanno limitazioni di payload in rete a seconda del tipo di istanza (10 v. 100).
- AWS CloudFormation i modelli non sono ancora supportati.

Raccomandazioni

Ti consigliamo di fare quanto segue quando usi la query diretta:

- Inserisci dati in Amazon S3 utilizzando i formati di partizione di anno, mese, giorno e ora per velocizzare le query.
- Usa dei limiti per le tue query per assicurarti di non recuperare troppi dati.
- Utilizza Index State Management (ove applicabile) per mantenere lo spazio di archiviazione per le viste materializzate e gli indici di copertura.
- Eliminate i job e gli indici di accelerazione quando non sono più necessari.
- Quando crei indici ignoranti, usa i filtri bloom per una cardinalità elevata e min/max per intervalli ampi. Si consiglia di utilizzare il valore impostato su un campo ad alta cardinalità.
- Utilizza le guide di riferimento per esportare i dati in Amazon S3. È possibile utilizzare AWS log come CloudFrontCloudTrail, ed Elastic Load Balancing.

Quote

Il tuo account ha le seguenti quote relative alle query OpenSearch Service Direct con Amazon S3. Ogni volta che avvii una query, OpenSearch Service apre una sessione e la mantiene attiva per almeno dieci minuti. Ciò riduce la latenza delle query rimuovendo il tempo di avvio della sessione nelle query successive.

Descrizione	Massimo	Può sovrascrivere
Connessioni per dominio	10	Sì
Fonti di dati per dominio	20	Sì
Indici per dominio	5	Sì
Sessioni simultanee per origine dati	10	Sì
Numero massimo di OCU per query	60	Sì

Descrizione	Massimo	Può sovrascrivere
Tempo massimo di esecuzione della query (minuti)	30	Sì
Numero massimo di OCU per accelerazione	20	Sì
Archiviazione effimera massima	20	Sì

Regioni supportate

Le seguenti regioni sono disponibili per le query dirette del OpenSearch servizio con Amazon S3: Asia Pacifico (Hong Kong), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Tokyo), Canada (Centrale), Europa (Francoforte), Europa (Irlanda), Europa (Stoccolma), Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio) e Stati Uniti Ovest (Oregon).

Creazione di integrazioni di sorgenti dati Amazon OpenSearch Service con Amazon S3

Puoi creare una nuova origine dati Amazon S3 a query diretta per OpenSearch Service tramite o l' AWS Management Console API. Ogni nuova fonte di dati utilizza AWS Glue Data Catalog per gestire le tabelle che rappresentano i bucket Amazon S3.

Argomenti

Prerequisiti

Prima di poter creare un'origine dati, devi disporre di un OpenSearch dominio con la versione 2.13 o successiva. Per istruzioni su come configurarlo, consultathe section called “ Creazione di domini OpenSearch di servizio”.

Configurare una nuova fonte di dati con interrogazione diretta

Puoi configurare un'origine dati con query diretta su un dominio con AWS Management Console o l'API di servizio. OpenSearch

AWS Management Console

1. Accedi alla console di Amazon OpenSearch Service all'indirizzohttps://console.aws.amazon.com/aos/.
2. Nel riquadro di navigazione a sinistra, scegli Domains (Domini).
3. Seleziona il dominio per cui desideri configurare una nuova fonte di dati. Si apre la pagina dei dettagli del dominio. Scegli la scheda Connessioni sotto i dettagli generali del dominio e trova la sezione Direct Query.
4. Scegli Crea.
5. Nella pagina di creazione dell'origine dati, inserisci un nome per la tua nuova fonte di dati. In Tipo di origine dati, scegli Amazon S3. Scegli un ruolo IAM esistente con limitazioni per ciò a cui è possibile accedere in Amazon S3. AWS Glue Data Catalog
6. Scegli Crea. Si apre la schermata dei dettagli dell'origine dati con un URL di OpenSearch Dashboards. Puoi accedere a questo URL per completare i passaggi successivi.

OpenSearch API di servizio

Usa l'operazione AddDataSourceAPI per creare una nuova fonte di dati nel tuo 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"
}
```

La seguente policy di esempio illustra le autorizzazioni con privilegi minimi necessarie per creare e gestire un'origine dati. Se disponi di autorizzazioni più ampie, ad esempio `s3:*` o la policy, queste autorizzazioni comprendono le autorizzazioni con il `AdminstratorAccess` privilegio minimo della politica di esempio.

L'integrazione richiede l'accesso per scrivere su Amazon S3 e. AWS Glue Data Catalog Per Amazon S3, abbiamo bisogno dell'accesso in scrittura per mantenere una posizione di controllo quando si generano accelerazioni. Infatti AWS Glue Data Catalog, abbiamo bisogno dell'accesso in scrittura per gestire database, tabelle e partizioni necessarie per l'integrazione dall'interno di Service. OpenSearch

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"HttpActionsForOpenSearchDomain",
         "Effect":"Allow",
         "Action":"es:ESHttp*",
         "Resource":"arn:aws:es:<region>:<account>:domain/<domain_name>/*"
      },
      {
         "Sid":"AmazonOpenSearchS3GlueDirectQueryReadAllS3Buckets",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:ListBucket"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"<account>"
            }
         },
         "Resource":"*"
      },
      {
         "Sid":"AmazonOpenSearchDirectQueryGlueCreateAccess",
         "Effect":"Allow",
         "Action":[
```

```
            "glue:CreateDatabase",
            "glue:CreatePartition",
            "glue:CreateTable",
            "glue:BatchCreatePartition"
         ],
         "Resource":"*"
      },
      {
         "Sid":"AmazonOpenSearchS3GlueDirectQueryModifyAllGlueResources",
         "Effect":"Allow",
         "Action":[
            "glue:DeleteDatabase",
            "glue:DeletePartition",
            "glue:DeleteTable",
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetPartition",
            "glue:GetPartitions",
            "glue:GetTable",
            "glue:GetTableVersions",
            "glue:GetTables",
            "glue:UpdateDatabase",
            "glue:UpdatePartition",
            "glue:UpdateTable",
            "glue:BatchGetPartition",
            "glue:BatchDeletePartition",
            "glue:BatchDeleteTable"
         ],
         "Resource":[
            "arn:aws:glue:us-east-1:<account>:table/*",
            "arn:aws:glue:us-east-1:<account>:database/*",
            "arn:aws:glue:us-east-1:<account>catalog"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"<account>"
            }
         }
      },
      {
         "Sid":"ReadAndWriteActionsForS3CheckpointBucket",
         "Effect":"Allow",
         "Action":[
            "s3:ListMultipartUploadParts",
```

```
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:PutObject",
            "s3:GetBucketLocation",
            "s3:ListBucket"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"<account>"
            }
         },
         "Resource":[
            "arn:aws:s3:::<checkpoint_bucket_name>",
            "arn:aws:s3:::<checkpoint_bucket_name>/*"
         ]
      }
   ]
}
```

Per supportare i bucket Amazon S3 in diversi account, dovrai includere una condizione nella policy di Amazon S3 e aggiungere l'account appropriato.

```
"Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
```

Il ruolo deve inoltre avere la seguente politica di fiducia, che specifica l'ID di destinazione.

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

Per istruzioni sulla creazione del ruolo, consulta Creazione di un ruolo utilizzando policy di attendibilità personalizzate.

Se hai abilitato il controllo granulare degli accessi in OpenSearch Service, verrà creato automaticamente un nuovo ruolo di controllo OpenSearch degli accessi granulare per la tua fonte di dati. Il nome del nuovo ruolo di controllo degli accessi a grana fine sarà. `AWSOpenSearchDirectQuery <name of data source>`

Per impostazione predefinita, il ruolo ha accesso solo agli indici delle origini dati delle query dirette. Sebbene sia possibile configurare il ruolo per limitare o concedere l'accesso all'origine dati, si consiglia di non modificare l'accesso di questo ruolo. Se elimini l'origine dati, questo ruolo verrà eliminato. Ciò rimuoverà l'accesso per tutti gli altri utenti se sono mappati al ruolo.

Mappa il AWS Glue Data Catalog ruolo (se il controllo granulare degli accessi è abilitato dopo aver creato l'origine dati)

Se hai abilitato il controllo granulare degli accessi dopo aver creato un'origine dati, devi mappare gli utenti non amministratori a un ruolo IAM con AWS Glue Data Catalog accesso per eseguire query dirette. Per creare manualmente un ruolo di backend da mappare al `glue_access` ruolo IAM, procedi nel seguente modo:

> **Note**
>
> Gli indici vengono utilizzati per qualsiasi interrogazione sulla fonte di dati. Un utente con accesso in lettura all'indice delle richieste per una determinata origine dati può leggere tutte le query relative a tale origine dati. Un utente con accesso in lettura all'indice dei risultati può leggere i risultati di tutte le query eseguite su quell'origine dati.

1. Dal menu principale di OpenSearch Dashboard, scegli Sicurezza, Ruoli e Crea ruoli.
2. Assegna un nome al ruolo glue_access.
3. Per le autorizzazioni del cluster, selezionaindices:data/write/bulk*,. `indices:data/read/scroll` `indices:data/read/scroll/clear`
4. Per Indice, inserisci i seguenti indici a cui desideri concedere all'utente con il ruolo l'accesso:
   - `.query_execution_request_<name of data source>`
   - `query_execution_result_<name of data source>`

- `flint_*`

5. Per le autorizzazioni di indicizzazione, seleziona. `indices_all`
6. Scegliere Create (Crea) .
7. Scegliere Utenti mappati, Gestisci mappatura.
8. In Ruoli di backend, aggiungi l'ARN del ruolo che richiede AWS Glue l'autorizzazione per chiamare il tuo dominio.

```
arn:aws:iam::account-id:role/role-name
```

9. Seleziona Mappa e conferma che il ruolo sia visualizzato in Utenti mappati.

Per ulteriori informazioni sulla mappatura dei ruoli, vedere. the section called “Mappatura dei ruoli agli utenti”

Passaggi successivi

Dopo aver creato un'origine dati, OpenSearch Service fornisce un URL per i OpenSearch dashboard. È possibile utilizzarlo per configurare il controllo degli accessi, definire tabelle, configurare dashboard basati sui tipi di log per i tipi di log più diffusi e interrogare i dati.

Configurazione di un'origine dati nei dashboard OpenSearch

Ora che hai creato la tua origine dati, puoi configurare le impostazioni di sicurezza, definire le tabelle Amazon S3 o configurare l'indicizzazione accelerata dei dati. Questa sezione illustra vari casi d'uso con la tua fonte di dati nelle OpenSearch dashboard prima di interrogare i dati.

Per configurare le seguenti sezioni, devi prima accedere alla tua origine dati in OpenSearch Dashboards. Nella barra di navigazione a sinistra, in Gestione, scegli Origini dati. In Gestisci fonti di dati, seleziona il nome dell'origine dati che hai creato nella console.

Configurazione del controllo degli accessi

Nella pagina dei dettagli della tua origine dati, trova la sezione Controlli di accesso e scegli Modifica. Se hai installato il plug-in di sicurezza, scegli Restricted e seleziona i gruppi basati sui ruoli a cui desideri fornire l'accesso alla nuova fonte di dati. Puoi anche scegliere Amministratore solo se desideri che solo l'amministratore abbia accesso all'origine dati.

> **Important**
>
> Gli indici vengono utilizzati per qualsiasi interrogazione sull'origine dati. Un utente con accesso in lettura all'indice delle richieste per una determinata origine dati può leggere tutte le query relative a tale origine dati. Un utente con accesso in lettura all'indice dei risultati può leggere i risultati di tutte le query eseguite su quell'origine dati.

Imposta le integrazioni per i tipi di log più diffusi AWS

OpenSearch Le dashboard consentono di iniziare rapidamente a utilizzare i tipi di log più comuni archiviati in Amazon S3 utilizzando log non elaborati, ad eccezione dei log di Amazon VPC Flow che sono supportati nel formato Parquet. OpenSearch Dashboards offre integrazioni che installano l'accesso a risorse come AWS Glue Data Catalog tabelle, query salvate e dashboard. Queste risorse sono alimentate da OpenSearch accelerazioni e si aggiorneranno automaticamente dopo l'installazione. Puoi configurare le integrazioni dalla pagina dei dettagli della fonte di dati o dalla barra di navigazione a sinistra. Per farlo:

1. Seleziona il tipo di registro che desideri installare. Assicurati che il tipo di log che installi abbia il tag Amazon S3.
2. Seleziona il tipo di connessione come connessione Amazon S3 se non è già selezionato.
3. Seleziona il nome dell'origine dati su cui desideri installare l'integrazione, la posizione Amazon S3 per i dati, il checkpoint che desideri utilizzare per mantenere lo stato di indicizzazione dell'accelerazione e gli asset desiderati in base al tuo caso d'uso.

> **Note**
>
> Durante la creazione del ruolo IAM, hai specificato una risorsa Amazon S3 per un checkpoint con autorizzazioni di azione di scrittura per la posizione del checkpoint. Dovrai fare riferimento a una posizione del bucket Amazon S3 con accesso in scrittura per la posizione del checkpoint. In caso contrario, le accelerazioni installate dall'integrazione falliranno.

> **Note**
>
> L'integrazione dei log di flusso di Amazon VPC richiede l'installazione di una patch tramite OpenSearch dashboard. Potrebbero essere necessari alcuni minuti per compilare i dashboard che hai installato.

Guide di riferimento per esportare dati in Amazon S3

Puoi utilizzare le seguenti guide di riferimento per esportare dati in Amazon S3:

Fonti:

- Apache Access
- CloudFront
- CloudTrail

- Elastic Load Balancing
- Amazon S3
- AWS WAF
- Flusso di Amazon VPC
- NGINX

Crea tabelle Spark utilizzando Query Workbench

Le query dirette dal OpenSearch Servizio ad Amazon S3 utilizzano le tabelle Spark all'interno di. AWS Glue Data Catalog Puoi creare tabelle dall'interno di Query Workbench senza dover uscire dai dashboard. OpenSearch

Per gestire database e tabelle esistenti nella tua fonte di dati o per creare nuove tabelle su cui desideri utilizzare le query dirette, seleziona Query Workbench dalla barra di navigazione a sinistra e seleziona l'origine dati Amazon S3 dal menu a discesa delle fonti di dati.

Per impostare una tabella per i log di flusso VPC archiviati in S3 in formato Parquet, esegui la seguente query:

```
CREATE TABLE
datasourcename.gluedatabasename.vpclogstable (version INT, account_id STRING,
 interface_id STRING,
srcaddr STRING, dstaddr STRING, srcport INT, dstport INT, protocol INT, packets
 BIGINT,
bytes BIGINT, start BIGINT, end BIGINT, action STRING, log_status STRING,
`aws-account-id` STRING, `aws-service` STRING, `aws-region` STRING, year STRING,
month STRING, day STRING, hour STRING)

USING parquet PARTITIONED BY (aws-account-id, aws-service, aws-region, year, month,
day, hour)

LOCATION "s3://accountnum-vpcflow/AWSLogs"
```

Dopo aver creato la tabella, esegui la seguente query per assicurarti che sia compatibile con le query dirette:

```
MSCK REPAIR TABLE  datasourcename.databasename.vpclogstable
```

Interrogazioni accelerate

Nella pagina dei dettagli dell'origine dati, scegli l'opzione Accelerate Performance. Per garantire un'esperienza rapida con i dati in Amazon S3, è possibile configurare tre diversi tipi di accelerazioni per indicizzare i dati nel OpenSearch servizio: gli indici saltati, le viste materializzate e gli indici di copertura.

Ignorare gli indici

Con un indice ignorante, puoi indicizzare solo i metadati dei dati archiviati in Amazon S3. Quando esegui una query su una tabella con un indice ignorante, il pianificatore di query fa riferimento all'indice e riscrive la query per localizzare i dati in modo efficiente, anziché scansionare tutte le partizioni e i file. Ciò consente all'indice di ignoramento di restringere rapidamente la posizione specifica dei dati archiviati.

Dalla pagina dei dettagli dell'origine dati, seleziona Accelera prestazioni, dove puoi iniziare selezionando il database e la tabella che desideri accelerare. In alternativa, puoi scegliere di generare automaticamente un indice di salto. Se preferisci aggiungere manualmente i campi da accelerare, puoi farlo selezionando il pulsante Aggiungi campi. Quando aggiungi i campi, ti verrà chiesto quale tipo di indice di omissione desideri aggiungere. Dovrai scegliere tra uno dei seguenti:

- Partizione: utilizza i dettagli della partizione dati per individuare i dati (ideale per colonne basate sul partizionamento come anno, mese, giorno, ora)
- MinMax: utilizza il limite inferiore e superiore della colonna indicizzata per individuare i dati (ideale per le colonne numeriche)
- ValueSet: utilizza un set di valori univoco per individuare i dati (ideale per le colonne con cardinalità bassa e moderata e che richiedono una corrispondenza esatta)
- BloomFilter: utilizza un filtro bloom per individuare i dati (ideale per le colonne con cardinalità elevata e che non richiedono una corrispondenza esatta)

È anche possibile creare manualmente un indice di salto sulla tabella utilizzando Query Workbench. Basta selezionare l'origine dati S3 dal menu a discesa delle fonti di dati e aggiungere la seguente query:

```
CREATE SKIPPING INDEX
ON datasourcename.gluedatabasename.vpclogstable(
 `srcaddr` BLOOM_FILTER,
 `dstaddr` BLOOM_FILTER,
 `day` PARTITION,
 `account_id`BLOOM_FILTER
 ) WITH (
index_settings = '{"number_of_shards":5,"number_of_replicas":1}',
auto_refresh = true,
checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint'
)
```

Viste materializzate

Con le viste materializzate, puoi utilizzare query complesse, come le aggregazioni, per potenziare le visualizzazioni della dashboard. Le viste materializzate inseriscono una piccola quantità di dati, a seconda della query, in Servicestorage. OpenSearch OpenSearch Service crea quindi un indice dai dati acquisiti che puoi utilizzare per le visualizzazioni. È possibile gestire l'indice delle viste materializzate conthe section called “Index State Management”, proprio come con qualsiasi altro indice. OpenSearch

Poiché specificherai un indice di destinazione, ti verrà chiesto di assegnare un nome all'indice e aggiungere il Watermark Delay, che definisce il ritardo con cui i dati possono arrivare ed essere comunque elaborati.

Utilizza la seguente query per creare una nuova vista materializzata per la tabella dei log di flusso VPC che hai creato in: the section called “Crea tabelle Spark utilizzando Query Workbench”

```
CREATE MATERIALIZED VIEW {table_name}__week_live_mview AS
  SELECT
    cloud.account_uid AS `aws.vpc.cloud_account_uid`,
    cloud.region AS `aws.vpc.cloud_region`,
    cloud.zone AS `aws.vpc.cloud_zone`,
    cloud.provider AS `aws.vpc.cloud_provider`,

    CAST(IFNULL(src_endpoint.port, 0) AS LONG) AS `aws.vpc.srcport`,
    CAST(IFNULL(src_endpoint.svc_name, 'Unknown') AS STRING)  AS `aws.vpc.pkt-src-aws-
service`,
    CAST(IFNULL(src_endpoint.ip, '0.0.0.0') AS STRING)  AS `aws.vpc.srcaddr`,
    CAST(IFNULL(src_endpoint.interface_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
interface_uid`,
    CAST(IFNULL(src_endpoint.vpc_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-vpc_uid`,
    CAST(IFNULL(src_endpoint.instance_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
instance_uid`,
    CAST(IFNULL(src_endpoint.subnet_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
subnet_uid`,

    CAST(IFNULL(dst_endpoint.port, 0) AS LONG) AS `aws.vpc.dstport`,
    CAST(IFNULL(dst_endpoint.svc_name, 'Unknown') AS STRING) AS `aws.vpc.pkt-dst-aws-
service`,
    CAST(IFNULL(dst_endpoint.ip, '0.0.0.0') AS STRING)  AS `aws.vpc.dstaddr`,
    CAST(IFNULL(dst_endpoint.interface_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
interface_uid`,
    CAST(IFNULL(dst_endpoint.vpc_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-vpc_uid`,
    CAST(IFNULL(dst_endpoint.instance_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
instance_uid`,
    CAST(IFNULL(dst_endpoint.subnet_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
subnet_uid`,
    CASE
      WHEN regexp(dst_endpoint.ip, '(10\\..*)|(192\\.168\\..*)|(172\\.1[6-9]\\..*)|
(172\\.2[0-9]\\..*)|(172\\.3[0-1]\\.*)')
        THEN 'ingress'
      ELSE 'egress'
      END AS `aws.vpc.flow-direction`,

    CAST(IFNULL(connection_info['protocol_num'], 0) AS INT) AS
 `aws.vpc.connection.protocol_num`,
```

```
    CAST(IFNULL(connection_info['tcp_flags'], '0') AS STRING)  AS
 `aws.vpc.connection.tcp_flags`,
    CAST(IFNULL(connection_info['protocol_ver'], '0') AS STRING)  AS
 `aws.vpc.connection.protocol_ver`,
    CAST(IFNULL(connection_info['boundary'], 'Unknown') AS STRING)  AS
 `aws.vpc.connection.boundary`,
    CAST(IFNULL(connection_info['direction'], 'Unknown') AS STRING)  AS
 `aws.vpc.connection.direction`,

    CAST(IFNULL(traffic.packets, 0) AS LONG) AS `aws.vpc.packets`,
    CAST(IFNULL(traffic.bytes, 0) AS LONG) AS `aws.vpc.bytes`,

    CAST(FROM_UNIXTIME(time / 1000) AS TIMESTAMP) AS `@timestamp`,
    CAST(FROM_UNIXTIME(start_time / 1000) AS TIMESTAMP) AS `start_time`,
    CAST(FROM_UNIXTIME(start_time / 1000) AS TIMESTAMP) AS `interval_start_time`,
    CAST(FROM_UNIXTIME(end_time / 1000) AS TIMESTAMP) AS `end_time`,
    status_code AS `aws.vpc.status_code`,

    severity AS `aws.vpc.severity`,
    class_name AS `aws.vpc.class_name`,
    category_name AS `aws.vpc.category_name`,
    activity_name AS `aws.vpc.activity_name`,
    disposition AS `aws.vpc.disposition`,
    type_name AS `aws.vpc.type_name`,

    region AS `aws.vpc.region`,
    accountid AS `aws.vpc.account-id`
  FROM
  datasourcename.gluedatabasename.vpclogstable
WITH (
  auto_refresh = true,
  refresh_interval = '15 Minute',
  checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint',
  watermark_delay = '1 Minute',
)
```

Indici di copertura

Con un indice di copertura, puoi inserire dati da una colonna specificata in una tabella. Si tratta del tipo di indicizzazione più performante tra i tre. Poiché OpenSearch Service acquisisce tutti i dati dalla colonna desiderata, si ottengono prestazioni migliori e si possono eseguire analisi avanzate.

Proprio come con le viste materializzate, OpenSearch Service crea un nuovo indice dai dati dell'indice di copertura. È possibile utilizzare questo nuovo indice per le visualizzazioni della dashboard e altre funzionalità del OpenSearch Servizio, come il rilevamento di anomalie o le funzionalità geospaziali. Puoi gestire l'indice della visualizzazione di copertura conthe section called "Index State Management", proprio come con qualsiasi altro indice. OpenSearch

Utilizza la seguente query per creare un nuovo indice di copertura per la tabella dei log di flusso VPC che hai creato in: the section called "Crea tabelle Spark utilizzando Query Workbench"

```
CREATE INDEX vpc_covering_index
ON datasourcename.gluedatabasename.vpclogstable (version, account_id, interface_id,
srcaddr, dstaddr, srcport, dstport, protocol, packets,
bytes, start, action, log_status STRING,
`aws-account-id`, `aws-service`, `aws-region`, year,
month, day, hour )
WITH (
  auto_refresh = true,
  refresh_interval = '15 minute',
  checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint'
)
```

Interrogazione dei dati nei dashboard OpenSearch

Dopo aver impostato le tabelle e configurato l'accelerazione delle query opzionale desiderata, ora puoi iniziare a eseguire analisi sui tuoi dati. Per interrogare i dati, seleziona la fonte di dati dal menu a discesa nella pagina Scopri o nella pagina Osservabilità nelle dashboard. OpenSearch

Se utilizzi un indice ignorante o non hai creato un indice, puoi utilizzare SQL o Piped Processing Language (PPL) per interrogare i dati. Se hai configurato una vista materializzata o un indice di copertura, disponi già di un indice e puoi utilizzare Dashboards Query Language (DQL) in tutte le dashboard. Puoi anche usare PPL con il plug-in Observability e SQL con il plug-in Query Workbench. Attualmente, solo i plugin Observability e Query Workbench supportano PPL e SQL. Per interrogare i dati utilizzando l'API di OpenSearch servizio, consulta la documentazione relativa all'API asincrona.

SQL

Utilizza la seguente query per eseguire una query SQL di esempio per la tabella dei log di flusso VPC che hai creato in: the section called "Crea tabelle Spark utilizzando Query Workbench"

```
SELECT srcaddr, SUM (CAST(bytes AS LONG)) as total_bytes
 FROM datasourcename.gluedatabasename.vpclogstable GROUP BY srcaddrORDER BY total_bytes
 DESCLIMIT 10;
```

PPL

Utilizza le seguenti query per eseguire query PPL di esempio per la tabella di log VPC che hai creato in: the section called “Crea tabelle Spark utilizzando Query Workbench”

```
source = datasourcename.gluedatabasename.vpclogstable | fields account_id, srcaddr,
 dstaddr, action | head 10
```

Raccomandazioni

In alcuni casi i risultati non vengono restituiti come previsto. In caso di problemi, ti consigliamo di intraprendere le seguenti azioni:

- `SELECT*` le istruzioni non restituiscono risultati: controlla la tabella per vedere se contiene colonne struc annidate che devono essere esplose.
- Quando selezionate più tabelle, utilizzate l'`SQL UNIO`Nistruzione per fare riferimento a più tabelle.
- Le accelerazioni sono impostate per utilizzare un numero specifico di lavoratori per eseguire una query. Se le query vengono restituite lentamente, è possibile assegnare manualmente più lavoratori per eseguire le query per aumentare le prestazioni.
- Durante la creazione di indici ignoranti, utilizza i filtri bloom per una cardinalità elevata e min/max per intervalli ampi per risparmiare spazio sul dominio. Si consiglia di impostare il valore su un campo a cardinalità moderata se è necessario eseguire una corrispondenza esatta.
- Per ulteriori informazioni sulle query SQL più comuni, vedere AWS Service Logs.

Gestione di una fonte di dati

La gestione dell'origine dati è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle fonti di dati con query dirette e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti per monitorare, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario.

Argomenti

- Monitoraggio con CloudWatch fonti di dati metriche

- Abilitazione e disabilitazione delle fonti di dati
- Monitoraggio con budget AWS
- Eliminazione di un'origine dati Amazon OpenSearch Service con Amazon S3

Monitoraggio con CloudWatch fonti di dati metriche

È possibile monitorare le interrogazioni dirette utilizzando CloudWatch. CloudWatch raccoglie dati grezzi e li elabora in metriche leggibili e quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web.

Puoi anche impostare allarmi per monitorare determinate soglie e inviare notifiche o intraprendere azioni quando tali soglie vengono raggiunte. Per ulteriori informazioni, consulta What is Amazon CloudWatch.

Direct Query riporta le seguenti metriche:

Parametro	Descrizione
AsyncQueryCreateAPI	Il numero totale di richieste inviate all'API per la creazione di query asincrone. Statistiche pertinenti: Media, massimo, somma Dimensioni:`ClientId`, `DomainName` Frequenza: 60 secondi
AsyncQueryGetApiRequestCount	Il numero totale di richieste inviate all'API per il recupero dei risultati delle query asincrone. Statistiche pertinenti: Media, massimo, somma Dimensioni:`ClientId`, `DomainName` Frequenza: 60 secondi

Parametro	Descrizione
AsyncQueryCancelApiRequestCount	Il numero totale di richieste inviate all'API per l'annullamento delle query asincrone. Statistiche pertinenti: Media, massimo, somma Dimensioni:`ClientId`, `DomainName` Frequenza: 60 secondi
A syncQueryGet ApiFailed RequestCusErrCount	Il numero di richieste non riuscite durante il recupero dei risultati delle query asincrone a causa di errori relativi al cliente (ad esempio, ID di query non valido). Statistiche pertinenti: Media, massimo, somma Dimensioni:`ClientId`, `DomainName` Frequenza: 60 secondi
AsyncQueryCancelApiFailedRequestCusErrCount	Il numero di richieste non riuscite durante il recupero dei risultati delle query asincrone a causa di errori relativi al cliente (ad esempio, ID di query non valido). Statistiche pertinenti: media, massima, somma Dimensioni:`ClientId`, `DomainName` Frequenza: 60 secondi

Parametro	Descrizione
AsyncQueryCancelApiFailedRequestSysErrCount	Il numero di richieste non riuscite durante la creazione di query asincrone a causa di errori relativi al cliente. Statistiche rilevanti: Average (Media), Maximum (Massimo), Sum (Somma) Dimensioni:, `ClientId` `DomainName` Frequenza: 60 secondi
A syncQueryGet ApiFailed RequestSysErrCount	Il numero di richieste non riuscite durante il recupero dei risultati delle query asincrone a causa di errori relativi al sistema. Statistiche rilevanti: Average (Media), Maximum (Massimo), Sum (Somma) Dimensioni:, `ClientId` `DomainName` Frequenza: 60 secondi

Abilitazione e disabilitazione delle fonti di dati

Nei casi in cui desideri interrompere l'utilizzo diretto delle query per un'origine dati, puoi scegliere di disabilitare l'origine dati. La disabilitazione di un'origine dati terminerà l'esecuzione delle query esistenti e interromperà l'esecuzione di tutte le nuove query da parte dell'utente.

La configurazione delle accelerazioni per migliorare le prestazioni delle query, ad esempio saltare gli indici, le viste materializzate e l'indice di copertura, verrà impostata su manuale una volta disattivata l'origine dati. Una volta che un'origine dati è impostata come attiva dopo essere stata disabilitata, le query degli utenti verranno eseguite come previsto. Le accelerazioni precedentemente configurate e impostate come manuali dovranno essere configurate manualmente per essere nuovamente eseguite secondo una pianificazione.

Monitoraggio con budget AWS

Amazon OpenSearch Service sta inserendo i dati sull'utilizzo dell'OCU a livello di account nel Cost Explorer di Billing and Cost Management. I clienti possono tenere conto dell'utilizzo dell'OCU a livello di account e impostare soglie e avvisi quando le soglie vengono superate.

Il formato del tipo di utilizzo su cui filtrare in Cost Explorer è simile a RegionCode: DirectQuery OCU (OCU-Hours). I clienti che desiderano essere avvisati quando l'utilizzo di DirectQuery OCU (OCU-Hours) raggiunge la soglia, possono creare un account AWS Budgets e configurare un avviso in base alla soglia impostata. Facoltativamente, i clienti possono scegliere di impostare un argomento Amazon SNS, che disattiverà un'origine dati nel caso in cui venga soddisfatto un criterio di soglia.

> **Note**
>
> I dati di utilizzo in AWS Budgets non sono in tempo reale e possono subire ritardi fino a 8 ore.

Eliminazione di un'origine dati Amazon OpenSearch Service con Amazon S3

Quando elimini un'origine dati, Amazon OpenSearch Service la rimuove dal tuo dominio. OpenSearch Il servizio rimuove anche gli indici associati all'origine dati. I tuoi dati transazionali non vengono eliminati da Amazon S3, ma Amazon S3 non invia nuovi dati a Service. OpenSearch

Puoi eliminare l'integrazione di un'origine dati utilizzando l'API AWS Management Console o il Service. OpenSearch

AWS Management Console

Per eliminare un'origine dati

1. Accedi alla console di Amazon OpenSearch Service all'indirizzohttps://console.aws.amazon.com/aos/.
2. Dal riquadro di navigazione a sinistra, scegli Domini.
3. Seleziona il dominio per il quale desideri eliminare un'origine dati. Si apre la pagina dei dettagli del dominio. Scegli la scheda Connessioni sotto le informazioni generali e trova la sezione Direct Query.
4. Seleziona l'origine dati che desideri eliminare, scegli Elimina e conferma l'eliminazione.

OpenSearch API di servizio

Utilizza l'operazione DeleteDataSourceAPI per eliminare un'origine dati esistente nel tuo dominio.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource/data-source-name
```

Monaggio Amazon OpenSearch Service

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di Amazon OpenSearch Service e delle altre AWS soluzioni. AWSfornisce i seguenti strumenti di monitoraggio per controllare le risorse OpenSearch del servizio, segnalare eventuali problemi ed eseguire operazioni automatiche quando appropriato:

Amazon CloudWatch

Amazon CloudWatch monitora le risorse OpenSearch del servizio in tempo reale. È possibile raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi che inviino una notifica o intraprendano azioni quando un parametro specificato raggiunge una determinata soglia. Per ulteriori informazioni, consulta la Guida per CloudWatch l'utente di Amazon.

CloudWatchRegistri Amazon

Amazon CloudWatch Logs consente di monitorare, archiviare e accedere ai file di OpenSearch log. CloudWatchLogs è in grado di monitorare le informazioni nei file di log e notificare quando vengono raggiunte determinate soglie. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon CloudWatch Logs.

Amazon EventBridge

Amazon EventBridge fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono le modifiche apportate ai OpenSearch domini Amazon. È possibile creare le regole che controllano determinati eventi e attivano operazioni automatiche in altri servizi AWS quando questi eventi si verificano. Per ulteriori informazioni, consulta la Guida per EventBridge l'utente di Amazon.

AWS CloudTrail

AWS CloudTrailacquisisce le chiamate all'API di configurazione effettuate a OpenSearch Service come eventi. Può distribuire questi eventi a un bucket Amazon S3 specificato. Con queste informazioni, è possibile identificare quali utenti e account hanno effettuato richieste, l'indirizzo IP di origine da cui sono state effettuate le richieste e quando sono avvenute. Per ulteriori informazioni, consulta la AWSCloudTrailGuida per l'utente di .

Argomenti

- Monitoraggio dei OpenSearch log con Amazon CloudWatch Logs
- Monitoraggio dei log di controllo in Amazon Service OpenSearch
- Monitoraggio degli eventi del OpenSearch servizio con Amazon EventBridge
- Monaggio delle chiamate API Amazon OpenSearch Service con AWS CloudTrail

Monitoraggio delle metriche dei OpenSearch cluster con Amazon CloudWatch

Amazon OpenSearch Service pubblica i dati dei tuoi domini su Amazon. CloudWatch CloudWatch ti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. OpenSearch Il servizio invia la maggior parte delle metriche a CloudWatch intervalli di 60 secondi. Se utilizzi volumi magnetici EBS o per uso generale, i parametri relativi al volume EBS si aggiorneranno ogni cinque minuti. Tutte le metriche cumulative (ad esempio`ThreadpoolSearchRejected`) sono in memoria e `ThreadpoolWriteRejeceted` perderanno lo stato. Le metriche verranno reimpostate durante la caduta di un nodo, il rimbalzo del nodo, la sostituzione del nodo e la distribuzione blu/verde. Per ulteriori informazioni su Amazon CloudWatch, consulta la Amazon CloudWatch User Guide.

La console OpenSearch di servizio mostra una serie di grafici basati sui dati grezzi di CloudWatch. A seconda delle esigenze, potresti preferire visualizzare i dati del cluster CloudWatch anziché i grafici nella console. Il servizio archivia i parametri per due settimane prima di eliminarli. Le metriche vengono fornite senza costi aggiuntivi, ma sono CloudWatch comunque a pagamento per la creazione di dashboard e allarmi. Per ulteriori informazioni, consulta i CloudWatchprezzi di Amazon.

OpenSearch Il servizio pubblica le seguenti metriche su: CloudWatch

- the section called “Parametri cluster”
- the section called “Parametri nodo master dedicato”
- the section called “Parametri volume EBS”
- the section called “Parametri dell'istanza”
- the section called “UltraWarm metriche”
- the section called “Parametri di archiviazione a freddo”
- the section called “Parametri di avvisi”
- the section called “Parametri di rilevamento delle anomalie”

- the section called “Parametri di ricerca asincrona”
- the section called “Parametri SQL”
- the section called “Parametri k-NN”
- the section called “Parametri di ricerca tra cluster”
- the section called “Parametri di replica tra cluster”
- the section called “Parametri di Learning to Rank”
- the section called “Parametri Piped Processing Language (PPL)”

Visualizzazione delle metriche in CloudWatch

CloudWatch le metriche vengono raggruppate prima in base allo spazio dei nomi del servizio e quindi in base alle varie combinazioni di dimensioni all'interno di ogni spazio dei nomi.

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione a sinistra, scegli Metrics (Parametri), quindi scegli All metrics (Tutti i parametri). Seleziona lo spazio dei OpenSearchService nomi ES/.
3. Scegliere una dimensione per visualizzare i parametri corrispondenti. I parametri per i singoli nodi si trovano nella dimensione `ClientId, DomainName, NodeId`. I parametri del cluster si trovano nella dimensione `Per-Domain, Per-Client Metrics`. Alcuni parametri dei nodi vengono aggregati a livello di cluster e quindi inclusi in entrambe le dimensioni. I parametri delle partizioni si trovano nella dimensione `ClientId, DomainName, NodeId, ShardRole`.

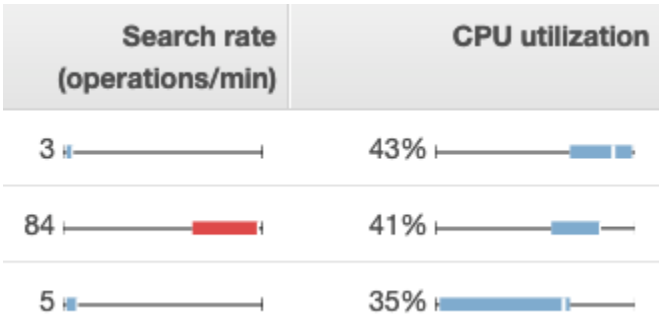
Per visualizzare un elenco di metriche utilizzando il AWS CLI

Esegui il comando seguente:

```
aws cloudwatch list-metrics --namespace "AWS/ES"
```

Interpretazione delle cartelle cliniche in Service OpenSearch

Per visualizzare le metriche in OpenSearch Service, utilizza le schede Cluster Health e Instance Health. La scheda Instance Health utilizza diagrammi a riquadri per fornire at-a-glance visibilità sullo stato di ogni OpenSearch nodo:



- Ogni casella colorata mostra l'intervallo di valori per il nodo nel periodo di tempo specificato.
- Le caselle blu rappresentano i valori che sono compatibili con gli altri nodi. Le caselle rosse rappresentano i valori erratici.
- La linea bianca all'interno di ogni casella mostra il valore corrente del nodo.
- Le "parentesi angolari" su entrambi i lati di ciascuna casella mostrano i valori minimo e massimo per tutti i nodi nel periodo di tempo.

Se si apportano modifiche alla configurazione del dominio, l'elenco delle singole istanze nelle schede Cluster health (Stato cluster) e Instance health (Stato istanza) raddoppierà spesso in dimensione per un breve periodo prima di tornare al numero corretto. Per una spiegazione del comportamento, consulta the section called “Modifiche di configurazione”.

Parametri cluster

Amazon OpenSearch Service fornisce le seguenti metriche per i cluster.

Parametro	Descrizione
`ClusterStatus.green`	Un valore pari a 1 indica che tutte le partizioni di indice sono assegnate a nodi nel cluster. Statistiche rilevanti: Massima
`ClusterStatus.yellow`	Un valore pari a 1 indica che le partizioni principali per tutti gli indici sono allocate a nodi nel cluster, ma che le partizioni di replica per almeno un indice non lo sono. Per ulteriori informazioni, consulta the section called “Stato giallo del cluster”. Statistiche rilevanti: Massima

Parametro	Descrizione
`ClusterStatus.red`	Un valore pari a 1 indica che le partizioni primarie e di replica di almeno un indice non sono allocate ai nodi nel cluster. Per ulteriori informazioni, consultare the section called “Cluster in stato rosso”. Statistiche rilevanti: Massima
`Shards.active`	Il numero totale di partizioni primarie e di replica attive. Statistiche rilevanti: Massima, Somma
`Shards.unassigned`	Il numero di partizioni non allocate ai nodi nel cluster. Statistiche rilevanti: Massima, Somma
`Shards.delayedUnassigned`	Il numero di partizioni la cui allocazione dei nodi è stata ritardata dalle impostazioni di timeout. Statistiche rilevanti: Massima, Somma
`Shards.activePrimary`	Il numero di partizioni primarie attive. Statistiche rilevanti: Massima, Somma
`Shards.initializing`	Il numero di partizioni in fase di inizializzazione. Statistiche rilevanti: Sum (Somma)
`Shards.relocating`	Il numero di partizioni in fase di rilocazione. Statistiche rilevanti: Sum (Somma)
`Nodes`	Il numero di nodi nel cluster di OpenSearch servizio, inclusi nodi master e UltraWarm nodi dedicati. Per ulteriori informazioni, consulta the section called “Modifiche di configurazione”. Statistiche rilevanti: Massima

Parametro	Descrizione
`SearchableDocuments`	Il numero totale di documenti disponibili per la ricerca tra tutti i nodi di dati nel cluster. Statistiche rilevanti: Minima, Massima, Media
`DeletedDocuments`	Il numero totale di documenti contrassegnati per l'eliminazione tra tutti i nodi di dati nel cluster. Questi documenti non vengono più visualizzati nei risultati di ricerca, ma rimuovono dal disco OpenSearch solo i documenti eliminati durante l'unione dei segmenti. Questo parametro aumenta dopo le richieste di eliminazione e diminuisce dopo la fusione dei segmenti. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`CPUUtilization`	Percentuale di utilizzo della CPU per i nodi di dati nel cluster. Il numero massimo mostra il nodo con il più alto utilizzo della CPU. La media rappresenta tutti i nodi del cluster. Questo parametro è disponibile anche per singoli nodi. Statistiche rilevanti: Maximum (Massimo), Average (Media)

Parametro	Descrizione
`FreeStorageSpace`	Lo spazio libero per i nodi di dati nel cluster. `Sum` mostra lo spazio libero totale per il cluster, ma è necessario lasciare il periodo a un minuto per ottenere un valore accurato. `Minimum` e `Maximum` mostrano i nodi con lo spazio libero maggiore e minore, rispettiv amente. Questa metrica è disponibile anche per i singoli nodi. OpenSearch Il servizio genera un `ClusterBlockException` quando questa metrica raggiunge. `0` Per risolvere il problema devi eliminare gli indici, aggiungere istanze più grandi oppure aggiunger e archiviazione basata su EBS alle istanze esistenti. Per ulteriori informazioni, consulta the section called “Mancanza di spazio di archiviazione disponibile”. La console OpenSearch di servizio visualizza questo valore in GiB. La CloudWatch console Amazon lo visualizza in MiB. **Note** `FreeStorageSpace` sarà sempre inferiore ai valori forniti dalle `_cat/allocation` API OpenSearch `_cluster/stats` e. OpenSearch Il servizio riserva una percentua le dello spazio di archiviazione su ogni istanza per le operazioni interne. Per ulteriori informazioni, consultare Calcolo dei requisiti di archiviazione. Statistiche rilevanti: Minimum (Minimo), Maximum (Massimo), Average (Media), Sum (Somma)
`ClusterUsedSpace`	Lo spazio totale utilizzato per il cluster. È necessario lasciare il periodo su un minuto per ottenere un valore preciso. La console OpenSearch di servizio visualizza questo valore in GiB. La CloudWatch console Amazon lo visualizza in MiB. Statistiche rilevanti: Minimum (Minimo), Maximum (Massimo)

Parametro	Descrizione
`ClusterIndexWritesBlocked`	Indica se il cluster accetta o blocca le richieste di scrittura in entrata. Un valore pari a 0 significa che il cluster accetta le richieste . Un valore pari a 1 significa che il cluster blocca le richieste. Alcuni fattori comuni sono i seguenti: `FreeStorageSpace` è troppo basso oppure `JVMMemoryPressure` è troppo alto. Per contenere questo problema, puoi decidere di aggiungere altro spazio su disco oppure di dimensionare il tuo cluster. Statistiche rilevanti: Massima
`JVMMemoryPressure`	La percentuale massima dell'heap Java utilizzata per tutti i nodi di dati del cluster. OpenSearch Il servizio utilizza metà della RAM di un'istanza per l'heap Java, fino a una dimensione dell'heap di 32 GiB. Puoi scalare le istanze verticalmente fino a 64 GiB di RAM e poi scalare orizzontalmente aggiungendo le istanze. Per informazi oni, consulta the section called “Allarmi consigliati CloudWatch ”. Statistiche rilevanti: Massima **Note** La logica di questo parametro è cambiata nel software del servizio R20220323. Per ulteriori informazioni, consulta le note di rilascio.
`OldGenJVMMemoryPressure`	La percentuale massima dell'heap Java utilizzata per la "vecchia generazione" di tutti i nodi di dati nel cluster. Questo parametro è disponibile anche a livello di nodo. Statistiche rilevanti: Massima

Parametro	Descrizione
`AutomatedSnapshotFailure`	Il numero di snapshot automatici non riusciti per il cluster. Un valore pari a 1 indica che non è stato acquisito alcuno snapshot automatico per il dominio nelle 36 ore precedenti. Statistiche rilevanti: Minimum (Minimo), Maximum (Massimo)
`CPUCreditBalance`	I crediti CPU rimanenti disponibili per i nodi di dati nel cluster. Un credito CPU fornisce le prestazioni di un core CPU completo per un minuto. Per ulteriori informazioni, consultare Crediti CPU nella Guida per gli sviluppatori di Amazon EC2. Questo parametro è disponibile solo per i tipi di istanza T2. Statistiche rilevanti: Minimum (Minimo)
`OpenSearchDashboardsHealthyNodes`	Un controllo dello stato di salute per Dashboards. OpenSearch Se il valore minimo, massimo e medio sono tutti uguali a 1, Dashboards si comporta normalmente. Se si dispone di 10 nodi con un massimo di 1, minimo di 0 e media di 0,7, allora significa che 7 nodi (70%) sono integri e 3 nodi (30%) non lo sono. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`OpensearchDashboardsReportingFailedRequestSysErrCount`	Il numero di richieste di generazione di report di OpenSearch Dashboard che non sono riuscite a causa di problemi del server o limitazioni delle funzionalità. Statistiche rilevanti: Sum (Somma)
`OpensearchDashboardsReportingFailedRequestUserErrCount`	Il numero di richieste di generazione di report di OpenSearch Dashboards che non sono riuscite a causa di problemi del client. Statistiche rilevanti: Sum (Somma)

Parametro	Descrizione
`OpensearchDashboardsReportingRequestCount`	Il numero totale di richieste per generare OpenSearch report Dashboards. Statistiche rilevanti: Sum (Somma)
`OpensearchDashboardsReportingSuccessCount`	Il numero di richieste riuscite per generare OpenSearch report Dashboards. Statistiche rilevanti: Sum (Somma)
`KMSKeyError`	Il valore 1 indica che la AWS KMS chiave utilizzata per crittogra fare i dati inattivi è stata disabilitata. Per ripristinare il dominio sulle operazioni normali, riabilita la chiave. La console visualizza questo parametro solo per i domini che crittografano i dati a riposo. Statistiche rilevanti: Minimum (Minimo), Maximum (Massimo)
`KMSKeyInaccessible`	Il valore 1 indica che la AWS KMS chiave utilizzata per crittografare i dati inattivi è stata eliminata o le relative concessioni al Servizio sono state revocate. OpenSearch Non è possibile recuperare i domini che sono in questo stato. Se hai una snapshot manuale, puoi utilizzarla per migrare i dati del dominio in un nuovo dominio. La console visualizza questo parametro solo per i domini che crittografano i dati a riposo. Statistiche rilevanti: Minimum (Minimo), Maximum (Massimo)

Parametro	Descrizione
`InvalidHostHeaderRequests`	Il numero di richieste HTTP effettuate al OpenSearch cluster che includevano un'intestazione host non valida (o mancante). Le richieste valide includono il nome host del dominio come valore dell'intestazione dell'host. OpenSearch Il servizio rifiuta le richieste non valide per i domini di accesso pubblico che non dispongono di una politica di accesso restrittiva. Si consiglia di applicare una policy di accesso restrittiva a tutti i domini. Se vedi valori elevati per questa metrica, conferma che i tuoi OpenSearch clienti includano il nome host del dominio (e non, ad esempio, il relativo indirizzo IP) nelle loro richieste. Statistiche rilevanti: Sum (Somma)
`OpenSearchRequests (previously ElasticsearchRequests)`	Il numero di richieste effettuate al OpenSearch cluster. Statistiche rilevanti: Sum (Somma)
`2xx, 3xx, 4xx, 5xx`	Il numero di richieste al dominio che hanno prodotto il codice di risposta HTTP specificato (2xx, 3xx, 4xx, 5xx). Statistiche rilevanti: Sum (Somma)

Parametro	Descrizione
`ThroughputThrottle`	Indica se i dischi sono stati limitati o meno. La limitazione si verifica quando la velocità effettiva combinata di `ReadThroughputMicroBursting` e `WriteThroughputMicroBursting` è superiore alla velocità massima,. `MaxProvisionedThroughput` `MaxProvisionedThroughput` è il valore più basso del throughput dell'istanza o del throughput di volume assegnato. Il valore 1 indica che i dischi sono stati limitati. Un valore 0 indica un comportamento normale. Per informazioni sulla velocità effettiva delle istanze, consulta Amazon EBS: istanze ottimizzate. Per informazioni sulla velocità effettiva dei volumi, consulta i tipi di volume di Amazon EBS. Statistiche rilevanti: Minimum (Minimo), Maximum (Massimo)
`IopsThrottle`	Indica se il numero di operazioni di input/output al secondo (IOPS) sul dominio è stato limitato o meno. La limitazione si verifica quando gli IOPS del nodo dati superano il limite massimo consentito o del volume EBS o dell'istanza EC2 del nodo dati. Per informazioni sugli IOPS delle istanze, consulta Amazon EBS: istanze ottimizzate. Per informazioni sugli IOPS di volume, consulta i tipi di volume di Amazon EBS. Statistiche rilevanti: Minimum (Minimo), Maximum (Massimo)

Parametri nodo master dedicato

Amazon OpenSearch Service fornisce le seguenti metriche per i nodi master dedicati.

Parametro	Descrizione
`MasterCPUUtilization`	La percentuale massima di risorse della CPU utilizzate dai nodi master dedicati. È consigliato aumentare le dimensioni del tipo di istanza quando questo parametro raggiunge 60%.

Parametro	Descrizione
	Statistiche rilevanti: Massima
`MasterFreeStorageSpace`	Questo parametro non è rilevante e può essere ignorato. Il servizio non utilizza i nodi master come nodi di dati.
`MasterJVMMemoryPressure`	La percentuale massima dell'heap di Java utilizzata per tutti i nodi master dedicati nel cluster. È consigliato passare a un tipo di istanza più grande quando questo parametro raggiunge 85%. Statistiche rilevanti: Massima **Note** La logica di questo parametro è cambiata nel software del servizio R20220323. Per ulteriori informazioni, consulta le note di rilascio.
`MasterOldGenJVMMemoryPressure`	La percentuale massima dell'heap Java utilizzata per la "vecchia generazione" per ciascun nodo principale. Statistiche rilevanti: Massima
`MasterCPUCreditBalance`	I crediti CPU rimanenti disponibili per i nodi master dedicati nel cluster. Un credito CPU fornisce le prestazioni di un core CPU completo per un minuto. Per ulteriori informazioni, consultare Crediti CPU nella Guida per gli sviluppatori di Amazon EC2. Questo parametro è disponibile solo per i tipi di istanza T2. Statistiche rilevanti: Minimum (Minimo)

Parametro	Descrizione
`MasterReachableFromNode`	Un controllo dello stato per le eccezioni `MasterNotDiscovered` . Un valore pari a 1 indica un comportamento normale. Un valore di pari a indica che `/_cluster/health/` ha avuto esito negativo. Gli errori indicano che il nodo master non è raggiungibile dal nodo di origine. Di solito sono il risultato di un problema di connettività di rete o di un AWS problema di dipendenza. Statistiche rilevanti: Massima
`MasterSysMemoryUtilization`	La percentuale di memoria del nodo master utilizzata. Statistiche rilevanti: Massima

Parametri volume EBS

Amazon OpenSearch Service fornisce le seguenti metriche per i volumi EBS.

Parametro	Descrizione
`ReadLatency`	La latenza, in secondi, per le operazioni di lettura sui volumi di EBS. Questo parametro è disponibile anche per singoli nodi. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`WriteLatency`	La latenza, in secondi, per le operazioni di scrittura sui volumi di EBS. Questo parametro è disponibile anche per singoli nodi. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`ReadThroughput`	Il throughput, in byte al secondo, per le operazioni di lettura sui volumi di EBS. Questo parametro è disponibile anche per singoli nodi.

Parametro	Descrizione
	Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`ReadThroughputMicroBursting`	Il throughput, in byte al secondo, per le operazioni di lettura sui volumi EBS quando si prende in considerazione il microbursting. Questo parametro è disponibile anche per singoli nodi. Il microbursting si verifica quando un volume EBS raggiunge livelli elevati di IOPS o di throughput per periodi di tempo significativamente più brevi (meno di un minuto). Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`WriteThroughput`	Il throughput, in byte al secondo, per le operazioni di scrittura sui volumi di EBS. Questo parametro è disponibile anche per singoli nodi. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`WriteThroughputMicroBursting`	La velocità effettiva, in byte al secondo, per le operazioni di scrittura su volumi EBS quando si prende in considerazione il microbursting. Questo parametro è disponibile anche per singoli nodi. Il microbursting si verifica quando un volume EBS raggiunge livelli elevati di IOPS o di throughput per periodi di tempo significativamente più brevi (meno di un minuto). Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`DiskQueueDepth`	Il numero di richieste di I/O in sospeso per un volume di EBS. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`ReadIOPS`	Il numero di operazioni I/O al secondo per le operazioni di lettura sui volumi di EBS. Questo parametro è disponibile anche per singoli nodi. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)

Parametro	Descrizione
`ReadIOPSMicroBursting`	Il numero di operazioni di input e output (I/O) al secondo per le operazioni di lettura sui volumi EBS quando si prende in considerazione il microbursting. Questo parametro è disponibile anche per singoli nodi. Il microbursting si verifica quando un volume EBS raggiunge livelli elevati di IOPS o di throughput per periodi di tempo significativamente più brevi (meno di un minuto). Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`WriteIOPS`	Il numero di operazioni I/O al secondo per le operazioni di scrittura sui volumi di EBS. Questo parametro è disponibile anche per singoli nodi. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`WriteIOPS MicroBursting`	Il numero di operazioni di input e output (I/O) al secondo per le operazioni di scrittura su volumi EBS quando si prende in considerazione il microbursting. Questo parametro è disponibile anche per singoli nodi. Il microbursting si verifica quando un volume EBS raggiunge livelli elevati di IOPS o di throughput per periodi di tempo significativamente più brevi (meno di un minuto). Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)
`BurstBalance`	La percentuale di crediti di input e output (I/O) che rimangono nel bucket burst per un volume EBS. Un valore pari a 100 indica che il volume ha accumulato il numero massimo di crediti. Se questa percentuale scende al di sotto del 70%, consulta the section called “Saldo di burst EBS basso”. Il saldo di espansione rimane a 0 per i domini con tipi di volumi gp3 e i domini con volumi gp2 con una dimensione del volume superiore a 1.000 GiB. Statistiche rilevanti: Minimum, Maximum, Average (Minimo, Massimo, Medio)

Parametri dell'istanza

Amazon OpenSearch Service fornisce le seguenti metriche per ogni istanza in un dominio. OpenSearch Il servizio aggrega inoltre questi parametri delle istanze per fornire informazioni sullo stato generale del cluster. È possibile verificare questo comportamento utilizzando la statistica Conteggio del campione nella console. Nota che ogni parametro nella tabella seguente dispone di statistiche rilevanti per il nodo e il cluster.

> **Important**
>
> Versioni diverse di Elasticsearch utilizzano pool di thread diversi per elaborare le chiamate all'API `_index`. Elasticsearch 1.5 e 2.3 utilizzano il pool di thread di indice. Elasticsearch 5.x, 6.0 e 6.2 utilizzano il pool di thread in blocco. OpenSearch e Elasticsearch 6.3 e versioni successive utilizzano il pool di thread di scrittura. Attualmente, la console OpenSearch di servizio non include un grafico per il pool di thread in blocco.
> Utilizzare `GET _cluster/settings?include_defaults=true` per controllare le dimensioni del pool di thread e della coda per il cluster.

Parametro	Descrizione
`ConcurrentSearchRate`	Il numero totale di richieste di ricerca che utilizzano la ricerca simultanea per segmenti al minuto per tutti gli shard su un nodo di dati. Una singola chiamata all'API `_search` potrebbe restituir e risultati da diverse partizioni. Se cinque di queste partizioni si trovano in un solo nodo, il nodo indicherà 5 per questo parametro, anche se il client ha effettuato una sola richiesta. Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Media, Massima, Somma
`ConcurrentSearchLatency`	La differenza nel tempo totale, in millisecondi, impiegato da tutte le ricerche utilizzando la ricerca simultanea per segmenti in un nodo tra il minuto N e il minuto (N-1). Statistiche di nodo rilevanti: Media

Parametro	Descrizione
	Statistiche del cluster rilevanti: Media, Massima
`IndexingLatency`	La differenza nel tempo totale, in millisecondi, rilevata da tutte le operazioni di indicizzazione in un nodo tra il minuto N e il minuto (N-1). Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Media, Massima
`IndexingRate`	Il numero di operazioni di indicizzazione al minuto. Una singola chiamata all'API `_bulk` che aggiunge due documenti e aggiorna due conteggi come quattro operazioni, che possono essere diffuse in uno o più nodi. Se tale indice ha una o più repliche e si trova in un OpenSearch dominio senza istanze ottimizzate, anche gli altri nodi del cluster registrano un totale di quattro operazioni di indicizzazione. Per i OpenSearch domini con istanze ottimizza te, gli altri nodi con repliche non registrano alcuna operazione. L'eliminazione di documenti non viene conteggiata ai fini di questo parametro. Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Media, Massima, Somma
`SearchLatency`	La differenza nel tempo totale, in millisecondi, rilevato da tutte le ricerche in un nodo tra il minuto N e il minuto (N-1). Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Media, Massima

Parametro	Descrizione
`SearchRate`	Il numero totale di richieste di ricerca al minuto per tutte le partizioni in un nodo di dati. Una singola chiamata all'API `_search` potrebbe restituire risultati da diverse partizioni. Se cinque di queste partizioni si trovano in un solo nodo, il nodo indicherà 5 per questo parametro, anche se il client ha effettuato una sola richiesta. Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Media, Massima, Somma
`SegmentCount`	Il numero di segmenti in un nodo di dati. Più segmenti hai, più tempo impiega ogni ricerca. OpenSearch occasionalmente unisce segmenti più piccoli in segmenti più grandi. Statistiche nodo rilevanti: Massima, Media Statistiche del cluster rilevanti: Somma, Massimo, Media
`SysMemoryUtilization`	La percentuale di memoria dell'istanza utilizzata. I valori elevati per questa metrica sono normali e in genere non rappresentano un problema con il cluster. Per un migliore indicatore dei potenziali problemi di prestazioni e stabilità, vedere la metrica `JVMMemoryPressure` . Statistiche di nodo rilevanti: Minima, Massima, Media Statistiche del cluster rilevanti: Minima, Massima, Media
`JVMGCYoungCollectionCount`	Il numero di volte in cui è stata eseguita la garbage collection di "nuova generazione". Un numero elevato e in continua crescita di esecuzioni è una parte normale delle operazioni del cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media

Parametro	Descrizione
`JVMGCYoungCollectionTime`	La quantità di tempo, in millisecondi, che il cluster ha impiegato per eseguire la garbage collection di "nuova generazione". Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`JVMGCOldCollectionCount`	Il numero di volte in cui è stata eseguita la garbage collection "vecchia generazione". In un cluster con risorse sufficienti, questo numero deve rimanere basso e senza frequenti incrementi. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`JVMGCOldCollectionTime`	La quantità di tempo, in millisecondi, che il cluster ha impiegato per eseguire la garbage collection "vecchia generazione". Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`OpenSearchDashboardsConcurrentConnections`	Il numero di connessioni simultanee attive alle dashboard. OpenSearch Se questo numero cresce costantemente, valutare la possibilità di dimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`OpenSearchDashboardsHealthyNode`	Un controllo dello stato del singolo nodo OpenSearch Dashboards. Un valore pari a 1 indica un comportamento normale. Un valore pari a 0 indica che Dashboards non è accessibile. Statistiche nodo rilevanti: Minima Statistiche del cluster rilevanti: Minima, Massima, Media

Parametro	Descrizione
`OpenSearchDashboardsHeapTotal`	La quantità di memoria heap allocata alle OpenSearch dashboard in MiB. Diversi tipi di istanza EC2 possono influire sull'esatta allocazione della memoria. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`OpenSearchDashboardsHeapUsed`	La quantità assoluta di memoria heap utilizzata dai OpenSearch dashboard in MiB. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`OpenSearchDashboardsHeapUtilization`	La percentuale massima di memoria heap disponibile utilizzata dai dashboard. OpenSearch Se questo valore supera l'80%, valutare la possibilità di dimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Minima, Massima, Media
`OpenSearchDashboardsOS1MinuteLoad`	La media di carico della CPU in un minuto per le dashboard. OpenSearch Il carico della CPU dovrebbe idealmente rimanere al di sotto di 1. Mentre i picchi temporanei vanno bene, se questo parametro è costantemente superiore a 1 si consiglia di aumentare la dimensione del tipo di istanza. Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Media, Massima

Parametro	Descrizione
`OpenSearchDashboardsRequestTotal`	Il numero totale di richieste HTTP inviate alle OpenSearch dashboard. Se il sistema è lento o viene visualizzato un numero elevato di richieste Dashboards, è consigliabile aumentare le dimensioni del tipo di istanza. Statistiche del nodo rilevanti: Somma Statistiche del cluster rilevanti: Somma
`OpenSearchDashboardsResponseTimesMaxInMillis`	Il tempo massimo, in millisecondi, impiegato dai OpenSearch dashboard per rispondere a una richiesta. Se le richieste richiedon o molto tempo per restituire i risultati, è consigliabile aumentare le dimensioni del tipo di istanza. Statistiche di nodo rilevanti: Massima Statistiche cluster rilevanti: Massima, Media
`SearchTaskCancelled`	Il numero di cancellazioni del nodo coordinatore. Statistiche del nodo rilevanti: Somma Statistiche del cluster rilevanti: Somma
`SearchShardTaskCancelled`	Il numero di cancellazioni dei nodi dati. Statistiche del nodo rilevanti: Somma Statistiche pertinenti sui cluster: somma,
`ThreadpoolForce_mergeQueue`	Il numero di attività in coda nel pool di thread forza unione. Se la dimensione della coda è costantemente elevata, valutare la possibilità di ridimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media

Parametro	Descrizione
`ThreadpoolForce_mergeRejected`	Il numero di attività rifiutate nel pool di thread forza unione. Se questo numero cresce costantemente, valutare la possibilità di ridimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma
`ThreadpoolForce_mergeThreads`	Le dimensioni del pool di thread forza unione. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma
`ThreadpoolIndexQueue`	Il numero di attività in coda nel pool di thread di indice. Se la dimensione della coda è costantemente elevata, valutare la possibilità di ridimensionare il cluster. La dimensione massima della coda dell'indice è di 200. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`ThreadpoolIndexRejected`	Il numero di attività rifiutate nel pool di thread di indice. Se questo numero cresce costantemente, valutare la possibilità di ridimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma
`ThreadpoolIndexThreads`	Le dimensioni del pool di thread di indice. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma

Parametro	Descrizione
`ThreadpoolSearchQueue`	Il numero di attività in coda nel pool di thread di ricerca. Se la dimensione della coda è costantemente elevata, valutare la possibilità di ridimensionare il cluster. La dimensione massima della coda di ricerca è di 1.000. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`ThreadpoolSearchRejected`	Il numero di attività rifiutate nel pool di thread di ricerca. Se questo numero cresce costantemente, valutare la possibilità di ridimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma
`ThreadpoolSearchThreads`	Le dimensioni del pool di thread di ricerca. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma
`Threadpoolsql-workerQueue`	Il numero di attività in coda nel pool di thread di ricerca SQL. Se la dimensione della coda è costantemente elevata, valutare la possibilità di ridimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`Threadpoolsql-workerRejected`	Il numero di attività rifiutate nel pool di thread di ricerca SQL. Se questo numero cresce costantemente, valutare la possibilità di ridimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma

Parametro	Descrizione
`Threadpoolsql-workerThreads`	Le dimensioni del pool di thread di ricerca SQL. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma
`ThreadpoolBulkQueue`	Il numero di attività in coda nel pool di thread blocco. Se la dimensione della coda è costantemente elevata, valutare la possibilità di ridimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`ThreadpoolBulkRejected`	Il numero di attività rifiutate nel pool di thread blocco. Se questo numero cresce costantemente, valutare la possibilità di ridimensionare il cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma
`ThreadpoolBulkThreads`	Le dimensioni del pool di thread blocco. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma
`ThreadpoolIndexSearcherQueue`	Il numero di attività in coda nel pool di thread di index searcher. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`ThreadpoolIndexSearcherRejected`	Il numero di attività rifiutate nel pool di thread di index searcher. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma

Parametro	Descrizione
`ThreadpoolIndexSearcherThreads`	La dimensione del pool di thread di Index Searcher. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma
`ThreadpoolWriteThreads`	La dimensione del pool di thread di scrittura. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma
`ThreadpoolWriteQueue`	Il numero di attività in coda nel pool di thread di scrittura. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma
`ThreadpoolWriteRejected`	Il numero di attività rifiutate nel pool di thread di scrittura. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma **Note** Poiché la dimensione predefinita della coda di scrittura è stata aumentata da 200 a 10000 nella versione 7.1, questa metrica non è più l'unico indicatore dei rifiuti da parte del Servizio. OpenSearch Utilizzare i parametri `CoordinatingWriteRejected` , `PrimaryWriteRejected` e `ReplicaWriteRejected` per monitorare i rifiuti nelle versioni 7.1 e successive.

Parametro	Descrizione
`CoordinatingWriteRejected`	Il numero totale di rifiuti si è verificato sul nodo di coordinamento a causa della pressione di indicizzazione dall'ultimo avvio del processo di servizio. OpenSearch Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma Questo parametro è disponibile nella versione 7.1 e nelle versioni successive.
`PrimaryWriteRejected`	Il numero totale di rifiuti si è verificato sugli shard primari a causa della pressione di indicizzazione dall'ultimo avvio del processo di servizio. OpenSearch Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma Questo parametro è disponibile nella versione 7.1 e nelle versioni successive.
`ReplicaWriteRejected`	Il numero totale di rifiuti si è verificato sugli shard di replica a causa della pressione di indicizzazione dall'ultimo avvio del processo di servizio. OpenSearch Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma Questo parametro è disponibile nella versione 7.1 e nelle versioni successive.

UltraWarm metriche

Amazon OpenSearch Service fornisce le seguenti metriche per UltraWarmi nodi.

Parametro	Descrizione
`WarmCPUUtilization`	La percentuale di utilizzo della CPU per UltraWarm i nodi del cluster. Il numero massimo mostra il nodo con il più alto utilizzo della CPU. La media rappresenta tutti UltraWarm i nodi del cluster. Questa metrica è disponibile anche per i singoli UltraWarm nodi. Statistiche rilevanti: Maximum (Massimo), Average (Media)
`WarmFreeStorageSpace`	La quantità di spazio di archiviazione a caldo gratuito in MiB. Poiché UltraWarm utilizza Amazon S3 anziché dischi collegati, `Sum` è l'unica statistica rilevante. È necessario lasciare il periodo su un minuto per ottenere un valore preciso. Statistiche rilevanti: Sum (Somma)
`WarmSearchableDocuments`	Il numero totale di documenti disponibili per la ricerca tra tutti gli indici a caldo nel cluster. È necessario lasciare il periodo su un minuto per ottenere un valore preciso. Statistiche rilevanti: Sum (Somma)
`WarmSearchLatency`	La differenza nel tempo totale, in millisecondi, rilevato da tutte le ricerche in un intervallo UltraWarm compreso tra il minuto N e il minuto (N-1). Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Media, Massima
`WarmSearchRate`	Il numero totale di richieste di ricerca al minuto per tutti gli shard su un nodo. UltraWarm Una singola chiamata all'API `_search` potrebbe restituire risultati da diverse partizioni. Se cinque di queste partizioni si trovano in un solo nodo, il nodo indicherà 5 per questo parametro, anche se il client ha effettuato una sola richiesta. Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Media, Massima, Somma

Parametro	Descrizione
`WarmStorageSpaceUtilization`	La quantità totale di spazio di archiviazione a caldo, in MiB, che sta utilizzando il cluster. Statistiche rilevanti: Massima
`HotStorageSpaceUtilization`	La quantità totale di spazio di archiviazione ad accesso frequente utilizzata dal cluster. Statistiche rilevanti: Massima
`WarmSysMemoryUtilization`	La percentuale di memoria del nodo Warm utilizzata. Statistiche rilevanti: Massima
`HotToWarmMigrationQueueSize`	Il numero di indici attualmente in attesa di migrazione dall'archiviazione ad accesso frequente a quella a caldo. Statistiche rilevanti: Massima
`WarmToHotMigrationQueueSize`	Il numero di indici attualmente in attesa di migrazione dall'archiviazione a caldo a quella ad accesso frequente. Statistiche rilevanti: Massima
`HotToWarmMigrationFailureCount`	Il numero totale di migrazioni da "ad accesso frequente" a "a caldo" non riuscite. Statistiche rilevanti: Sum (Somma)
`HotToWarmMigrationForceMergeLatency`	La latenza media della fase di unione forzata del processo di migrazione. Se questa fase richiede costantemente troppo tempo, prendere in considerazione l'aumento di `index.ultrawarm.migration.force_merge.max_num_segments` . Statistiche rilevanti: Average (Media)

Parametro	Descrizione
`HotToWarmMigrationSnapshotLatency`	La latenza media della fase di snapshot del processo di migrazione. Se questa fase richiede troppo tempo, assicurarsi che le partizioni siano dimensionate e distribuite in modo appropriato in tutto il cluster. Statistiche rilevanti: Average (Media)
`HotToWarmMigrationProcessingLatency`	La latenza media delle migrazioni riuscite da "ad accesso frequente" a "a caldo", senza includere il tempo trascorso nella coda. Questo valore è la somma del tempo necessario per completare le fasi di unione forzata, snapshot e rilocazione delle partizioni del processo di migrazione. Statistiche rilevanti: Average (Media)
`HotToWarmMigrationSuccessCount`	Il numero totale di migrazioni riuscite da "ad accesso frequente" a "a caldo". Statistiche rilevanti: Sum (Somma)
`HotToWarmMigrationSuccessLatency`	La latenza media delle migrazioni riuscite da "ad accesso frequente" a "a caldo", compreso il tempo trascorso nella coda. Statistiche rilevanti: Average (Media)
`WarmThreadpoolSearchThreads`	La dimensione del pool di thread UltraWarm di ricerca. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Media, Somma
`WarmThreadpoolSearchRejected`	Il numero di attività rifiutate nel pool UltraWarm di thread di ricerca. Se questo numero aumenta continuamente, valuta la possibilità di aggiungere altri UltraWarm nodi. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma

Parametro	Descrizione
`WarmThreadpoolSearchQueue`	Il numero di attività in coda nel pool di thread di UltraWarm ricerca. Se la dimensione della coda è costantemente elevata, valuta la possibilità di aggiungere altri nodi. UltraWarm Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`WarmJVMMemoryPressure`	La percentuale massima dell'heap Java utilizzata per i UltraWarm nodi. Statistiche rilevanti: Massima **Note** La logica di questo parametro è cambiata nel software del servizio R20220323. Per ulteriori informazioni, consulta le note di rilascio.
`WarmOldGenJVMMemoryPressure`	La percentuale massima dell'heap Java utilizzato per la «vecchia generazione» per UltraWarm nodo. Statistiche rilevanti: Massima
`WarmJVMGCYoungCollectionCount`	Il numero di volte in cui la raccolta dei rifiuti delle «giovani generazioni» è stata eseguita sui nodi. UltraWarm Un numero elevato e in continua crescita di esecuzioni è una parte normale delle operazioni del cluster. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`WarmJVMGCYoungCollectionTime`	La quantità di tempo, in millisecondi, impiegata dal cluster per eseguire la raccolta dei rifiuti di «nuova generazione» sui nodi. UltraWarm Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media

Parametro	Descrizione
`WarmJVMGCOldCollectionCount`	Il numero di volte in cui la raccolta dei rifiuti di «vecchia generazione» è stata eseguita sui nodi. UltraWarm In un cluster con risorse sufficienti, questo numero deve rimanere basso e senza frequenti incrementi. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media
`WarmConcurrentSearchRate`	Il numero totale di richieste di ricerca che utilizzano la ricerca simultane a per segmenti al minuto per tutti gli shard su un nodo. UltraWarm Una singola chiamata all'API `_search` potrebbe restituire risultati da diverse partizioni. Se cinque di queste partizioni si trovano in un solo nodo, il nodo indicherà 5 per questo parametro, anche se il client ha effettuato una sola richiesta. Statistiche di nodo rilevanti: Media Statistiche del cluster rilevanti: Somma, Massimo, Media
`WarmConcurrentSearchLatency`	La differenza nel tempo totale, in millisecondi, impiegato da tutte le ricerche utilizzando la ricerca simultanea per segmenti in un UltraWarm nodo tra il minuto N e il minuto (N-1). Statistiche di nodo rilevanti: Media Statistiche cluster rilevanti: Massima, Media
`WarmThreadpoolIndexSearcherQueue`	Il numero di attività in coda nel pool di thread di index searcher. UltraWarm Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma, Massimo, Media

Parametro	Descrizione
`WarmThreadpoolIndexSearcherRejected`	Il numero di attività rifiutate nel pool di thread di UltraWarm index searcher. Statistiche di nodo rilevanti: Massima Statistiche del cluster rilevanti: Somma
`WarmThreadpoolIndexSearcherThreads`	La dimensione del pool di thread di UltraWarm index searcher. Statistiche di nodo rilevanti: Massima Statistiche pertinenti sui cluster: somma, media

Parametri di archiviazione a freddo

Amazon OpenSearch Service fornisce le seguenti metriche per la conservazione a freddo.

Parametro	Descrizione
`ColdStorageSpaceUtilization`	La quantità totale di spazio di archiviazione a freddo, in MiB, utilizzato dal cluster. Statistiche rilevanti: Max (Massimo)
`ColdToWarmMigrationFailureCount`	Il numero totale di migrazioni da freddo a caldo non riuscite. Statistiche rilevanti: Sum (Somma)
`ColdToWarmMigrationLatency`	Il tempo necessario per completare le migrazioni da freddo a caldo riuscite. Statistiche rilevanti: Average (Media)
`ColdToWarmMigrationQueueSize`	Il numero di indici attualmente in attesa di migrazione dall'archiviazione a freddo a quella a caldo. Statistiche rilevanti: Massima

Parametro	Descrizione
`ColdToWarmMigrationSuccessCount`	Il numero totale di migrazioni da freddo a caldo riuscite. Statistiche rilevanti: Sum (Somma)
`WarmToColdMigrationFailureCount`	Il numero totale di migrazioni da caldo a freddo non riuscite. Statistiche rilevanti: Sum (Somma)
`WarmToColdMigrationLatency`	Il tempo necessario per completare le migrazioni da caldo a freddo riuscite. Statistiche rilevanti: Average (Media)
`WarmToColdMigrationQueueSize`	Il numero di indici attualmente in attesa di migrazione dall'archiviazione a caldo a quella a freddo. Statistiche rilevanti: Massima
`WarmToColdMigrationSuccessCount`	Il numero totale di migrazioni da caldo a freddo riuscite. Statistiche rilevanti: Sum (Somma)

Metriche OR1

Amazon OpenSearch Service fornisce i seguenti parametri per le istanze OR1.

Parametro	Descrizione
`RemoteStorageUsedSpace`	La quantità totale di spazio Amazon S3, in MiB, utilizzata dal cluster. Statistiche rilevanti: Sum (Somma)
`RemoteStorageWriteRejected`	Il numero totale di richieste rifiutate sugli shard primari a causa della pressione di storage e replica remoti. Viene calcolato a partire dall'ultimo avvio del processo OpenSearch di servizio. Statistiche rilevanti: Sum (Somma)

Parametri di avvisi

Amazon OpenSearch Service fornisce le seguenti metriche per gli avvisi.

Parametro	Descrizione
`AlertingDegraded`	Il valore 1 indica che l'indice di allerta è rosso oppure uno o più nodi non sono pianificati. Un valore 0 indica un comportamento normale. Statistiche rilevanti: Massima
`AlertingIndexExists`	Un valore pari a 1 significa che l'indice `.opensearch-alerting-config` esiste. Un valore pari a 0 significa che non esiste. Fino a quando non si utilizza la funzione di allarme per la prima volta, questo valore rimane 0. Statistiche rilevanti: Massima
`AlertingIndexStatus.green`	La salute dell'indice. Un valore pari a 1 significa verde. Un valore pari a 0 significa che l'indice non esiste o non è verde. Statistiche rilevanti: Massima
`AlertingIndexStatus.red`	La salute dell'indice. Un valore pari a 1 significa rosso. Un valore pari a 0 significa che l'indice non esiste o non è rosso. Statistiche rilevanti: Massima
`AlertingIndexStatus.yellow`	La salute dell'indice. Un valore pari a 1 significa giallo. Un valore pari a 0 significa che l'indice non esiste o non è giallo. Statistiche rilevanti: Massima
`AlertingNodesNotOnSchedule`	Il valore 1 indica che alcuni processi non sono in esecuzione nei tempi previsti. Il valore 0 indica che tutti i processi di allerta sono in esecuzione e nella pianificazione (o che non esistono processi di avvisi). Controlla la console OpenSearch di servizio o fai una `_nodes/stats` richiesta per vedere se alcuni nodi mostrano un elevato utilizzo delle risorse. Statistiche rilevanti: Massima

Parametro	Descrizione
`AlertingNodesOnSchedule`	Il valore 1 indica che tutti i processi di allerta sono in esecuzione nella pianificazione (o che non esistono processi di avvisi). Un valore pari a 0 indica che alcuni processi non sono in esecuzione nella pianificazione. Statistiche rilevanti: Massima
`AlertingScheduledJobEnabled`	Il valore 1 indica che l'impostazione del cluster `opensearch.scheduled_jobs.enabled` è true. Il valore 0 indica che è falsa e i processi pianificati sono disabilitati. Statistiche rilevanti: Massima

Parametri di rilevamento delle anomalie

Amazon OpenSearch Service fornisce le seguenti metriche per il rilevamento delle anomalie.

Parametro	Descrizione
`ADPluginUnhealthy`	Il valore 1 indica che il plug-in di rilevamento delle anomalie non funziona correttamente, a causa di un numero elevato di errori o perché uno degli indici utilizzati è rosso. Il valore 0 indica che il plugin funziona come previsto. Statistiche rilevanti: Massima
`ADExecuteRequestCount`	Numero di richieste per il rilevamento delle anomalie. Statistiche rilevanti: Sum (Somma)
`ADExecuteFailureCount`	Numero di richieste non riuscite per il rilevamento delle anomalie. Statistiche rilevanti: Sum (Somma)
`ADHCExecuteFailureCount`	Il numero di richieste non riuscite per il rilevamento delle anomalie per i rilevatori ad alta cardinalità. Statistiche rilevanti: Sum (Somma)

Parametro	Descrizione
`ADHCExecuteRequestCount`	Il numero di richieste per il rilevamento delle anomalie per i rilevatori ad alta cardinalità. Statistiche rilevanti: Sum (Somma)
`ADAnomalyResultsIndexStatusIndexExists`	Il valore 1 indica che l'indice a cui punta l'alias `.opensearch-anomaly-results` esiste. Fino a quando non si utilizza la funzionalità di rilevamento delle anomalie per la prima volta, questo valore rimane 0. Statistiche rilevanti: Massima
`ADAnomalyResultsIndexStatus.red`	Il valore 1 indica che l'indice a cui punta l'alias `.opensearch-anomaly-results` è rosso. Un valore pari a 0 significa che non lo è. Fino a quando non si utilizza la funzionalità di rilevamento delle anomalie per la prima volta, questo valore rimane 0. Statistiche rilevanti: Massima
`ADAnomalyDetectorsIndexStatusIndexExists`	Un valore pari a 1 significa che l'indice `.opensearch-anomaly-detectors` esiste. Un valore pari a 0 significa che non esiste. Fino a quando non si utilizza la funzionalità di rilevamento delle anomalie per la prima volta, questo valore rimane 0. Statistiche rilevanti: Massima
`ADAnomalyDetectorsIndexStatus.red`	Un valore pari a 1 indica che l'indice `.opensearch-anomaly-detectors` è rosso. Un valore pari a 0 significa che non lo è. Fino a quando non si utilizza la funzionalità di rilevamento delle anomalie per la prima volta, questo valore rimane 0. Statistiche rilevanti: Massima
`ADModelsCheckpointIndexStatusIndexExists`	Un valore pari a 1 significa che l'indice `.opensearch-anomaly-checkpoints` esiste. Un valore pari a 0 significa che non esiste. Fino a quando non si utilizza la funzionalità di rilevamento delle anomalie per la prima volta, questo valore rimane 0. Statistiche rilevanti: Massima

Parametro	Descrizione
`ADModelsCheckpointIndexStatus.red`	Un valore pari a 1 indica che l'indice `.opensearch-anomaly-checkpoints` è rosso. Un valore pari a 0 significa che non lo è. Fino a quando non si utilizza la funzionalità di rilevamento delle anomalie per la prima volta, questo valore rimane 0. Statistiche rilevanti: Massima

Parametri di ricerca asincrona

Amazon OpenSearch Service fornisce le seguenti metriche per la ricerca asincrona.

Statistiche del nodo coordinatore di ricerca asincrona (per nodo coordinatore)

Parametro	Descrizione
`AsynchronousSearchSubmissionRate`	Il numero di ricerche asincrone inviate nell'ultimo minuto.
`AsynchronousSearchInitializedRate`	Il numero di ricerche asincrone inizializzate nell'ultimo minuto.
`AsynchronousSearchRunningCurrent`	Il numero di ricerche asincrone correntemente in esecuzione.
`AsynchronousSearchCompletionRate`	Il numero di ricerche asincrone completate correttamente nell'ultimo minuto.
`AsynchronousSearchFailureRate`	Il numero di ricerche asincrone completate e non riuscite nell'ultimo minuto.

Parametro	Descrizione
`AsynchronousSearchPersistRate`	Il numero di ricerche asincrone conservate nell'ultimo minuto.
`AsynchronousSearchPersistFailedRate`	Il numero di ricerche asincrone che non sono state conservate nell'ultimo minuto.
`AsynchronousSearchRejected`	Il numero totale di ricerche asincrone rifiutate dall'attivazione del nodo.
`AsynchronousSearchCancelled`	Il numero totale di ricerche asincrone cancellate dall'attivazione del nodo.
`AsynchronousSearchMaxRunningTime`	La durata della ricerca asincrona più lunga in esecuzione su un nodo nell'ultimo minuto.

Statistiche del cluster di ricerca asincrona

Parametro	Descrizione
`AsynchronousSearchStoreHealth`	Lo stato dell'archiviazione nell'indice persistente (rosso/non rosso) nell'ultimo minuto.
`AsynchronousSearchStoreSize`	La dimensione dell'indice di sistema su tutte le partizioni nell'ultimo minuto.
`AsynchronousSearch`	Il numero di risposte memorizzate nell'indice di sistema nell'ultimo minuto.

Parametro	Descrizione
StoredResponseCount	

Metriche Auto-Tune

Amazon OpenSearch Service fornisce le seguenti metriche per Auto-Tune.

Parametro	Descrizione
AutoTuneChangesHistoryHeapSize	La cronologia delle modifiche in MiB per i valori di ottimizzazione delle dimensioni dell'heap.
AutoTuneChangesHistoryJVMYoungGenArgs	La cronologia delle modifiche per gli argomenti JVM. YongGen
AutoTuneFailed	Un valore booleano che indica se la modifica Auto-Tune non è riuscita.
AutoTuneSucceeded	Un valore booleano che indica se la modifica Auto-Tune è stata completata.
AutoTuneValue	La cronologia delle modifiche alla coda (count) e le ottimizzazioni della cache modificano la cronologia (in MiB) per modifiche senza interruzioni.

Multi-AZ con metriche Standby

Amazon OpenSearch Service fornisce le seguenti metriche per Multi-AZ with Standby.

Metriche a livello di nodo per i nodi di dati nelle zone di disponibilità attive

Parametro	Descrizione
CPUUtilization	Percentuale di utilizzo della CPU per i nodi di dati nel cluster. Il numero massimo mostra il nodo con il più alto utilizzo della CPU. La media

Parametro	Descrizione
	rappresenta tutti i nodi del cluster. Questo parametro è disponibile anche per singoli nodi.
`FreeStorageSpace`	Lo spazio libero per i nodi di dati nel cluster. `Sum` mostra lo spazio libero totale per il cluster, ma è necessario lasciare il periodo a un minuto per ottenere un valore accurato. `Minimum` e `Maximum` mostrano i nodi con lo spazio libero maggiore e minore, rispettivamente. Questa metrica è disponibile anche per i singoli nodi. OpenSearch Il servizio genera un `ClusterBlockException` quando questa metrica raggiunge. `0` Per risolvere il problema devi eliminare gli indici, aggiunger e istanze più grandi oppure aggiungere archiviazione basata su EBS alle istanze esistenti. Per ulteriori informazioni, consulta the section called “Mancanza di spazio di archiviazione disponibile”. La console OpenSearch di servizio visualizza questo valore in GiB. La CloudWatch console Amazon lo visualizza in MiB.
`JVMMemoryPressure`	La percentuale massima dell'heap Java utilizzata per tutti i nodi di dati del cluster. OpenSearch Il servizio utilizza metà della RAM di un'istanza per l'heap Java, fino a una dimensione dell'heap di 32 GiB. Puoi scalare le istanze verticalmente fino a 64 GiB di RAM e poi scalare orizzonta lmente aggiungendo le istanze. Per informazioni, consulta the section called “Allarmi consigliati CloudWatch ”.
`SysMemoryUtilization`	La percentuale di memoria dell'istanza utilizzata. I valori elevati per questa metrica sono normali e in genere non rappresentano un problema con il cluster. Per un migliore indicatore dei potenziali problemi di prestazioni e stabilità, vedere la metrica `JVMMemoryPressure` .
`IndexingLatency`	La differenza nel tempo totale, in millisecondi, rilevata da tutte le operazioni di indicizzazione in un nodo tra i minuti N e i minuti (N-1).
`IndexingRate`	Il numero di operazioni di indicizzazione al minuto.
`SearchLatency`	La differenza nel tempo totale, in millisecondi, rilevato da tutte le ricerche in un nodo tra il minuto N e il minuto (N-1).

Parametro	Descrizione
SearchRate	Il numero totale di richieste di ricerca al minuto per tutte le partizioni in un nodo di dati.
ThreadpoolSearchQueue	Il numero di attività in coda nel pool di thread di ricerca. Se la dimensione della coda è costantemente elevata, valutare la possibilità di ridimensionare il cluster. La dimensione massima della coda di ricerca è di 1.000.
ThreadpoolWriteQueue	Il numero di attività in coda nel pool di thread di scrittura.
ThreadpoolSearchRejected	Il numero di attività rifiutate nel pool di thread di ricerca. Se questo numero cresce costantemente, valutare la possibilità di ridimensionare il cluster.
ThreadpoolWriteRejected	Il numero di attività rifiutate nel pool di thread di scrittura.

Metriche a livello di cluster per i cluster nelle zone di disponibilità attive

Parametro	Descrizione
DataNodes	Il numero totale di shard attivi e in standby.
DataNodes Shards.active	Il numero totale di partizioni primarie e di replica attive.
DataNodes Shards.unassigned	Il numero di partizioni non allocate ai nodi nel cluster.
DataNodes Shards.initializing	Il numero di partizioni in fase di inizializzazione.

Parametro	Descrizione
`DataNodes Shards.relocating`	Il numero di partizioni in fase di rilocazione.

Metriche di rotazione della zona di disponibilità

`SeActiveReads.`*`Availability-Zone`* `= 1`, allora la zona è attiva.
`SeActiveReads.`*`Availability-Zone`* `= 0`, allora la zona è in standby.

Metriche puntuali

Amazon OpenSearch Service fornisce le seguenti metriche per le ricerche point-in-time (PIT).

Statistiche sul nodo coordinatore PIT (per nodo coordinatore)

Parametro	Descrizione
`CurrentPointInTime`	Il numero di contesti di ricerca PIT attivi nel nodo.
`TotalPointInTime`	Il numero di contesti di ricerca PIT scaduti dal momento dell'attività del nodo.
`AvgPointInTimeAliveTime`	Il mantenimento medio dei contesti di ricerca PIT dal momento dell'attività del nodo.
`HasActivePointInTime`	Il valore 1 indica che ci sono contesti PIT attivi sui nodi sin dal momento in cui il nodo è attivo. Un valore pari a 0 significa che non ce ne sono.
`HasUsedPointInTime`	Il valore 1 indica che ci sono contesti PIT scaduti sui nodi dal momento in cui il nodo è attivo. Un valore pari a 0 significa che non ce ne sono.

Parametri SQL

Amazon OpenSearch Service fornisce le seguenti metriche per il supporto SQL.

Parametro	Descrizione
`SQLFailedRequestCountByCusErr`	Numero di richieste all'API `_sql` non riuscite a causa di un problema client. Ad esempio, una richiesta potrebbe restituire il codice di stato HTTP 400 a causa di un `IndexNotFoundException` . Statistiche rilevanti: Sum (Somma)
`SQLFailedRequestCountBySysErr`	Numero di richieste all'API `_sql` non riuscite a causa di un problema del server o di una limitazione della funzionalità. Ad esempio, una richiesta potrebbe restituire il codice di stato HTTP 503 a causa di un `VerificationException` . Statistiche rilevanti: Sum (Somma)
`SQLRequestCount`	Il numero di richieste all'API `_sql`. Statistiche rilevanti: Sum (Somma)
`SQLDefaultCursorRequestCount`	Simile a`SQLRequestCount` , ma conta solo le richieste di impaginazione. Statistiche rilevanti: Sum (Somma)
`SQLUnhealthy`	Il valore 1 indica che, in risposta a determinate richieste, il plugin SQL restituisce 5 codici di risposta xx o sta passando una query DSL non valida a. OpenSearch Altre richieste dovrebbero continuare ad avere esito positivo. Un valore pari a 0 indica nessun errore recente. Se viene visualizzato un valore sostenuto pari a 1, risolvere i problemi relativi alle richieste che i client stanno facendo al plugin. Statistiche rilevanti: Massima

Parametri k-NN

Amazon OpenSearch Service include le seguenti metriche per il plugin k-Nearest Neighbor (k-NN).

Parametro	Descrizione
KNNCacheCapacityReached	Parametro per nodo per stabilire se è stata raggiunta la capacità della cache. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Massima
KNNCircuitBreakerTriggered	Parametro per cluster per indicare se l'interruttore è attivato. Se alcuni nodi restituiscono un valore pari a 1 per KNNCacheCapacityReached , anche questo valore restituirà 1. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Massima
KNNEvictionCount	Parametro per nodo per il numero di grafici rimossi dalla cache a causa di vincoli di memoria o tempo di inattività. Le rimozioni esplicite che si verificano a causa dell'eliminazione dell'indice non vengono conteggiate. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Sum (Somma)
KNNGraphIndexErrors	Parametro per nodo per il numero di richieste da aggiungere il campo knn_vector di un documento a un grafico che ha generato un errore. Statistiche rilevanti: Sum (Somma)
KNNGraphIndexRequests	Parametro per nodo per il numero di richieste per aggiungere il campo knn_vector di un documento a un grafico. Statistiche rilevanti: Sum (Somma)
KNNGraphMemoryUsage	Parametro per nodo per la dimensione della cache corrente (dimensione totale di tutti i grafici in memoria) in kilobyte. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Average (Media)

Parametro	Descrizione
`KNNGraphQueryErrors`	Parametro per nodo per il numero di query del grafico che hanno generato un errore. Statistiche rilevanti: Sum (Somma)
`KNNGraphQueryRequests`	Parametro per nodo per il numero di query del grafico. Statistiche rilevanti: Sum (Somma)
`KNNHitCount`	Parametro per nodo per il numero di occorrenze della cache. Una occorrenza della cache si verifica quando un utente esegue una query su un grafico già caricato in memoria. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Sum (Somma)
`KNNLoadExceptionCount`	Parametro per nodo per il numero di volte in cui si è verificat a un'eccezione durante il tentativo di caricare un grafico nella cache. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Sum (Somma)
`KNNLoadSuccessCount`	Parametro per nodo per il numero di volte in cui il plug-in ha caricato correttamente un grafico nella cache. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Sum (Somma)
`KNNMissCount`	Parametro per nodo per il numero di mancati riscontri nella cache. Un mancato riscontro nella cache si verifica quando un utente esegue una query su un grafico non ancora caricato in memoria. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Sum (Somma)

Parametro	Descrizione
KNNQueryRequests	Parametro per nodo per il numero di richieste di query ricevute dal plugin k-NN. Statistiche rilevanti: Sum (Somma)
KNNScriptCompilationErrors	Parametro per nodo per il numero di errori durante la compilazione dello script. Questa statistica è rilevante solo per la ricerca di script di punteggio k-NN. Statistiche rilevanti: Sum (Somma)
KNNScriptCompilations	Parametro per nodo per il numero di volte in cui lo script k-NN è stato compilato. Questo valore dovrebbe in genere essere 1 o 0, ma se la cache contenente gli script compilati viene riempita, lo script k-NN potrebbe essere ricompilato. Questa statistica è rilevante solo per la ricerca di script di punteggio k-NN. Statistiche rilevanti: Sum (Somma)
KNNScriptQueryErrors	Parametro per nodo per il numero di errori durante le query dello script. Questa statistica è rilevante solo per la ricerca di script di punteggio k-NN. Statistiche rilevanti: Sum (Somma)
KNNScriptQueryRequests	Parametro per nodo per il numero totale di query dello script. Questa statistica è rilevante solo per la ricerca di script di punteggio k-NN. Statistiche rilevanti: Sum (Somma)
KNNTotalLoadTime	Il tempo in nanosecondi impiegato da k-NN per caricare i grafici nella cache. Questo parametro è rilevante solo per approssimare la ricerca k-NN. Statistiche rilevanti: Sum (Somma)

Parametri di ricerca tra cluster

Amazon OpenSearch Service fornisce le seguenti metriche per la ricerca tra cluster.

Parametri del dominio di origine

Parametro	Dimensione	Descrizione
`CrossClusterOutboundConnections`	`ConnectionId`	Numero di nodi connessi. Se la risposta include uno o più domini ignorati, utilizzare questo parametro per tracciare eventuali connessioni non integre. Se questo numero scende a 0, la connessione non è integra.
`CrossClusterOutboundRequests`	`ConnectionId`	Numero di richieste di ricerca inviate al dominio di destinazione. Utilizzare per verificare se il carico di richieste di ricerca tra cluster sta sovraccaricando il dominio; correlare eventuali picchi in questo parametro con eventuali picchi JVM/CPU.

Parametri del dominio di destinazione

Parametro	Dimensione	Descrizione
`CrossClusterInboundRequests`	`ConnectionId`	Numero di richieste di connessione in ingresso ricevute dal dominio di origine.

Aggiungi un CloudWatch allarme nel caso in cui perdi una connessione in modo imprevisto. Per i passaggi per creare un allarme, vedi Creare un CloudWatch allarme basato su una soglia statica.

Parametri di replica tra cluster

Amazon OpenSearch Service fornisce le seguenti metriche per la replica tra cluster.

Parametro	Descrizione
`ReplicationRate`	La percentuale media di operazioni di replica al secondo. Questo parametro è analogo al parametro `IndexingRate` .
`LeaderCheckPoint`	Per una connessione specifica, la somma dei valori del checkpoint leader in tutti gli indici di replica. Puoi utilizzare questo parametro per misurare la latenza di replica.
`FollowerCheckPoint`	Per una connessione specifica, la somma dei valori del checkpoint follower in tutti gli indici di replica. Puoi utilizzare questo parametro per misurare la latenza di replica.
`ReplicationNumSyncingIndices`	Il numero di indici con uno stato di replica di `SYNCING`.
`ReplicationNumBootstrappingIndices`	Il numero di indici con uno stato di replica di `BOOTSTRAPPING` .
`ReplicationNumPausedIndices`	Il numero di indici con uno stato di replica di `PAUSED`.
`ReplicationNumFailedIndices`	Il numero di indici con uno stato di replica di `FAILED`.
`CrossClusterOutboundReplicationRequests`	Il numero di richieste di trasporto di replica sul dominio del follower. Le richieste di trasporto sono interne e si verificano ogni volta che viene chiamata un'operazione API di replica. Si verificano anche quando il polling del dominio follower cambia rispetto al dominio leader.
`CrossClusterInboun`	Il numero di richieste di trasporto di replica sul dominio leader. Le richieste di trasporto sono interne e si verificano ogni volta che viene chiamata un'operazione API di replica.

Parametro	Descrizione
`dReplicationRequests`	
`AutoFollowNumSuccessStartReplication`	Il numero di indici follower creati correttamente da una regola di replica per una connessione specifica.
`AutoFollowNumFailedStartReplication`	Il numero di indici follower che non sono stati creati da una regola di replica in presenza di un modello corrispondente. Questo problema potrebbe sorgere a causa di un problema di rete sul cluster remoto o di un problema di sicurezza (ad esempio, il ruolo associato non ha l'autorizzazione per avviare la replica).
`AutoFollowLeaderCallFailure`	Se ci sono state query non riuscite dall'indice follower all'indice leader per estrarre nuovi dati. Un valore pari a 1 significa che ci sono state una o più chiamate non riuscite nell'ultimo minuto.

Parametri di Learning to Rank

Amazon OpenSearch Service fornisce le seguenti metriche per Learning to Rank.

Parametro	Descrizione
`LTRRequestTotalCount`	Conteggio totale delle richieste di classificazione.
`LTRRequestErrorCount`	Conteggio totale delle richieste non riuscite.
`LTRStatus.red`	Traccia se uno degli indici necessari per eseguire il plug-in è rosso.
`LTRMemoryUsage`	La memoria totale utilizzata dal plug-in.

Parametro	Descrizione
`LTRFeatureMemoryUsageInBytes`	La quantità di memoria, espressa in byte, utilizzata dai campi della funzionalità Learning to Rank.
`LTRFeaturesetMemoryUsageInBytes`	La quantità di memoria, espressa in byte, utilizzata dai set di funzionalità Learning to Rank.
`LTRModelMemoryUsageInBytes`	La quantità di memoria, espressa in byte, utilizzata da tutti i modelli Learning to Rank.

Parametri Piped Processing Language (PPL)

Amazon OpenSearch Service fornisce le seguenti metriche per Piped Processing Language.

Parametro	Descrizione
`PPLFailedRequestCountByCusErr`	Numero di richieste all'API `_ppl` non riuscite a causa di un problema client. Ad esempio, una richiesta potrebbe restituire il codice di stato HTTP 400 a causa di un `IndexNotFoundException` .
`PPLFailedRequestCountBySysErr`	Numero di richieste all'API `_ppl` non riuscite a causa di un problema del server o di una limitazione della funzionalità. Ad esempio, una richiesta potrebbe restituire il codice di stato HTTP 503 a causa di un `VerificationException` .
`PPLRequestCount`	Il numero di richieste all'API `_ppl`.

Monitoraggio dei OpenSearch log con Amazon CloudWatch Logs

Amazon OpenSearch Service espone i seguenti OpenSearch log tramite Amazon CloudWatch Logs:

- Log di errore
- Registri lenti delle richieste di ricerca

- Condividi gli slow log
- Log di verifica

Gli slow log degli shard di ricerca, gli slow log di indicizzazione degli shard e i log degli errori sono utili per la risoluzione dei problemi di prestazioni e stabilità. I log di verifica tengono traccia dell'attività degli utenti a fini di conformità Tutti i log sono disabilitati per impostazione predefinita. Se abilitata, si applica la tariffa standard. CloudWatch

> **Note**
>
> I log degli errori sono disponibili solo per le versioni 5.1 OpenSearch e successive di Elasticsearch. Gli slow log sono disponibili per tutte OpenSearch le versioni e per quelle di Elasticsearch.

Per i suoi log, OpenSearch utilizza Apache Log4j 2 e i suoi livelli di registro incorporati (dal più basso al più severo) di`TRACE`,,, e. `DEBUG` `INFO` `WARN` `ERROR` `FATAL`

Se abiliti i log degli errori, OpenSearch Service pubblica le righe di registro di, e to. `WARN` `ERROR` `FATAL` CloudWatch OpenSearch Il servizio pubblica anche diverse eccezioni dal `DEBUG` livello, tra cui le seguenti:

- `org.opensearch.index.mapper.MapperParsingException`
- `org.opensearch.index.query.QueryShardException`
- `org.opensearch.action.search.SearchPhaseExecutionException`
- `org.opensearch.common.util.concurrent.OpenSearchRejectedExecutionException`
- `java.lang.IllegalArgumentException`

I log di errore possono aiutarti con la risoluzione dei problemi in molti casi, tra cui i seguenti:

- Problemi di compilazione di script Painless
- Query non valide
- Problemi di indicizzazione
- Snapshot non riuscite
- Errori di migrazione di Index State Management

Argomenti

Abilitazione della pubblicazione di log (console)

La console OpenSearch di servizio è il modo più semplice per abilitare la pubblicazione dei log su. CloudWatch

Per abilitare la pubblicazione dei log su CloudWatch (console)

1. Andare all'indirizzo https://aws.amazon.com e quindi scegliere Sign In to the Console (Accedi alla console).
2. In Analytics, scegli Amazon OpenSearch Service.
3. Selezionare il dominio da aggiornare.
4. Nella scheda Log, seleziona un tipo di log e scegli Abilita.
5. Crea un nuovo gruppo di CloudWatch log o scegline uno esistente.

   > **Note**
   >
   > Se si pianifica di abilitare molteplici log, consigliamo di pubblicarli ognuno sul proprio gruppo di log. Questa separazione rende più semplice analizzare i log.

6. Scegliere una policy d'accesso che contiene le autorizzazioni appropriate oppure creare una policy utilizzando il formato JSON che la console offre:

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

```
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn:*"
    }
  ]
}
```

Si consiglia di aggiungere le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` alla policy per proteggersi dal problema del "confused deputy". L'account fonte è il proprietario del flusso di log e l'ARN fonte è l'ARN del dominio. Per aggiungere queste chiavi di condizione, il dominio deve trovarsi sul software di servizio R20211203 o versioni successive.

Ad esempio, è possibile aggiungere il seguente blocco di condizione alla policy:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

> **Important**
>
> CloudWatch Logs supporta 10 politiche di risorse per regione. Se si prevede di abilitare i log per diversi domini di OpenSearch servizio, è necessario creare e riutilizzare una politica più ampia che includa più gruppi di log per evitare di raggiungere questo limite. Per le fasi dell'aggiornamento della policy, consulta the section called “Abilitazione della pubblicazione di log (AWS CLI)”.

7. Scegli Abilita .

Lo stato del dominio cambia da Attivo a Elaborazione. Lo stato deve tornare su Attivo prima che venga abilitata la pubblicazione dei log. Questa modifica richiede in genere 30 minuti, ma può richiedere più tempo a seconda della configurazione del dominio.

Se hai abilitato uno degli shard slow log, vedi. the section called “Impostazione di soglie di slow log condivise” Se sono stati abilitati i log di verifica, consultare the section called “Passaggio 2: attiva i registri di controllo nelle dashboard OpenSearch ”. Se sono stati abilitati solo i log di errore, non è necessario eseguire operazioni di configurazione aggiuntive.

Abilitazione della pubblicazione di log (AWS CLI)

Prima di poter abilitare la pubblicazione dei log, è necessario un gruppo di CloudWatch log. Se non se ne dispone già di uno, è possibile crearlo utilizzando il comando seguente:

```
aws logs create-log-group --log-group-name my-log-group
```

Immettere il comando successivo per individuare l'ARN del gruppo di log e quindi annotarlo:

```
aws logs describe-log-groups --log-group-name my-log-group
```

Ora puoi concedere al OpenSearch servizio le autorizzazioni di scrittura nel gruppo di log. È necessario indicare l'ARN del gruppo di log vicino al termine 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 supporta 10 politiche di risorse per regione. Se prevedi di abilitare gli shard slow log per diversi domini di OpenSearch servizio, dovresti creare e riutilizzare una politica più ampia che includa più gruppi di log per evitare di raggiungere questo limite.

Se è necessario rivedere questa policy in un secondo momento, utilizza il comando `aws logs describe-resource-policies`. Per aggiornare la policy, esegui lo stesso comando `aws logs put-resource-policy` con un nuovo documento di policy.

Infine, è possibile utilizzare l'opzione `--log-publishing-options` per abilitare la pubblicazione. La sintassi dell'opzione è identica per entrambi i comandi `create-domain` e `update-domain-config`.

Parametro	Valori validi
`--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**
>
> Se si pianifica di abilitare molteplici log, consigliamo di pubblicarli ognuno sul proprio gruppo di log. Questa separazione rende più semplice analizzare i log.

Esempio

L'esempio seguente consente la pubblicazione di slow log degli shard di ricerca e indicizzazione per il dominio specificato:

```
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}"
```

Per disabilitare la pubblicazione su CloudWatch, esegui lo stesso comando con. `Enabled=false`

Se hai abilitato uno degli slow log dello shard, vedi. the section called “Impostazione di soglie di slow log condivise” Se sono stati abilitati i log di verifica, consultare the section called “Passaggio 2: attiva i registri di controllo nelle dashboard OpenSearch ”. Se sono stati abilitati solo i log di errore, non è necessario eseguire operazioni di configurazione aggiuntive.

Abilitazione della pubblicazione di log (SDK AWS)

Prima di poter abilitare la pubblicazione dei log, è necessario creare un gruppo di CloudWatch log, ottenerne l'ARN e concedere al OpenSearch Service le autorizzazioni di scrittura su di esso. Le operazioni pertinenti sono documentate nell'Amazon CloudWatch Logs API Reference:

- `CreateLogGroup`
- `DescribeLogGroup`
- `PutResourcePolicy`

È possibile accedere a tali operazioni utilizzando gli SDK AWS.

Gli AWS SDK (ad eccezione degli SDK per Android e iOS) supportano tutte le operazioni definite nell'Amazon OpenSearch Service API Reference, inclusa l'`--log-publishing-options`opzione per `CreateDomain` e. `UpdateDomainConfig`

Se hai abilitato uno degli slow log degli shard, vedi. the section called “Impostazione di soglie di slow log condivise” Se sono stati abilitati solo i log di errore, non è necessario eseguire operazioni di configurazione aggiuntive.

Abilitazione della pubblicazione di log (CloudFormation)

In questo esempio, creiamo CloudFormation un gruppo di log chiamato`opensearch-logs`, assegniamo le autorizzazioni appropriate e quindi creiamo un dominio con la pubblicazione dei log abilitata per i log delle applicazioni, gli slow log degli shard di ricerca e gli slow log di indicizzazione.

Prima di poter abilitare la pubblicazione dei log, è necessario creare un gruppo di log: CloudWatch

```
Resources:
```

```
  OpenSearchLogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: opensearch-logs
Outputs:
  Arn:
    Value:
      'Fn::GetAtt':
        - OpenSearchLogGroup
        - Arn
```

Il modello emette l'ARN del gruppo di log. In questo caso, l'ARN è `arn:aws:logs:us-east-1:123456789012:log-group:opensearch-logs`.

Utilizzando l'ARN, create una politica delle risorse che dia al OpenSearch servizio le autorizzazioni di scrittura nel gruppo di log:

```
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:*\"}]}"
```

Infine, crea il seguente CloudFormation stack, che genera un dominio di OpenSearch servizio con pubblicazione dei log. La politica di accesso consente all'utente di Account AWS effettuare tutte le richieste 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
```

Per informazioni dettagliate sulla sintassi, consultare Opzioni di pubblicazione dei log nella Guida per l'utente di AWS CloudFormation

Impostazione delle soglie di slow log delle richieste di ricerca

Gli slow log delle richieste di ricerca sono disponibili per la ricerca nei domini di OpenSearch servizio in esecuzione nella versione 2.13 e successive. Le soglie di slow log delle richieste di ricerca sono configurate per il tempo totale impiegato dalla richiesta. Ciò è diverso dagli slow log delle richieste di shard, che sono configurati in base al tempo impiegato dai singoli shard.

È possibile specificare gli slow log delle richieste di ricerca con le impostazioni del cluster. Ciò è diverso dagli shard slow log, che puoi abilitare con le impostazioni dell'indice. Ad esempio, puoi specificare le seguenti impostazioni tramite l' OpenSearch API REST:

```
PUT domain-endpoint/_cluster/settings
```

```
{
  "transient": {
    "cluster.search.request.slowlog.threshold.warn": "5s",
    "cluster.search.request.slowlog.threshold.info": "2s"
  }
}
```

Impostazione di soglie di slow log condivise

OpenSearch disabilita gli slow log degli shard per impostazione predefinita. Dopo aver abilitato la pubblicazione degli shard slow log su CloudWatch, è comunque necessario specificare le soglie di registrazione per ogni indice. OpenSearch Queste soglie definiscono esattamente cosa deve essere registrato e a quale livello di log.

Ad esempio, puoi specificare queste impostazioni tramite l'API REST: OpenSearch

```
PUT domain-endpoint/index/_settings
{
  "index.search.slowlog.threshold.query.warn": "5s",
  "index.search.slowlog.threshold.query.info": "2s"
}
```

Test degli slow log

Per verificare che sia la richiesta di ricerca che gli shard slow log vengano pubblicati correttamente, è consigliabile iniziare con valori molto bassi per verificare che i log vengano visualizzati CloudWatch, e quindi aumentare le soglie portandole a livelli più utili.

Se i log non vengono visualizzati, verificare quanto segue:

- Il gruppo di log esiste? CloudWatch Controlla la CloudWatch console.
- Il OpenSearch servizio dispone delle autorizzazioni per scrivere nel gruppo di log? Controlla la console OpenSearch di servizio.
- Il dominio del OpenSearch servizio è configurato per la pubblicazione nel gruppo di log? Controlla la console di OpenSearch servizio, utilizza l' AWS CLI `describe-domain-config`opzione o chiama `DescribeDomainConfig` utilizzando uno degli SDK.
- Le soglie OpenSearch di registrazione sono sufficientemente basse da consentire alle tue richieste di superarle?

Per esaminare le soglie di slow log della richiesta di ricerca per un dominio, usa il seguente comando:

```
GET domain-endpoint/_cluster/settings?flat_settings
```

Per esaminare le soglie di slow log dello shard per un indice, utilizzate il seguente comando:

```
GET domain-endpoint/index/_settings?pretty
```

Se desideri disattivare i log di query lente per un indice, ripristinare le soglie modificate sul valore predefinito di `-1`.

La disattivazione della pubblicazione per l' CloudWatch utilizzo della console di OpenSearch servizio o AWS CLI non OpenSearch impedisce la generazione dei log; interrompe solo la pubblicazione di tali registri. Assicurati di controllare le impostazioni dell'indice se non hai più bisogno degli shard slow log e le impostazioni del dominio se non hai più bisogno degli slow log della richiesta di ricerca.

Visualizzazione dei registri

Visualizzare l'applicazione e gli slow log in CloudWatch è come visualizzare qualsiasi altro registro. CloudWatch Per ulteriori informazioni, consulta View Log Data nella Amazon CloudWatch Logs User Guide.

Di seguito sono elencate alcune considerazioni per la visualizzazione dei log:

- OpenSearch Il servizio pubblica solo i primi 255.000 caratteri di ogni riga su. CloudWatch Il contenuto rimanente viene troncato. Per i log di verifica, sono possibili 10.000 caratteri per messaggio.
- In CloudWatch, i nomi dei flussi di registro hanno il suffisso`-index-slow-logs`, `-search-slow-logs-application-logs`, e `-audit-logs` per facilitare l'identificazione del contenuto.

Monitoraggio dei log di controllo in Amazon Service OpenSearch

Se il tuo dominio Amazon OpenSearch Service utilizza un controllo granulare degli accessi, puoi abilitare i log di controllo per i tuoi dati. I log di controllo sono altamente personalizzabili e ti consentono di tenere traccia delle attività degli utenti sui tuoi OpenSearch cluster, compresi i successi

e gli errori di autenticazione, le richieste, le modifiche all'indice e le query di ricerca in OpenSearch arrivo. La configurazione predefinita tiene traccia di una serie comune di azioni utente, ma si consiglia di personalizzare le impostazioni in base alle proprie esigenze.

Proprio come i log OpenSearch delle applicazioni e gli slow log, Service pubblica i log di controllo su Logs. OpenSearch CloudWatch Se abilitato, si applica il prezzo standard. CloudWatch

> **Note**
>
> Per abilitare i log di controllo, il ruolo utente deve essere mappato al `security_manager` ruolo, che consente di accedere all'API OpenSearch `plugins/_security` REST. Per ulteriori informazioni, consulta the section called “Modifica dell'utente principale”.

Argomenti

Limitazioni

I log di verifica hanno le seguenti limitazioni:

- I log di verifica non includono le richieste della ricerca tra cluster rifiutate dalla policy di accesso al dominio della destinazione.
- La dimensione massima di ogni messaggio del log di verifica è 10.000 caratteri. Il messaggio del log di verifica viene troncato se supera questo limite.

Abilitazione dei log di verifica

La procedura per abilitare i log di verifica prevede due fasi: Innanzitutto, configuri il tuo dominio per pubblicare i log di controllo in Logs. CloudWatch Quindi, abiliti i registri di controllo nelle OpenSearch dashboard e li configuri in base alle tue esigenze.

> **Important**
>
> Se si verifica un errore durante la procedura descritta di seguito, consultare the section called "Impossibile abilitare i log di verifica" per informazioni sulla risoluzione dei problemi.

Passaggio 1: abilitare i log di verifica e configurare una policy di accesso

In questi passaggi viene descritto come abilitare i log di verifica tramite la console. Puoi anche abilitarli utilizzando o AWS CLI l'API di OpenSearch servizio.

Per abilitare i registri di controllo per un dominio OpenSearch di servizio (console)

1. Scegliere il dominio per aprire la sua configurazione, quindi andare alla scheda Log.
2. Selezionare Audit logs (Log di verifica) e poi Enable (Abilita).
3. Crea un gruppo di CloudWatch log o scegline uno esistente.
4. Scegliere una policy d'accesso che contiene le autorizzazioni appropriate oppure creare una policy utilizzando il formato JSON che la console offre:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn"
    }
  ]
```

```
}
```

Si consiglia di aggiungere le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` alla policy per proteggersi dal problema del "confused deputy". L'account fonte è il proprietario del flusso di log e l'ARN fonte è l'ARN del dominio. Per aggiungere queste chiavi di condizione, il dominio deve trovarsi sul software di servizio R20211203 o versioni successive.

Ad esempio, è possibile aggiungere il seguente blocco di condizione alla policy:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

5. Scegli Abilita .

Passaggio 2: attiva i registri di controllo nelle dashboard OpenSearch

Dopo aver abilitato i registri di controllo nella console di OpenSearch servizio, devi abilitarli anche nelle OpenSearch dashboard e configurarli in base alle tue esigenze.

1. Apri OpenSearch Dashboard e scegli Sicurezza dal menu a sinistra.
2. Scegliere Log di verifica.
3. Scegliere Abilita registrazione di verifica.

L'interfaccia utente di Dashboards offre il controllo completo delle impostazioni del log di verifica in Impostazioni generali e Impostazioni di conformità. Per una descrizione di tutte le opzioni di configurazione, consultare Impostazioni dei log di verifica.

Abilita la registrazione di controllo utilizzando il AWS CLI

Il AWS CLI comando seguente abilita i registri di controllo su un dominio esistente:

```
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}"
```

È inoltre possibile abilitare i log di verifica quando si crea un dominio. Per ulteriori informazioni, consultare Riferimento ai comandi AWS CLI.

Abilitare la registrazione di controllo tramite l'API di configurazione

La seguente richiesta all'API di configurazione abilita i log di verifica su un dominio esistente:

```
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
    }
  }
}
```

Per ulteriori informazioni, consulta il riferimento all'API OpenSearch di Amazon Service.

Livelli e categorie dei log di verifica

La comunicazione del cluster avviene su due livelli separati: il livello REST e il livello di trasporto.

- Il livello REST copre la comunicazione con i client HTTP come curl, Logstash, OpenSearch Dashboards, il client REST di alto livello Java, la libreria Python Requests, tutte le richieste HTTP che arrivano al cluster.
- Il livello di trasporto copre la comunicazione tra i nodi. Ad esempio, dopo che una richiesta di ricerca arriva al cluster (sul livello REST), il nodo di coordinamento che serve la richiesta invia la query ad altri nodi, riceve le risposte, raccoglie i documenti necessari e li unisce nella risposta finale. Operazioni come l'allocazione delle partizioni e il ribilanciamento si verificano anche sul livello di trasporto.

È possibile abilitare o disabilitare i log di verifica per interi livelli, nonché per singole categorie di controllo per un livello. La tabella seguente contiene un riepilogo delle categorie di verifica e dei livelli per i quali sono disponibili.

Categoria	Descrizione	Disponibile per REST	Disponibile per il trasporto
FALLITO_LOGIN	Una richiesta conteneva credenziali non valide e l'autenticazione non è riuscita.	Sì	Sì
MISSING_PRIVILEGES	Un utente non disponeva dei privilegi per effettuare la richiesta.	Sì	Sì
GRANTED_PRIVILEGES	Un utente disponeva dei privilegi per effettuare la richiesta.	Sì	Sì
OPENSEARCH_SECURITY_INDEX_ATTEMPT	Una richiesta ha provato a modificare l'indice `.opendistro_security` .	No	Sì
AUTHENTICATED	Una richiesta conteneva credenziali valide e l'autenticazione è riuscita.	Sì	Sì
INDEX_EVENT	Una richiesta ha eseguito un'operazione amministrativa su un indice, ad esempio la creazione , l'impostazione di un alias o l'esecuzione di un'unione forzata.	No	Sì

Categoria	Descrizione	Disponibile per REST	Disponibile per il trasporto
	L'elenco completo delle `indices:admin/` azioni incluse in questa categoria è disponibile nella documentazione. OpenSearch		

Oltre a queste categorie standard, il controllo granulare degli accessi offre diverse categorie aggiuntive progettate per soddisfare i requisiti di conformità dei dati.

Categoria	Descrizione
COMPLIANCE_DOC_READ	Una richiesta ha eseguito un evento di lettura su un documento in un indice.
COMPLIANCE_DOC_WRITE	Una richiesta ha eseguito un evento di scrittura su un documento in un indice.
COMPLIANCE_INTERNAL_CONFIG_READ	Una richiesta ha eseguito un evento di lettura sull'indice `.opendistro_security` .
COMPLIANCE_INTERNAL_CONFIG_WRITE	Una richiesta ha eseguito un evento di scrittura sull'indice `.opendistro_security` .

È possibile disporre di una combinazione di categorie e attributi di messaggio. Ad esempio, se si invia una richiesta REST per indicizzare un documento, è possibile che vengano visualizzate le seguenti righe nei log di verifica:

- AUTHENTICATED sul livello REST (autenticazione)
- GRANTED_PRIVILEGE a livello di trasporto (autorizzazione)

- COMPLIANCE_DOC_WRITE (documento scritto su un indice)

Impostazioni dei log di verifica

I log di verifica dispongono di numerose opzioni di configurazione.

Impostazioni generali

Le impostazioni generali consentono di abilitare o disabilitare singole categorie o interi livelli. Si consiglia vivamente di lasciare GRANTED_PRIVILES e AUTHENTICATED come categorie escluse. In caso contrario, queste categorie vengono registrate per ogni richiesta valida al cluster.

Nome	Impostazione del back-end	Descrizione
Livello REST	enable_rest	Abilitare o disabilitare gli eventi che si verificano sul livello REST.
Categorie REST disabilitate	disabled_rest_categories	Specificare le categorie di verifica da ignorare sul livello REST. La modifica di queste categorie può aumentare notevolmente le dimensioni dei log di verifica.
Livello di trasporto	enable_transport	Abilitare o disabilitare gli eventi che si verificano sul livello di trasporto.
Categorie di trasporto disabilitate	disabled_transport_categories	Specificare le categorie di verifica che devono essere ignorate sul livello di trasporto. La modifica di queste categorie può aumentare notevolmente le dimensioni dei log di verifica.

Le impostazioni degli attributi consentono di personalizzare la quantità di dettagli in ogni riga di log.

Nome	Impostazione del back-end	Descrizione
Richieste in blocco	resolve_bulk_requests	L'abilitazione di questa impostazione genera un log per ogni documento in una richiesta in blocco, che può aumentare notevolmente le dimensioni dei log di verifica.
Corpo della richiesta	log_request_body	Includere il corpo della richiesta delle richieste.
Risoluzione di indici	resolve_indices	Risolvere gli alias sugli indici.

Utilizzare Ignora impostazioni per escludere un set di utenti o percorsi API:

Nome	Impostazione del back-end	Descrizione
Utenti ignorati	ignore_users	Specificare gli utenti che si desidera escludere.
Richieste ignorate	ignore_requests	Specificare i modelli di richiesta che si desidera escludere.

Impostazioni di conformità

Le impostazioni di conformità consentono di regolare l'accesso a livello di indice, documento o campo.

Nome	Impostazione del back-end	Descrizione
Registrazione della conformità	enable_compliance	Abilitare o disabilitare la registrazione della conformità.

È possibile specificare le seguenti impostazioni per la registrazione degli eventi di lettura e scrittura.

Nome	Impostazione del back-end	Descrizione
Registrazione della configurazione interna	internal_config	Abilitare o disabilitare la registrazione degli eventi sull'indice `.opendistro_security` .

È possibile specificare le seguenti impostazioni per gli eventi di lettura.

Nome	Impostazione del back-end	Descrizione
Lettura di metadati	read_metadata_only	Includere solo i metadati per gli eventi di lettura. Non includere campi di documento.
Utenti ignorati	read_ignore_users	Non includere determinati utenti per gli eventi di lettura.
Campi osservati	read_watched_fields	Specificare gli indici e i campi da controllare per gli eventi di lettura. L'aggiunta di campi controllati genera un log per accesso ai documenti, che può aumentare notevolmente le dimensioni dei log di verifica. I campi osservati supportano i modelli di indice e i modelli di campo: `{ "index-name-pattern": [ "field-name-pattern" ], "logs*": [ "message" ], "twitter": [ "id", "user*" ] }`

È possibile specificare le seguenti impostazioni per gli eventi di scrittura.

Nome	Impostazione del back-end	Descrizione
Scrittura di metadati	write_metadata_only	Includere solo i metadati per gli eventi di scrittura. Non includere campi di documento.
Differenze dei log	write_log_diffs	Se write_metadata_only è false, includere solo le differenze tra gli eventi di scrittura.
Utenti ignorati	write_ignore_users	Non includere determinati utenti per gli eventi di scrittura.
Osservazione di indici	write_watched_indices	Specificare gli indici o i modelli di indice da controllare per gli eventi di scrittura. L'aggiunta di campi controllati genera un log per accesso ai documenti, che può aumentare notevolmente le dimensioni dei log di verifica.

Esempi di log di verifica

Questa sezione include una configurazione di esempio, una richiesta di ricerca e il log di verifica risultante per tutti gli eventi di lettura e scrittura di un indice.

Fase 1: Configurazione dei log di verifica

Dopo aver abilitato la pubblicazione dei log di controllo in un gruppo CloudWatch Logs, accedi alla pagina di registrazione di audit di OpenSearch Dashboards e scegli Abilita registrazione di controllo.

1. In Impostazioni generali, scegliere Configura e assicurarsi che il livello REST sia abilitato.
2. In Impostazioni di conformità, scegliere Configura.
3. In Scrittura, in Campi osservati, aggiungere `accounts` per tutti gli eventi di scrittura su questo indice.
4. In Lettura, in Campi osservati, aggiungere i campi `ssn` e `id-` dell'indice `accounts`:

```
{
  "accounts-": [
    "ssn",
```

```
    "id-"
  ]
}
```

Fase 2: Esecuzione di eventi di lettura e scrittura

1. Passa a OpenSearch Dashboards, scegli Dev Tools e indicizza un documento di esempio:

```
PUT accounts/_doc/0
{
  "ssn": "123",
  "id-": "456"
}
```

2. Per verificare un evento di lettura, inviare la seguente richiesta:

```
GET accounts/_search
{
  "query": {
    "match_all": {}
  }
}
```

Fase 3: Osservazione dei log

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, selezionare Log groups (Gruppi di log).
3. Scegliere il gruppo di log specificato durante l'abilitazione dei log di verifica. All'interno del gruppo di log, OpenSearch Service crea un flusso di log per ogni nodo del dominio.
4. In Flussi di log, scegliere Cerca tutto.
5. Per gli eventi di lettura e scrittura, consultare i log corrispondenti. È possibile prevedere un ritardo di 5 secondi prima che venga visualizzato il log.

   Log di verifica della scrittura di esempio

```
{
  "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"
  ]
}
```

Log di verifica della lettura di esempio

```
{
  "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"
  ]
}
```

Per includere il corpo della richiesta, torna alle impostazioni di conformità nei OpenSearch dashboard e disabilita Write metadata. Per escludere eventi da un utente specifico, aggiungere l'utente a Utenti ignorati.

Per una descrizione di ogni campo del log di verifica, consultare Riferimento ai campi dei log di verifica. Per informazioni sulla ricerca e l'analisi dei dati dei log di controllo, consulta Analyzing Log Data with CloudWatch Logs Insights nella Amazon CloudWatch Logs User Guide.

Configurazione dei log di verifica tramite la REST API

Ti consigliamo di utilizzare OpenSearch le dashboard per configurare i log di controllo, ma puoi anche utilizzare l'API REST per il controllo degli accessi a grana fine. In questa sezione è riportata una richiesta di esempio. La documentazione completa sull'API REST è disponibile nella documentazione. OpenSearch

```
PUT _opendistro/_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"
    ]
  }
}
```

Monitoraggio degli eventi del OpenSearch servizio con Amazon EventBridge

Amazon OpenSearch Service si integra con Amazon EventBridge per notificarti determinati eventi che influiscono sui tuoi domini. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Gli stessi eventi vengono inviati anche ad Amazon CloudWatch Events, il predecessore di Amazon EventBridge. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali azioni automatizzate intraprendere quando un evento corrisponde a una regola. Le azioni che possono essere attivate automaticamente includono le seguenti:

- Invocare una funzione AWS Lambda
- Richiamo di un Run Command di Amazon EC2
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un argomento Amazon SNS o di una coda Amazon SQS

Per ulteriori informazioni, consulta la sezione Guida introduttiva ad Amazon EventBridge nella Amazon EventBridge User Guide.

Argomenti

Eventi di aggiornamento del software di servizio

OpenSearch Il servizio invia eventi EventBridge quando si verifica uno dei seguenti eventi di aggiornamento del software di servizio.

Aggiornamento del software di servizio disponibile

OpenSearch Il servizio invia questo evento quando è disponibile un aggiornamento del software di servizio.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
```

```
  "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"
  }
}
```

Aggiornamento del software di servizio pianificato

OpenSearch Il servizio invia questo evento quando è stato pianificato un aggiornamento del software di servizio. Per gli aggiornamenti opzionali, si riceve la notifica nella data pianificata e si ha la possibilità di riprogrammarli in qualsiasi momento. Per gli aggiornamenti richiesti, ricevi la notifica tre giorni prima della data pianificata e hai la possibilità di riprogrammarla entro la finestra obbligatoria.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Aggiornamento del software di servizio riprogrammato

OpenSearch Il servizio invia questo evento quando un aggiornamento opzionale del software di servizio viene riprogrammato. Per ulteriori informazioni, consulta the section called “Aggiornamenti facoltativi e aggiornamenti obbligatori”.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
```

```
}
```

Aggiornamento del software di servizio avviato

OpenSearch Il servizio invia questo evento quando viene avviato un aggiornamento del software di servizio.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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.
  }
}
```

Aggiornamento del software di servizio completato

OpenSearch Il servizio invia questo evento quando viene completato un aggiornamento del software di servizio.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Aggiornamento del software di servizio annullato

OpenSearch Il servizio invia questo evento quando un aggiornamento del software di servizio viene annullato.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Aggiornamento programmato del software di servizio annullato

OpenSearch Il servizio invia questo evento quando un aggiornamento del software di servizio precedentemente pianificato per il dominio è stato annullato.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Aggiornamento del software di servizio non eseguito

OpenSearch Il servizio invia questo evento quando non è in grado di avviare un aggiornamento del software di servizio.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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]"
  }
}
```

Aggiornamento del software di servizio non riuscito

OpenSearch Il servizio invia questo evento quando un aggiornamento del software di servizio fallisce.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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].
  }
}
```

Aggiornamento del software di servizio richiesto

OpenSearch Il servizio invia questo evento quando è richiesto un aggiornamento del software di servizio. Per ulteriori informazioni, consulta the section called “Aggiornamenti facoltativi e aggiornamenti obbligatori”.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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"
  }
}
```

Eventi di regolazione automatica

OpenSearch Il servizio invia eventi EventBridge quando si verifica uno dei seguenti eventi Auto-Tune.

Regolazione automatica in sospeso

OpenSearch Il servizio invia questo evento quando Auto-Tune ha identificato i consigli di ottimizzazione per migliorare le prestazioni e la disponibilità del cluster. Questo evento verrà visualizzato solo per i domini con la regolazione automatica disabilitata.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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}"
  }
}
```

Regolazione automatica avviata

OpenSearch Il servizio invia questo evento quando Auto-Tune inizia ad applicare nuove impostazioni al dominio.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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%}."
  }
}
```

La regolazione automatica richiede una implementazione blu/verde pianificata

OpenSearch Il servizio invia questo evento quando Auto-Tune ha identificato consigli di ottimizzazione che richiedono un'implementazione pianificata blu/verde.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Regolazione automatica annullata

OpenSearch Il servizio invia questo evento quando la pianificazione di Auto-Tune è stata annullata perché non ci sono consigli di ottimizzazione in sospeso.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Regolazione automatica completata

OpenSearch Il servizio invia questo evento quando Auto-Tune ha completato la distribuzione blu/verde e il cluster è operativo con le nuove impostazioni JVM.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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%}."
  }
}
```

Regolazione automatica disabilitata e modifiche ripristinate

OpenSearch Il servizio invia questo evento quando Auto-Tune è stato disabilitato e le modifiche applicate sono state ripristinate.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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}"
  }
}
```

Regolazione automatica disabilitata e modifiche conservate

OpenSearch Il servizio invia questo evento quando Auto-Tune è stato disabilitato e le modifiche applicate sono state mantenute.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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}"
  }
}
```

Eventi sull'integrità del cluster

OpenSearch Il servizio invia determinati eventi EventBridge quando lo stato del cluster è compromesso.

Avviato il recupero del cluster rosso

OpenSearch Il servizio invia questo evento dopo che lo stato del cluster è rimasto ininterrottamente in rosso per più di un'ora. Tenta di ripristinare automaticamente uno o più indici rossi da uno snapshot per correggere lo stato del cluster.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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]"
   }
}
```

Recupero del cluster rosso parzialmente completato

OpenSearch Il servizio invia questo evento quando è stato in grado di ripristinare solo un sottoinsieme di indici rossi da un'istantanea durante il tentativo di correggere lo stato di un cluster rosso.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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."
   }
}
```

Recupero del cluster rosso non riuscito

OpenSearch Il servizio invia questo evento quando non riesce a ripristinare alcun indice durante il tentativo di correggere lo stato di un cluster rosso.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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."
   }
}
```

Partizioni da eliminare

OpenSearch Il servizio invia questo evento quando tenta di correggere automaticamente lo stato del cluster rosso dopo che era rimasto in rosso ininterrottamente per 14 giorni, ma uno o più indici rimangono rossi. Dopo altri 7 giorni (21 giorni totali in cui il colore è continuamente rosso), il OpenSearch Servizio procede all'eliminazione degli shard non assegnati su tutti gli indici rossi.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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"
   }
}
```

Partizioni eliminate

OpenSearch Il servizio invia questo evento dopo che lo stato del cluster è rimasto in rosso ininterrottamente per 21 giorni. Si procede all'eliminazione delle partizioni non assegnate (archiviazione e calcolo) su tutti gli indici rossi. Per informazioni dettagliate, vedi the section called “Correzione automatico di cluster rossi”.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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"
   }
}
```

Avviso di conteggio di partizioni elevate

OpenSearch Il servizio invia questo evento quando il numero medio di shard negli hot data node ha superato il 90% del limite predefinito consigliato di 1.000. Sebbene le versioni successive di Elasticsearch OpenSearch supportino un limite massimo configurabile per il numero massimo di shard per nodo, consigliamo di non avere più di 1.000 shard per nodo. Vedi Scelta del numero di partizioni.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Superamento del limite del numero di partizioni

OpenSearch Il servizio invia questo evento quando il numero medio di shard nei nodi di hot data ha superato il limite predefinito consigliato di 1.000. Sebbene le versioni successive di Elasticsearch OpenSearch supportino un limite massimo configurabile per il numero massimo di shard per nodo, consigliamo di non avere più di 1.000 shard per nodo. Vedi Scelta del numero di partizioni.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
```

```
  }
}
```

Spazio su disco ridotto

OpenSearch Il servizio invia questo evento quando uno o più nodi del cluster hanno meno del 25% dello spazio di archiviazione disponibile o meno di 25 GB.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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"
  }
}
```

Violazione del watermark su disco ridotta

OpenSearch Il servizio invia questo evento quando tutti i nodi del cluster hanno meno del 10% dello spazio di archiviazione disponibile o meno di 10 GB. Quando tutti i nodi superano la soglia di esaurimento del disco, ogni nuovo indice genera un cluster giallo e, quando tutti i nodi scendono al di sotto del limite massimo del disco, viene visualizzato un cluster rosso.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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".
  }
}
```

Saldo di burst EBS inferiore al 70%

OpenSearch Il servizio invia questo evento quando il saldo del burst di EBS su uno o più nodi di dati scende al di sotto del 70%. L'esaurimento del saldo di burst EBS può causare una diffusa indisponibilità del cluster e la limitazione delle richieste di I/O, che possono portare a latenze e timeout elevati per le richieste di indicizzazione e ricerca. Per la procedura per correggere questo problema, consulta la sezione the section called “Saldo di burst EBS basso”.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Saldo di burst EBS inferiore al 20%

OpenSearch Il servizio invia questo evento quando il saldo del burst di EBS su uno o più nodi di dati scende al di sotto del 20%. L'esaurimento del saldo di burst EBS può causare una diffusa indisponibilità del cluster e la limitazione delle richieste di I/O, che possono portare a latenze e timeout elevati per le richieste di indicizzazione e ricerca. Per la procedura per correggere questo problema, consulta la sezione the section called “Saldo di burst EBS basso”.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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.
  }
}
```

Limitazione della velocità di trasmissione effettiva del disco

OpenSearch Il servizio invia questo evento quando le richieste di lettura e scrittura verso il dominio vengono limitate a causa delle limitazioni di throughput dei volumi EBS o dell'istanza EC2. Se ricevi questa notifica, valuta la possibilità di aumentare i volumi o le istanze seguendo le best practice consigliate. AWS Se il tipo di volume è`gp2`, aumenta la dimensione del volume. Se il tipo di volume è lo stesso`gp3`, fornisci una maggiore velocità effettiva. Puoi anche verificare che la base dell'istanza e il throughput EBS massimo siano maggiori o uguali al throughput di volume assegnato e aumentare di conseguenza.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
   }
}
```

Frammenti di grandi dimensioni

OpenSearch Il servizio invia questo evento quando uno o più shard nel cluster hanno superato i 50 GiB o i 65 GiB. Per garantire prestazioni e stabilità ottimali del cluster, riduci le dimensioni degli shard.

Per ulteriori informazioni, consulta le migliori pratiche di sharding.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Elevato utilizzo JVM

OpenSearch Il servizio invia questo evento quando la `JVMMemoryPressure` metrica per il tuo dominio ha superato l'80%. Se supera il 92% per 30 minuti, tutte le operazioni di scrittura sul cluster verranno bloccate. Per garantire una stabilità ottimale del cluster, riduci il traffico verso il cluster o ridimensiona il dominio per fornire memoria sufficiente per il carico di lavoro.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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 insufficiente

OpenSearch Il servizio invia questo evento quando la JVM massima è superiore al 70% e la differenza tra il massimo e il minimo è inferiore al 30%. Ciò può indicare che la JVM non è in grado di recuperare memoria sufficiente durante i cicli di raccolta dei rifiuti per il carico di lavoro. Ciò può portare a risposte sempre più lente e latenze più elevate e, in alcuni casi, persino a cadute dei nodi a causa dei controlli di integrità scaduti. Per garantire una stabilità ottimale del cluster, riduci il traffico verso il cluster o ridimensiona il dominio per fornire memoria sufficiente per il carico di lavoro.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Avviso di routing dell'indice personalizzato

OpenSearch Il servizio invia questo evento quando il dominio è in stato di elaborazione e contiene indici con impostazioni index.routing.allocation personalizzate che possono causare il blocco delle distribuzioni blu-verdi. Verifica che le impostazioni siano applicate correttamente.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
```

```
  }
}
```

Shard lock non riuscito

OpenSearch Il servizio invia questo evento quando il dominio non è integro a causa di shard non assegnati con. `[ShardLockObtainFailedException]` Per ulteriori informazioni, consulta Come posso risolvere l'eccezione dello shard lock in memoria in Amazon OpenSearch Service?

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
}
```

Eventi di endpoint VPC

OpenSearch Il servizio invia determinati eventi agli endpoint EventBridge correlati all'AWS PrivateLink interfaccia.

Creazione dell'endpoint VPC non riuscita

OpenSearch Il servizio invia questo evento quando non è in grado di creare un endpoint VPC richiesto. Questo errore potrebbe verificarsi perché hai raggiunto il limite del numero di endoint

VPC consentiti all'interno di una regione. Questo errore verrà visualizzato anche se non esiste una sottorete o un gruppo di sicurezza specificato.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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."
   }
}
```

Aggiornamento dell'endpoint VPC non riuscito

OpenSearch Il servizio invia questo evento quando non è in grado di eliminare un endpoint VPC richiesto.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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>."
   }
}
```

Eliminazione dell'endpoint VPC non riuscita

OpenSearch Il servizio invia questo evento quando non è in grado di eliminare un endpoint VPC richiesto.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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."
```

```
    }
}
```

Eventi di ritiro dei nodi

OpenSearch Il servizio invia gli eventi EventBridge quando si verifica uno dei seguenti eventi di ritiro del nodo.

Ritiro del nodo pianificato

OpenSearch Il servizio invia questo evento quando è stato pianificato il ritiro di un nodo.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Ritiro del nodo completato

OpenSearch Il servizio invia questo evento quando il ritiro di un nodo è completato.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Ritiro del nodo non riuscito

OpenSearch Il servizio invia questo evento quando il ritiro di un nodo fallisce.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
```

```
  }
}
```

Eventi di ritiro dei nodi degradati

OpenSearch Il servizio invia questi eventi quando è necessaria la sostituzione di un nodo a causa di un hardware danneggiato su un nodo.

Notifica di ritiro del nodo danneggiato

OpenSearch Il servizio invia questo evento quando l'azione automatica di ritiro e sostituzione di un nodo danneggiato è stata pianificata per il dominio.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "version":"0",
   "id":"db233454-aad1-7676-3b15-10a84b052baa",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T08:16:06Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"An automated action to retire and replace a node has
 been scheduled on your domain. For more information, please see https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/monitoring-events.html.",
      "event":"Degraded Node Retirement Notification",
      "status":"Scheduled"
   }
}
```

Ritiro del nodo degradato completato

OpenSearch Il servizio invia questo evento quando un nodo danneggiato viene ritirato e sostituito con un nuovo nodo.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "version":"0",
   "id":"7444215c-90f9-a52d-bcda-e85973a9a762",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T10:20:30Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"The node has been retired and replaced with a new node.",
      "event":"Degraded Node Retirement Notification",
      "status":"Completed"
   }
}
```

Ritiro del nodo danneggiato non riuscito

OpenSearch Il servizio invia questo evento se il ritiro del nodo danneggiato non riesce.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "version":"0",
   "id":"c328e9bb-93b9-c0b2-b17a-df527fdf96b6",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T08:31:38Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
```

```
      "severity":"Medium",
      "description":"Node retirement failed. No actions are required from your end. We
 will automatically re-try replacing the node.",
      "event":"Degraded Node Retirement Notification",
      "status":"Failed"
   }
}
```

Eventi di errore di dominio

OpenSearch Il servizio invia gli eventi EventBridge quando si verifica uno dei seguenti errori di dominio.

Errore di convalida dell'aggiornamento del dominio

OpenSearch Il servizio invia questo evento se rileva uno o più errori di convalida durante il tentativo di aggiornare o eseguire una modifica della configurazione su un dominio. Per risolvere questi errori, consulta the section called “Risoluzione degli errori di convalida”.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
   "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"
```

```
   }
}
```

Chiave KMS inaccessibile

OpenSearch Il servizio invia questo evento quando non può accedere alla tua chiave. AWS KMS

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
  "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."
  }
}
```

Isolamento del dominio

OpenSearch Il servizio invia questo evento quando il dominio diventa isolato e non può ricevere, leggere o scrivere richieste perché non è raggiungibile dalla rete.

Esempio

Di seguito è illustrato un evento di esempio di questo tipo:

```
{
```

```
  "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: ascolto degli EventBridge eventi OpenSearch di Amazon Service

In questo tutorial, configuri una semplice AWS Lambda funzione che ascolta gli eventi di Amazon OpenSearch Service e li scrive in un flusso di log di CloudWatch Logs.

Prerequisiti

Questo tutorial presuppone che tu disponga di un dominio Service esistente OpenSearch . Se non è stato creato un dominio, attenersi alla procedura descritta in Creazione e gestione dei domini per crearne uno.

Fase 1: Creazione della funzione Lambda

In questa procedura, si crea una semplice funzione Lambda che funga da destinazione per i messaggi degli eventi OpenSearch di servizio.

Per creare una funzione Lambda di destinazione

1. Apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Scegli Create function (Crea funzione) e Author from scratch (Crea da zero).
3. Per Nome funzione, immettere event-handler.

4. In Runtime, scegliere Python 3.8.
5. Scegli Crea funzione.
6. Nella sezione Function code (Codice della funzione), modifica il codice di esempio affinché corrisponda all'esempio seguente:

```
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))
```

   Questa è una semplice funzione Python 3.8 che stampa gli eventi inviati da Service. OpenSearch Se tutto è configurato correttamente, alla fine di questo tutorial, i dettagli dell'evento vengono visualizzati nel flusso di log CloudWatch Logs associato a questa funzione Lambda.
7. Seleziona Deploy (Implementa).

Fase 2: Registrazione di una regola di evento

In questo passaggio, crei una EventBridge regola che acquisisce gli eventi dai tuoi OpenSearch domini di servizio. Questa regola acquisisce tutti gli eventi all'interno dell'account in cui è definita. Gli stessi messaggi di evento contengono informazioni sull'origine dell'evento, tra cui il dominio da cui ha origine. È possibile utilizzare queste informazioni per filtrare e ordinare gli eventi a livello di programmazione.

Per creare una regola EventBridge

1. Apri la EventBridge console all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.
3. Assegnare alla regola il nome event-rule.
4. Seleziona Successivo.
5. Per lo schema dell'evento, seleziona AWS services, Amazon OpenSearch Service e All Events. Questo modello si applica a tutti i domini di OpenSearch servizio e a tutti gli eventi OpenSearch del servizio. In alternativa, è possibile creare una regola più specifica per filtrare alcuni risultati.
6. Premere Next (Successivo).

7. Per la destinazione, scegli Lambda function (Funzione Lambda). Nel menu a discesa della funzione, scegli event-handler.
8. Premere Next (Successivo).
9. Ignorare i tag e premere di nuovo Next (Successivo).
10. Rivedi la configurazione e scegli Create rule (Crea regola).

Fase 3: Test della configurazione

La prossima volta che ricevi una notifica nella sezione Notifiche della console di OpenSearch servizio, se tutto è configurato correttamente, la funzione Lambda viene attivata e scrive i dati dell'evento in un flusso di log di CloudWatch Logs per la funzione.

Per testare la configurazione

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, scegliere Log e selezionare il gruppo di log per la funzione Lambda (ad esempio /aws/lambda/event-handler).
3. Seleziona un flusso di log per visualizzare i dati di evento.

Esercitazione: Invio di avvisi Amazon SNS per gli aggiornamenti software disponibili

In questo tutorial, configuri una regola di EventBridge evento Amazon che acquisisce le notifiche per gli aggiornamenti del software di servizio disponibili in Amazon OpenSearch Service e ti invia una notifica e-mail tramite Amazon Simple Notification Service (Amazon SNS).

Prerequisiti

Questo tutorial presuppone che tu disponga di un dominio di servizio esistente OpenSearch . Se non è stato creato un dominio, attenersi alla procedura descritta in Creazione e gestione dei domini per crearne uno.

Fase 1: Creazione e sottoscrizione a un argomento Amazon SNS

Configurare un argomento Amazon SNS che funga da destinazione evento per la nuova regola di evento.

Per creare una destinazione Amazon SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Scegliere Argomenti e Crea argomento.
3. Per il tipo di processo, scegliere Standard e assegnare al processo il nome software-update.
4. Scegli Create topic (Crea argomento).
5. Una volta creato l'argomento, scegliere Crea una sottoscrizione.
6. Per Protocollo, scegli E-mail. In Endpoint, inserire un indirizzo e-mail a cui si ha accesso correntemente, quindi scegliere Crea sottoscrizione.
7. Controllare l'account e-mail e attendere di ricevere una e-mail di conferma della sottoscrizione. Una volta ricevuta, seleziona Confirm subscription (Conferma sottoscrizione).

Fase 2: Registrazione di una regola di evento

Quindi, registrare una regola di evento che acquisisca solo gli eventi di aggiornamento del software di servizio.

Per creare una regola di evento

1. Apri la EventBridge console all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.
3. Assegnare alla regola il nome softwareupdate-rule.
4. Seleziona Successivo.
5. Per lo schema dell'evento, seleziona AWS services, Amazon OpenSearch Service e Amazon OpenSearch Service Software Update Notification. Questo schema corrisponde a qualsiasi evento di aggiornamento del software di OpenSearch servizio fornito da Service. Per ulteriori informazioni sui pattern di eventi, consulta la pagina Amazon EventBridge Event Patterns nella Amazon EventBridge User Guide.
6. Facoltativamente, è possibile solo in base alle gravità specifiche. Per le gravità di ogni evento, consulta the section called “Eventi di aggiornamento del software di servizio”.
7. Seleziona Successivo.
8. Per destinazione, scegli SNS topic (Argomento SNS) e seleziona software-update.
9. Seleziona Successivo.
10. Ignora i tag e scegli Next (Successivo).

11. Rivedi la configurazione della regola e scegli Create rule (Crea regola).

La prossima volta che ricevi una notifica dal OpenSearch Servizio su un aggiornamento del software di servizio disponibile, se tutto è configurato correttamente, Amazon SNS dovrebbe inviarti un'e-mail di avviso sull'aggiornamento.

Monaggio delle chiamate API Amazon OpenSearch Service con AWS CloudTrail

Amazon OpenSearch Service è integrato conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un AWS servizio in OpenSearch Service. CloudTrailacquisisce le chiamate all'API di configurazione effettuate a OpenSearch Service as events.

> **Note**
>
> CloudTrailacquisisce solo le chiamate all'API di configurazione, ad esempio `CreateDomain` e`GetUpgradeStatus`. CloudTrailnon acquisisce le chiamate alle OpenSearchAPI, ad esempio `_search` e`_bulk`. Per queste chiamate, consultare the section called “Monitoraggio dei log di verifica”.

Le chiamate acquisite includono chiamate dalla console di OpenSearch servizio o un AWS SDK. AWS CLI Se si crea un trail, è possibile abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per OpenSearch Service. Se non configuri un trail, puoi comunque visualizzare gli eventi più recenti nella console CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da permettono CloudTrail di determinare la richiesta effettuata ad OpenSearch Service, l'indirizzo IP da cui è stata effettuata la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, consulta la Guida per l'utente di AWS CloudTrail.

Informazioni sul OpenSearch servizio Amazon in CloudTrail

CloudTrail è abilitato sull'Account AWS al momento della sua creazione. Quando si verifica un'attività in OpenSearch Service, questa viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti

nell'account Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'Account AWSaccount, inclusi gli eventi per OpenSearch Service, crea un trail. Un trail consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Creazione di un trail per il tuo Account AWS
- AWSintegrazioni di servizi con Logs CloudTrail
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni e Ricezione di file di log CloudTrail da più account

Tutte le operazioni dell'API di configurazione del OpenSearch servizio vengono registrate CloudTrail e sono documentate in Amazon OpenSearch Service.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente AWS Identity and Access Management (IAM) o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci del file di log Amazon OpenSearch Service

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail contengono una o più voci di log. Un evento rappresenta una singola richiesta da un'fonte e include informazioni sul operazione richiesta, data e ora dell'operazione, parametri richiesti e così via. I file di log di CloudTrail non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione `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"
}
```

Sicurezza in Amazon OpenSearch Service

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per maggiori informazioni sui programmi di conformità che si applicano ad Amazon OpenSearch Service, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza il OpenSearch Servizio. I seguenti argomenti mostrano come configurare il OpenSearch servizio per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse OpenSearch del Servizio.

Argomenti

- Utilizzo di ruoli collegati ai servizi per Amazon Service OpenSearch

Protezione dei dati in Amazon OpenSearch Service

Il modello di responsabilità AWS di si applica alla protezione dei dati in Amazon OpenSearch Service. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con OpenSearch Service o altro Servizi AWS utilizzando la console, l'API o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati inattivi per Amazon OpenSearch Service

OpenSearch I domini di servizio offrono la crittografia dei dati inattivi, una funzionalità di sicurezza che aiuta a prevenire l'accesso non autorizzato ai tuoi dati. La funzionalità utilizza AWS Key Management Service (AWS KMS) per archiviare e gestire le chiavi di crittografia e l'algoritmo Advanced Encryption Standard con chiavi a 256 bit (AES-256) per eseguire la crittografia. Se abilitata, la funzionalità crittografa gli elementi seguenti di un dominio:

- Tutti gli indici (compresi quelli archiviati) UltraWarm
- OpenSearch registri
- File di swap
- Tutti gli altri dati presenti nella directory dell'applicazione
- Snapshot automatici

Gli elementi seguenti non vengono crittografati quando abiliti la crittografia dei dati a riposo, ma puoi eseguire operazioni aggiuntive per proteggerli:

- Istantanee manuali: al momento non è possibile utilizzare AWS KMS le chiavi per crittografare le istantanee manuali. Tuttavia, è possibile usare la crittografia lato server con chiavi gestite da S3 o chiavi KMS per crittografare il bucket che si utilizza come repository degli snapshot. Per istruzioni, consultare the section called “Registrazione di un repository di snapshot manuali”.
- Slow log e log degli errori: se pubblichi log e desideri crittografarli, puoi crittografare il relativo gruppo di log CloudWatch Logs utilizzando la stessa chiave del dominio del servizio. AWS KMS OpenSearch Per ulteriori informazioni, consulta Encrypt log data in CloudWatch Logs using AWS KMS nella Amazon CloudWatch Logs User Guide.

> **Note**
>
> Non puoi abilitare la crittografia a riposo su un dominio esistente se UltraWarm sul dominio è abilitata la memorizzazione a freddo. È necessario innanzitutto UltraWarm disabilitare la memorizzazione a freddo, abilitare la crittografia a riposo e quindi riattivare UltraWarm la conservazione a freddo. Se si desidera conservare gli indici in una conservazione a caldo UltraWarm o a freddo, è necessario spostarli nella memorizzazione a caldo prima di UltraWarm disattivarli o archiviarli a freddo.

OpenSearch Il servizio supporta solo chiavi KMS con crittografia simmetrica, non asimmetriche. Per informazioni su come creare chiavi simmetriche, consultare Creazione di chiavi nella Guida per gli sviluppatori di AWS Key Management Service .

Indipendentemente dal fatto che la crittografia a riposo sia abilitata, tutti i domini crittografano automaticamente i pacchetti personalizzati utilizzando AES-256 e chiavi gestite dal servizio. OpenSearch

Autorizzazioni

Per utilizzare la console di OpenSearch servizio per configurare la crittografia dei dati inattivi, è necessario disporre delle autorizzazioni di lettura per AWS KMS, ad esempio la seguente politica basata sull'identità:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Se desideri utilizzare una chiave diversa da quella di AWS proprietà, devi disporre anche delle autorizzazioni per creare concessioni per la chiave. Queste autorizzazioni in genere hanno la forma di una policy basata su risorse specificata quando crei la chiave.

Se desideri mantenere la tua chiave esclusiva per OpenSearch Service, puoi aggiungere la ViaService condizione kms: a quella policy chiave:

```
"Condition": {
  "StringEquals": {
    "kms:ViaService": "es.us-west-1.amazonaws.com"
  },
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
```

```
}
```

Per ulteriori informazioni, consulta Utilizzo delle politiche chiave in AWS KMS nella Guida per gli AWS Key Management Service sviluppatori.

Abilitazione della crittografia dei dati a riposo

La crittografia dei dati archiviati su nuovi domini richiede Elasticsearch OpenSearch 5.1 o versione successiva. Per abilitarla su domini esistenti è necessario Elasticsearch 6.7 OpenSearch o versione successiva.

Come abilitare la crittografia dei dati a riposo (console)

1. Apri il dominio nella AWS console, quindi scegli Azioni e Modifica configurazione di sicurezza.
2. In Encryption (Crittografia), seleziona Enable encryption of data at rest (Abilita la crittografia dei dati a riposo).
3. Scegli una AWS KMS chiave da usare, quindi scegli Salva modifiche.

Puoi abilitare la crittografia anche tramite l'API di configurazione. La seguente richiesta abilita la crittografia dei dati a riposo su un dominio esistente:

```
{
   "ClusterConfig":{
      "EncryptionAtRestOptions":{
         "Enabled": true,
         "KmsKeyId":"arn:aws:kms:us-east-1:123456789012:alias/my-key"
      }
   }
}
```

Chiave KMS disabilitata o eliminata

Se disabiliti o elimini la chiave che hai usato per crittografare un dominio, il dominio diventa inaccessibile. OpenSearch Il servizio ti invia una notifica che ti informa che non può accedere alla chiave KMS. Riabilita immediatamente la chiave per accedere al dominio.

Il team OpenSearch di assistenza non può aiutarti a recuperare i dati se la chiave viene eliminata. AWS KMS elimina le chiavi solo dopo un periodo di attesa di almeno sette giorni. Se la tua chiave è in attesa di cancellazione, annulla la cancellazione o prendi uno Snapshot manuale del dominio per evitare la perdita di dati.

Disabilitazione della crittografia dei dati a riposo

Dopo aver configurato un dominio per crittografare i dati a riposo, non puoi disabilitare l'impostazione. Puoi invece acquisire una snapshot manuale del dominio esistente, creare un altro dominio, migrare i dati ed eliminare il dominio precedente.

Monitoraggio dei domini che crittografano dati a riposo

I domini che crittografano i dati a riposo hanno due parametri aggiuntivi: `KMSKeyError` e `KMSKeyInaccessible`. Questi parametri vengono visualizzati solo se il dominio rileva un problema con la chiave di crittografia. Per una descrizione completa di questi parametri, consulta the section called “Parametri cluster”. Puoi visualizzarli utilizzando la console OpenSearch di servizio o la CloudWatch console Amazon.

> **Tip**
>
> Ogni metrica rappresenta un problema significativo per un dominio, quindi ti consigliamo di creare CloudWatch allarmi per entrambi. Per ulteriori informazioni, consulta the section called “Allarmi consigliati CloudWatch ”.

Altre considerazioni

- La rotazione automatica delle chiavi preserva le proprietà delle AWS KMS chiavi, quindi la rotazione non ha alcun effetto sulla capacità di accedere ai dati. OpenSearch I domini OpenSearch di Encrypted Service non supportano la rotazione manuale delle chiavi, che comporta la creazione di una nuova chiave e l'aggiornamento di eventuali riferimenti alla vecchia chiave. Per ulteriori informazioni, consultare Rotazione delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service .
- Alcuni tipi di istanza non supportano la crittografia dei dati a riposo. Per dettagli, consulta the section called “Tipi di istanze supportati”.
- I domini che crittografano i dati a riposo usano un nome di repository diverso per i propri snapshot automatici. Per ulteriori informazioni, consultare the section called “Ripristino di snapshot”.
- Anche se consigliamo vivamente di abilitare la crittografia dei dati a riposo, questa potrebbe aggiungere un sovraccarico aggiuntivo della CPU e alcuni millisecondi di latenza. Tuttavia, la maggior parte dei casi d'uso non è sensibile a queste differenze e l'entità dell'impatto dipende dalla configurazione del cluster, dei client e del profilo di utilizzo.

ode-to-node Crittografia N per Amazon OpenSearch Service

La ode-to-node crittografia N fornisce un ulteriore livello di sicurezza oltre alle funzionalità predefinite di Amazon OpenSearch Service.

Ogni dominio OpenSearch di servizio, indipendentemente dal fatto che utilizzi l'accesso VPC, risiede all'interno del proprio VPC dedicato. Questa architettura impedisce ai potenziali aggressori di intercettare il traffico tra i nodi e protegge il cluster. OpenSearch Per impostazione predefinita, tuttavia, il traffico all'interno del VPC non è crittografato. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno del VPC.

Se invii dati al OpenSearch Servizio tramite HTTPS, la node-to-node crittografia aiuta a garantire che i dati rimangano crittografati durante la OpenSearch distribuzione (e la ridistribuzione) in tutto il cluster. Se i dati arrivano non crittografati tramite HTTP, OpenSearch Service li crittografa dopo aver raggiunto il cluster. Puoi richiedere che tutto il traffico verso il dominio arrivi tramite HTTPS utilizzando la console o l'API AWS CLI di configurazione.

Non è richiesta alcuna ode-to-node crittografia se si abilita il controllo granulare degli accessi.

Attivazione della node-to-node crittografia

ode-to-node La crittografia N sui nuovi domini richiede qualsiasi versione di OpenSearch Elasticsearch 6.0 o successiva. L'abilitazione della node-to-node crittografia sui domini esistenti richiede qualsiasi versione di Elasticsearch 6.7 o OpenSearch successiva. Scegli il dominio esistente nella console AWS , seleziona Operazioni, quindi Modifica configurazione di sicurezza.

In alternativa, puoi utilizzare l'API o di configurazione. AWS CLI Per ulteriori informazioni, consulta il riferimento alle API AWS CLI Command Reference e OpenSearch Service.

Disabilitazione della crittografia node-to-node

Dopo aver configurato un dominio per utilizzare node-to-node la crittografia, non puoi disabilitare l'impostazione. Puoi invece acquisire una snapshot manuale del dominio crittografato, creare un altro dominio, migrare i dati ed eliminare il dominio precedente.

Identity and Access Management in Amazon OpenSearch Service

Amazon OpenSearch Service offre diversi modi per controllare l'accesso ai tuoi domini. In questa sezione sono descritti i diversi tipi di policy, il modo in cui interagiscono tra loro ed è riportato come creare le policy personalizzate.

> **Important**
>
> Il supporto VPC introduce alcune considerazioni aggiuntive sul controllo degli accessi ai OpenSearch servizi. Per ulteriori informazioni, consulta the section called “Informazioni sulle policy d'accesso nei domini VPC”.

Tipi di policy

OpenSearch Il servizio supporta tre tipi di politiche di accesso:

- the section called “Policy basate su risorse”
- the section called “Policy basate su identità”
- the section called “Policy basate su IP”

Policy basate su risorse

Quando si crea un dominio, viene aggiunta una policy basata su risorse, talvolta denominata policy di accesso al dominio. Queste policy specificano le operazioni che un principale può eseguire sulle risorse secondarie del dominio (con l'eccezione della ricerca tra cluster). Le sottorisorse includono OpenSearch indici e API. L'elemento Principal specifica l'account, gli utenti o i ruoli a cui è consentito l'accesso. L'elemento Resource specifica a quali risorse secondarie questi principali possono accedere.

Ad esempio, la seguente policy basata sulle risorse concede un accesso completo `test-user` (`es:*`) alle risorse secondarie in `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/*"
    }
  ]
}
```

Due considerazioni importanti si applicano a questa policy:

- Questi privilegi si applicano solo a questo dominio. A meno che non vengano create policy simili su altri domini, `test-user` può accedere solo a `test-domain`.
- I caratteri `/*` finali nell'elemento `Resource` sono significativi e indicano che le policy basate sulle risorse si applicano solo alle risorse secondarie del dominio e non al dominio stesso. Nelle policy basate sulle risorse, l'operazione `es:*` equivale a `es:ESHttp*`.

  Ad esempio, `test-user` può effettuare richieste su un indice (`GET https://search-test-domain.us-west-1.es.amazonaws.com/test-index`), ma non è in grado di aggiornare la configurazione del dominio (`POST https://es.us-west-1.amazonaws.com/2021-01-01/opensearch/domain/test-domain/config`). Nota la differenza tra i due endpoint. L'accesso all'API di configurazione richiede una policy basata sull'identità.

È possibile specificare un nome di indice parziale aggiungendo un carattere jolly. Questo esempio identifica gli indici che iniziano con `commerce`:

```
arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce*
```

In questo caso, l'uso del carattere jolly significa che `test-user` può fare richieste agli indici nel dominio `test-domain` che hanno nomi che iniziano con `commerce`.

Per limitare ulteriormente `test-user`, è possibile applicare la seguente policy:

```
{
  "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"
    }
  ]
}
```

Ora `test-user` è in grado di eseguire un'unica operazione: effettua una ricerca sull'indice `commerce-data`. Tutti gli altri indici all'interno del dominio sono inaccessibili e senza le autorizzazioni necessarie per utilizzare le operazioni `es:ESHttpPut` o `es:ESHttpPost`, `test-user` non è in grado di aggiungere o modificare i documenti.

Quindi, è possibile decidere di configurare un ruolo per gli utenti avanzati. Questa policy fornisce l'accesso `power-user-role` ai metodi HTTP GET e PUT per tutti gli URI nell'indice:

```
{
  "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/
*"
    }
  ]
}
```

Se il dominio si trova in un VPC o utilizza un controllo granulare degli accessi, è possibile usare una policy di accesso al dominio aperto. In caso contrario, la policy di accesso al dominio deve contenere alcune limitazioni, sia per principal che per indirizzo IP.

Per ulteriori informazioni su tutte le azioni disponibili, consultare the section called “Riferimenti agli elementi della policy”. Per un controllo molto più dettagliato sui dati, utilizzare una policy di accesso al dominio aperto con il controllo granulare degli accessi.

Policy basate su identità

A differenza delle politiche basate sulle risorse, che fanno parte di ogni dominio del OpenSearch servizio, è possibile allegare politiche basate sull'identità a utenti o ruoli utilizzando il servizio (IAM). AWS Identity and Access Management Proprio come le policy basate sulle risorse, le policy basate su identità specificano chi può accedere a un servizio, quali azioni può eseguire e, ove applicabile, le risorse su cui può eseguire tali operazioni.

Mentre le policy basate su identità tendono a essere più generiche. Spesso regolamentano solo le operazioni delle API di configurazione che possono essere eseguite da un utente. Dopo aver implementato queste politiche, puoi utilizzare le politiche basate sulle risorse (o il controllo granulare degli accessi) in Service per offrire agli utenti l'accesso a indici e API. OpenSearch OpenSearch

> **Note**
>
> Gli utenti con la `AmazonOpenSearchServiceReadOnlyAccess` policy AWS gestita non possono visualizzare lo stato di integrità del cluster sulla console. Per consentire loro di visualizzare lo stato di integrità del cluster (e altri OpenSearch dati), aggiungi l'`es:ESHttpGet`azione a una politica di accesso e allegala ai loro account o ruoli.

Poiché le policy basate su identità si collegano a utenti o ruoli (principali), il formato JSON non specifica un principale. La policy seguente consente di concedere l'accesso alle azioni che iniziano con `Describe` e `List`. Questa combinazione di azioni fornisce accesso in sola lettura alle configurazioni di dominio, ma non ai dati archiviati nel dominio:

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

```
    }
  ]
}
```

Un amministratore potrebbe avere pieno accesso al OpenSearch servizio e a tutti i dati archiviati su tutti i domini:

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

Le policy basate sull'identità consentono di utilizzare i tag per controllare l'accesso all'API di configurazione. La policy riportata di seguito, ad esempio, consente ai principal collegati di visualizzare e aggiornare la configurazione di un dominio se il dominio dispone del tag `team:devops`:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:UpdateDomainConfig",
      "es:DescribeDomain",
      "es:DescribeDomainConfig"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/team": [
          "devops"
        ]
      }
    }
```

```
  }]
}
```

Puoi anche utilizzare i tag per controllare l'accesso all' OpenSearch API. Le politiche basate su tag per l' OpenSearch API si applicano solo ai metodi HTTP. Ad esempio, la seguente politica consente ai principali collegati di inviare richieste GET e PUT all' OpenSearch API se il dominio ha il `environment:production` tag:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:ESHttpGet",
      "es:ESHttpPut"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Per un controllo più granulare dell' OpenSearch API, prendi in considerazione l'utilizzo di un controllo granulare degli accessi.

> **Note**
>
> Dopo aver aggiunto una o più OpenSearch API a qualsiasi policy basata su tag, devi eseguire un'unica operazione di tag (ad esempio aggiungere, rimuovere o modificare un tag) affinché le modifiche abbiano effetto su un dominio. È necessario utilizzare il software di servizio R20211203 o versione successiva per includere OpenSearch le operazioni API nelle politiche basate su tag.

OpenSearch Il servizio supporta le chiavi `RequestTag` di condizione `TagKeys` globali per l'API di configurazione, non l'API. OpenSearch Queste condizioni si applicano solo alle chiamate API che includono tag all'interno della richiesta, ad esempio `CreateDomain`, `AddTags` e `RemoveTags`. La policy seguente consente ai principal collegati di creare domini, ma solo se includono il tag `team:it` nella richiesta:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "es:CreateDomain",
      "es:AddTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/team": [
          "it"
        ]
      }
    }
  }
}
```

Per maggiori dettagli sull'utilizzo dei tag per il controllo degli accessi e sulle differenze tra policy basate sulle risorse e policy basate su identità, consultare la Guida per l'utente IAM.

Policy basate su IP

Le policy basate su IP limitano l'accesso a un dominio a uno o più indirizzi IP o blocchi CIDR. Tecnicamente, le policy basate su IP non sono un tipo distinto di policy. Al contrario, sono solo policy basate sulle risorse che specificano un principale anonimo e includono un elemento Condition speciale.

L'attrattiva principale delle politiche basate su IP è che consentono richieste non firmate a un dominio di OpenSearch servizio, il che consente di utilizzare client come curl e OpenSearch Dashboards o accedere al dominio tramite un server proxy. Per ulteriori informazioni, consultare the section called “Utilizzo di un proxy per accedere al servizio da dashboard OpenSearch OpenSearch ”.

> **Note**
>
> Se è stato abilitato l'accesso VPC al dominio, non è possibile configurare una policy basata su IP. Invece è possibile utilizzare i gruppi di sicurezza per controllare gli indirizzi IP che possono accedere al dominio. Per ulteriori informazioni, consultare the section called "Informazioni sulle policy d'accesso nei domini VPC".

La seguente policy concede a tutte le richieste HTTP che provengono dall'intervallo di IP specificato l'accesso 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/*"
    }
  ]
}
```

Se il dominio dispone di un endpoint pubblico e non utilizza il controllo granulare degli accessi, è consigliabile combinare le entità IAM e gli indirizzi IP. Questa policy concede l'accesso HTTP `test-user` solo se la richiesta proviene dall'intervallo IP specificato:

```
{
  "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/*"
  }]
}
```

Effettuazione e firma di richieste di servizio OpenSearch

Anche se configuri una politica di accesso completamente aperta basata su risorse, tutte le richieste all'API di configurazione del OpenSearch servizio devono essere firmate. Se le tue policy specificano ruoli o utenti IAM, anche le richieste alle OpenSearch API devono essere firmate utilizzando AWS Signature Version 4. Il metodo della firma differisce in base alle API:

- Per effettuare chiamate all'API OpenSearch di configurazione del servizio, ti consigliamo di utilizzare uno degli AWS SDK. Gli SDK semplificano enormemente il processo e permettono di risparmiare molto tempo rispetto alla creazione e alla firma delle richieste. Gli endpoint dell'API di configurazione utilizzano il seguente formato:

  ```
  es.region.amazonaws.com/2021-01-01/
  ```

  Ad esempio, la seguente richiesta consente di apportare una modifica di configurazione al dominio `movies`, ma l'utente deve firmarla manualmente (scelta non consigliata):

  ```
  POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/movies/config
  {
    "ClusterConfig": {
      "InstanceType": "c5.xlarge.search"
  ```

```
  }
}
```

Se utilizzi uno degli SDK, ad esempio Boto 3, questo gestisce automaticamente la firma della richiesta:

```
import boto3

client = boto3.client(es)
response = client.update_domain_config(
  DomainName='movies',
  ClusterConfig={
    'InstanceType': 'c5.xlarge.search'
  }
)
```

Per un esempio di codice Java, consulta the section called “Uso degli SDK AWS”.

- Per effettuare chiamate alle OpenSearch API, devi firmare le tue richieste. Le OpenSearch API utilizzano il seguente formato:

```
domain-id.region.es.amazonaws.com
```

Ad esempio, la seguente richiesta esegue una ricerca nell'indice `movies` per thor:

```
GET https://my-domain.us-east-1.es.amazonaws.com/movies/_search?q=thor
```

> **Note**
>
> Il servizio ignora i parametri passati negli URL per le richieste HTTP POST che sono firmate con Signature Version 4.

Quando le policy entrano in collisione

Sorgono problemi quando le policy dissentono o non effettuano alcuna menzione esplicita di un utente. Introduzione al funzionamento di IAM nella Guida per l'utente IAM fornisce un riepilogo conciso della logica di valutazione delle policy:

- Come impostazione predefinita, tutte le richieste vengono negate.
- Un permesso esplicito sostituisce questa impostazione di default.
- Un rifiuto esplicito sovrascrive tutti i consensi.

Ad esempio, se una policy basata sulle risorse ti concede l'accesso a una sottorisorsa di dominio (un OpenSearch indice o un'API), ma una policy basata sull'identità ti nega l'accesso, ti viene negato l'accesso. Se una policy basata sull'identità consente l'accesso e una policy basata sulle risorse non specifica se si dispone o meno dell'accesso, è consentito l'accesso. Consultare la seguente tabella di policy che si sovrappongono per un riepilogo dei risultati per le risorse secondarie del dominio.

	Consentito nella policy basata sulle risorse	Rifiutato nella policy basata sulle risorse	Non consentito né rifiutato nella policy basata sulle risorse
Allowed in identity-based policy	Consenso	Rifiuta	Consenso
Denied in identity-based policy	Rifiuta	Rifiuta	Rifiuta
Neither allowed nor denied in identity-based policy	Consenso	Rifiuta	Rifiuta

Riferimenti agli elementi della policy

OpenSearch Il servizio supporta la maggior parte degli elementi delle policy nello IAM Policy Elements Reference, ad eccezione di. `NotPrincipal` La tabella riportata di seguito mostra gli elementi più comuni.

Elemento della policy JSON	Riepilogo
`Version`	La versione corrente del linguaggio della policy è `2012-10-17` . Tutte le policy d'accesso devono specificare questo valore.

Elemento della policy JSON	Riepilogo
`Effect`	L'elemento specifica se l'istruzione consente o nega l'accesso alle azioni specificate. I valori validi sono `Allow` e `Deny`.
`Principal`	Questo elemento specifica il ruolo Account AWS o l'utente IAM a cui è consentito o negato l'accesso a una risorsa e può assumere diverse forme: • AWS account: `"Principal":{"AWS": ["123456789012"]}` o `"Principal":{"AWS": ["arn:aws:iam::123456789012:root"]}` • Utenti IAM: `"Principal":{"AWS": ["arn:aws:iam::123456789012:user/test-user"]}` • Ruoli IAM: `"Principal":{"AWS": ["arn:aws:iam::123456789012:role/test-role"]}` **Important** La specifica del carattere jolly * consente l'accesso anonimo al dominio, che non è consigliabile a meno che non si aggiunga una condizione basata su IP, non si usi il supporto VPC o non si abiliti il controllo granulare degli accessi. Inoltre, esamina attentamente le seguenti politiche per confermare che non garantiscano un ampio accesso: • Politiche basate sull'identità collegate ai AWS principali associati (ad esempio, ruoli IAM) • Politiche basate sulle risorse collegate alle AWS risorse associate (ad esempio, chiavi KMS) AWS Key Management Service

Elemento della policy JSON	Riepilogo

`Action`	OpenSearch Il servizio utilizza `ESHttp*` azioni per i metodi HTTP. OpenSearch Il resto delle operazioni si applica all'API di configurazione.
	
	Alcune azioni `es:` supportano le autorizzazioni a livello di risorsa. Ad esempio, è possibile assegnare a un utente autorizzazioni per eliminare un determinato dominio senza garantirgli le autorizzazioni per eliminare qualsiasi dominio. Altre azioni si applicano solo al servizio. Ad esempio, `es:ListDomainNames` non ha senso nel contesto di un singolo dominio e quindi richiede un carattere jolly.
	
	Per un elenco di tutte le azioni disponibili e se si applicano alle sottorisorse del dominio (`test-domain/*`), alla configurazione del dominio (`test-domain`) o solo al servizio (`*`), consulta Azioni, risorse e chiavi di condizione per Amazon OpenSearch Service nel Service Authorization Reference
	Le policy basate sulle risorse differiscono dalle autorizzazioni a livello di risorsa. Le policy basate sulle risorse sono policy JSON complete che si collegano ai domini. Le autorizzazioni a livello di risorsa consentono di limitare le azioni a particolari domini o risorse secondarie. In pratica, si possono considerare le autorizzazioni a livello di risorsa una parte opzionale di una policy basata sulle risorse o sull'identità.
	
	Mentre le autorizzazioni a livello di risorsa per `es:CreateDomain` potrebbero sembrare poco intuitive (dopo tutto, perché offrire a un utente le autorizzazioni per creare un dominio già esistente?) l'uso di un carattere jolly consente di implementare uno schema di denominazione semplice per i domini, ad esempio `"Resource": "arn:aws:es:us-west-1:987654321098:domain/my-team-name-*"`.
	
	Naturalmente, è ugualmente possibile includere azioni insieme a elementi di risorse meno restrittivi, come i seguenti:
	
	`{`
	`"Version": "2012-10-17",`

Elemento della policy JSON	Riepilogo

	<pre>"Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "es:ESHttpGet",
	  "es:DescribeDomain"
	  ],
	  "Resource": "*"
	  }
	]
	}</pre>
	Per ulteriori informazioni sull'accoppiamento di azioni e risorse, fare riferimento all'elemento `Resource` in questa tabella.

`Condition`	OpenSearch Il servizio supporta la maggior parte delle condizioni descritte nelle chiavi di contesto delle condizioni AWS globali nella IAM User Guide. Le eccezioni più importanti includono la `aws:PrincipalTag` chiave, che OpenSearch Service non supporta.
	
	Durante la configurazione di una policy basata su IP, è necessario specificare gli indirizzi IP o i blocchi CIDR come condizione, come ad esempio:
	
	<pre>"Condition": {
	  "IpAddress": {
	  "aws:SourceIp": [
	  "192.0.2.0/32"
	  ]
	  }
	}</pre>
	Come indicato inthe section called “Policy basate su identità”, le chiavi `aws:ResourceTag` `aws:RequestTag` , e `aws:TagKeys` condition si applicano all'API di configurazione e alle OpenSearch API.

Elemento della policy JSON	Riepilogo

`Resource`	OpenSearch Il servizio utilizza `Resource` gli elementi in tre modi fondamentali:
	
	• Per azioni che si applicano al OpenSearch Servizio stesso`es:ListDomainNames` , come o per consentire l'accesso completo, usa la seguente sintassi:
	
	`"Resource": "*"`
	
	• Per le azioni che implicano una configurazione del dominio, ad esempio `es:DescribeDomain` , è possibile utilizzare la sintassi seguente:
	
	`"Resource": "arn:aws:es:` *`region`*`:`*`aws-account-id`*`:domain/`*`domain-name`*` "`
	
	• Per le azioni che si applicano alle risorse secondarie di un dominio, ad esempio `es:ESHttpGet` , è possibile utilizzare la sintassi seguente:
	
	`"Resource": "arn:aws:es:` *`region`*`:`*`aws-account-id`*`:domain/`*`domain-name`*` /*"`
	
	Non è necessario utilizzare un jolly. OpenSearch Il servizio consente di definire una politica di accesso diversa per ogni OpenSearch indice o API. Ad esempio, è possibile limitare le autorizzazioni di un utente per l'indice `test-index` :
	
	`"Resource": "arn:aws:es:` *`region`*`:`*`aws-account-id`*`:domain/`*`domain-name`*` /test-index"`
	
	Invece dell'accesso completo a `test-index` , è preferibile limitare la policy all'API di ricerca:
	
	`"Resource": "arn:aws:es:` *`region`*`:`*`aws-account-id`*`:domain/`*`domain-name`*` /test-index/_search"`

Elemento della policy JSON	Riepilogo
	È possibile anche controllare l'accesso ai singoli documenti: `"Resource": "arn:aws:es:  region:aws-account-id:domain/domain-name /test-index/test-type/1"` In sostanza, se OpenSearch esprime la sottorisorsa come URI, è possibile controllarne l'accesso utilizzando una politica di accesso. Per un controllo ancora maggiore sulle risorse a cui un utente può accedere, vedere the section called “Controllo granulare degli accessi”. Per ulteriori informazioni su quali azioni supportano le autorizzazioni a livello di risorsa, fare riferimento all'elemento `Action` in questa tabella.

Opzioni avanzate e considerazioni sulle API

OpenSearch Il servizio ha diverse opzioni avanzate, una delle quali ha implicazioni sul controllo degli accessi:. `rest.action.multi.allow_explicit_index` Con l'impostazione predefinita true, consente agli utenti di ignorare le autorizzazioni a livello di risorsa secondaria in determinate circostanze.

Ad esempio, considerare la seguente policy basata sulle risorse:

```
{
  "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/*"
    }
  ]
}
```

Questa politica garantisce l'accesso `test-user` completo `test-index` e alla OpenSearch massa delle API. Consente inoltre `GET` le richieste a `restricted-index`.

La seguente richiesta di indicizzazione, come è prevedibile, ha esito negativo a causa di un errore delle autorizzazioni:

```
PUT https://search-test-domain.us-west-1.es.amazonaws.com/restricted-index/movie/1
{
  "title": "Your Name",
  "director": "Makoto Shinkai",
  "year": "2016"
}
```

A differenza dell'API dell'indice, l'API bulk consente la creazione, l'aggiornamento e l'eliminazione di molti documenti in una sola chiamata. Tuttavia spesso si specificano queste operazioni nel corpo della richiesta, anziché nell'URL della richiesta. Poiché OpenSearch Service utilizza gli URL per controllare l'accesso alle sottorisorse del dominio, `test-user` può, di fatto, utilizzare l'API in blocco per apportare modifiche. `restricted-index` Anche se l'utente non dispone di autorizzazioni `POST` per l'indice, la seguente richiesta ha esito positivo:

```
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" }
```

In questo caso, la policy d'accesso non riesce a soddisfare i suoi intenti. Per impedire agli utenti di aggirare questi tipi di restrizioni, è possibile modificare `rest.action.multi.allow_explicit_index` in false. Se questo valore è false, tutte le chiamate alle API bulk, mget, e msearch che specificano i nomi degli indici nel corpo della richiesta smettono di funzionare. In altre parole, le chiamate a `_bulk` non funzionano, ma le chiamate a `test-index/_bulk` sì. Questo secondo endpoint contiene un nome dell'indice, perciò non è necessario specificarne uno nel corpo nella richiesta.

OpenSearch Dashboards si basa molto su mget e msearch, quindi è improbabile che funzioni correttamente dopo questa modifica. Per la correzione parziale, è possibile lasciare `rest.action.multi.allow_explicit_index` come true e negare a determinati utenti l'accesso a una o più di queste API.

Per informazioni su come modificare questa impostazione, consultare the section called “Impostazioni avanzate del cluster”.

Analogamente, la seguente policy basata sulle risorse contiene due problemi di lieve entità:

```
{
  "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/*"
    }
```

```
  ]
}
```

- Nonostante il rifiuto esplicito, `test-user` può comunque effettuare chiamate come `GET https://search-test-domain.us-west-1.es.amazonaws.com/_all/_search` e `GET https://search-test-domain.us-west-1.es.amazonaws.com/*/_search` per accedere ai documenti in `restricted-index`.
- Poiché l'elemento `Resource` fa riferimento a `restricted-index/*`, `test-user` non dispone delle autorizzazioni per accedere direttamente ai documenti dell'indice. L'utente, tuttavia, dispone delle autorizzazioni necessarie per eliminare l'intero indice. Per prevenire l'accesso e l'eliminazione, la policy deve specificare `restricted-index*`.

Anziché combinare permessi ampi e negazioni strette, la soluzione più sicura è seguire il principio del privilegio minimo e concedere solo le autorizzazioni necessarie per eseguire un'operazione. Per ulteriori informazioni sul controllo dell'accesso a singoli indici o operazioni, vedere. OpenSearch the section called “Controllo granulare degli accessi”

> **Important**
>
> Specificando il carattere jolly * si abilita l'accesso anonimo al dominio. Non è consigliabile utilizzare il carattere jolly. Inoltre, esamina attentamente le seguenti politiche per verificare che non garantiscano un accesso ampio:
>
> - Politiche basate sull'identità collegate ai AWS principali associati (ad esempio, ruoli IAM)
> - Politiche basate sulle risorse collegate alle AWS risorse associate (ad esempio, chiavi KMS) AWS Key Management Service

Configurazione delle policy di accesso

- Per istruzioni sulla creazione o la modifica di politiche basate su risorse e IP in Service, vedere. OpenSearch the section called “Configurazione delle policy di accesso”
- Per istruzioni su come creare o modificare le policy basate sull'identità in IAM, consultare Creazione di policy IAM nella Guida per l'utente IAM.

Altre policy di esempio

Sebbene questo capitolo includa molti esempi di policy, il controllo degli AWS accessi è un argomento complesso che può essere compreso meglio attraverso esempi. Per ulteriori informazioni, consultare Esempi di policy IAM basate su identità nella Guida per l'utente di IAM.

Riferimento alle autorizzazioni dell'API Amazon OpenSearch Service

Quando configuri il controllo degli accessi, scrivi politiche di autorizzazione che puoi allegare a un'identità IAM (politiche basate sull'identità). Per ulteriori informazioni, consultare gli argomenti seguenti nella Referenza sull'autorizzazione del servizio:

- Azioni, risorse e chiavi di condizione per Service. OpenSearch
- Azioni, risorse e chiavi di condizione per OpenSearch Ingestion.

Questo riferimento contiene informazioni su quali operazioni API possono essere utilizzate in una policy IAM. Include anche la AWS risorsa per la quale è possibile concedere le autorizzazioni e le chiavi di condizione che è possibile includere per un controllo granulare degli accessi.

Le operazioni, il valore della risorsa e le condizioni vengono specificati rispettivamente nei campi `Action`, `Resource` e `Condition` della policy. Per specificare un'azione per OpenSearch Service, utilizzate il `es:` prefisso seguito dal nome dell'operazione API (ad esempio,). `es:CreateDomain` Per specificare un'azione per OpenSearch Ingestion, utilizzate il `osis:` prefisso seguito dall'operazione API (ad esempio,). `osis:CreatePipeline`

AWS politiche gestite per Amazon OpenSearch Service

Una politica AWS gestita è una politica autonoma creata e amministrata da. AWS AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una

policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AmazonOpenSearchDirectQueryGlueCreateAccess

Concede ad Amazon OpenSearch Service Direct Query Service l'accesso a `CreateDatabase`,`CreatePartition`,`CreateTable`, e `BatchCreatePartition` AWS Glue API.

Puoi trovare la AmazonOpenSearchDirectQueryGlueCreateAccesspolicy nella console IAM.

AmazonOpenSearchServiceFullAccess

Garantisce l'accesso completo alle operazioni e alle risorse dell'API di configurazione del OpenSearch servizio per un Account AWS.

Puoi trovare la AmazonOpenSearchServiceFullAccesspolicy nella console IAM.

AmazonOpenSearchServiceReadOnlyAccess

Concede l'accesso in sola lettura a tutte le risorse del OpenSearch servizio per un. Account AWS

Puoi trovare la AmazonOpenSearchServiceReadOnlyAccesspolicy nella console IAM.

AmazonOpenSearchServiceRolePolicy

Non è possibile collegare `AmazonOpenSearchServiceRolePolicy`alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a OpenSearch Service di accedere alle risorse dell'account. Per ulteriori informazioni, consulta the section called “Autorizzazioni”.

Puoi trovare la AmazonOpenSearchServiceRolePolicypolicy nella console IAM.

AmazonOpenSearchServiceCognitoAccess

Fornisci le autorizzazioni minime di Amazon Cognito necessarie per abilitare l'autenticazione Cognito.

Puoi trovare la AmazonOpenSearchServiceCognitoAccesspolicy nella console IAM.

AmazonOpenSearchIngestionServiceRolePolicy

Non è possibile collegare `AmazonOpenSearchIngestionServiceRolePolicy`alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a OpenSearch Ingestion

di abilitare l'accesso VPC per le pipeline di ingestione, creare tag e pubblicare metriche relative all'importazione sul tuo account. CloudWatch Per ulteriori informazioni, consulta the section called “Uso di ruoli collegati ai servizi”.

AmazonOpenSearchIngestionServiceRolePolicyPuoi trovare la policy nella console IAM.

OpenSearchIngestionSelfManagedVpcePolicy

Non è possibile collegare `OpenSearchIngestionSelfManagedVpcePolicy`alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a OpenSearch Ingestion di abilitare l'accesso VPC autogestito per le pipeline di ingestione, creare tag e pubblicare metriche relative all'importazione sul tuo account. CloudWatch Per ulteriori informazioni, consulta the section called “Uso di ruoli collegati ai servizi”.

OpenSearchIngestionSelfManagedVpcePolicyPuoi trovare la policy nella console IAM.

AmazonOpenSearchIngestionFullAccess

Garantisce l'accesso completo alle operazioni e alle risorse dell'API OpenSearch Ingestion per un. Account AWS

Puoi trovare la AmazonOpenSearchIngestionFullAccesspolicy nella console IAM.

AmazonOpenSearchIngestionReadOnlyAccess

Concede l'accesso in sola lettura a tutte le risorse di OpenSearch Ingestion per un. Account AWS

Puoi trovare la AmazonOpenSearchIngestionReadOnlyAccesspolicy nella console IAM.

AmazonOpenSearchServerlessServiceRolePolicy

Fornisce le Amazon CloudWatch autorizzazioni minime necessarie per inviare dati metrici OpenSearch Serverless a. CloudWatch

Puoi trovare la AmazonOpenSearchServerlessServiceRolePolicypolicy nella console IAM.

OpenSearch Aggiornamenti del servizio alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per OpenSearch Service da quando questo servizio ha iniziato a tenere traccia delle modifiche.

Modifica	Descrizione	Data
Aggiunto `OpenSearchIngestionSelfManagedVpcePolicy`	Una nuova policy che consente a OpenSearch Ingestion di abilitare l'accesso VPC autogestito per le pipeline di ingestione, creare tag e pubblicare metriche relative all'importazione sul tuo account. CloudWatch Per la policy JSON, consultare Console IAM.	12 giugno 2024
Aggiunto `AmazonOpenSearchDirectQueryGlueCreateAccess`	Concede ad Amazon OpenSearch Service Direct Query Service l'accesso a `CreateDatabase` `CreatePartition` ,`CreateTable` , e `BatchCreatePartition` AWS Glue API.	6 maggio 2024
Aggiornati `AmazonOpenSearchServiceRolePolicy` e `AmazonElasticsearchServiceRolePolicy`	Sono state aggiunte le autorizzazioni necessarie al ruolo collegato al servizio per assegnare e annullare l'assegnazione degli indirizzi IPv6. Anche la policy obsoleta di Elasticsearch è stata aggiornata per garantire la compatibilità con le versioni precedenti.	18 ottobre 2023

Modifica	Descrizione	Data
Aggiunto `AmazonOpenSearchIngestionServiceRolePolicy`	Una nuova policy che consente a OpenSearch Ingestion di abilitare l'accesso VPC per le pipeline di importazione, creare tag e pubblicare metriche relative all'importazione sul tuo account. CloudWatch Per la policy JSON, consultare Console IAM.	26 aprile 2023
Aggiunto `AmazonOpenSearchIngestionFullAccess`	Una nuova policy che garantisce l'accesso completo alle operazioni e alle risorse dell'API OpenSearch Ingestion per un. Account AWS Per la policy JSON, consultare Console IAM.	26 aprile 2023
Aggiunto `AmazonOpenSearchIngestionReadOnlyAccess`	Una nuova politica che garantisce l'accesso in sola lettura a tutte le risorse di OpenSearch Ingestion per un. Account AWS Per la policy JSON, consultare Console IAM.	26 aprile 2023

Modifica	Descrizione	Data
Aggiunto `AmazonOpenSearchServerlessServiceRolePolicy`	Una nuova policy che fornisce le autorizzazioni minime necessarie per inviare dati metrici OpenSearch Serverless a Amazon CloudWatch Per la policy JSON, consultare Console IAM.	29 novembre 2022
Aggiornati `AmazonOpenSearchServiceRolePolicy` e `AmazonElasticsearchServiceRolePolicy`	Sono state aggiunte le autorizzazioni necessarie per il ruolo collegato al servizio per creare endpoint VPC gestiti dal servizio OpenSearch . Alcune azioni possono essere eseguite solo quando la richiesta contiene il tag `OpenSearchManaged=true` . Anche la policy obsoleta di Elasticsearch è stata aggiornata per garantire la compatibilità con le versioni precedenti.	7 novembre 2022

Modifica	Descrizione	Data
Aggiornati `AmazonOpenSearchServiceRolePolicy` e `AmazonElasticsearchServiceRolePolicy`	È stato aggiunto il supporto per l'`PutMetricData` azione, necessaria per pubblicare i parametri OpenSearch del cluster su Amazon CloudWatch. Anche la policy obsoleta di Elasticsearch è stata aggiornata per garantire la compatibilità con le versioni precedenti. Per la policy JSON, consultare Console IAM.	12 settembre 2022
Aggiornati `AmazonOpenSearchServiceRolePolicy` e `AmazonElasticsearchServiceRolePolicy`	Aggiunto il supporto per il tipo di risorsa `acm`. La policy fornisce l'autorizzazione minima AWS Certificate Manager (ACM) di sola lettura necessaria al ruolo collegato al servizio per verificare e convalidare le risorse ACM al fine di creare e aggiornare domini personalizzati abilitati agli endpoint. Anche la policy obsoleta di Elasticsearch è stata aggiornata per garantire la compatibilità con le versioni precedenti.	28 luglio 2022

Modifica	Descrizione	Data
Aggiornati `AmazonOpenSearchServiceCognitoAccess` e `AmazonESCognitoAccess`	È stato aggiunto il supporto per l'`UpdateUserPoolClient` azione, necessaria per impostare la configurazione del pool di utenti di Cognito durante l'aggiornamento da Elasticsearch a. OpenSearch Autorizzazioni corrette per l'operazione `SetIdentityPoolRoles` in modo da consentire l'accesso a tutte le risorse. Anche la policy obsoleta di Elasticsearch è stata aggiornata per garantire la compatibilità con le versioni precedenti.	20 dicembre 2021
Aggiornato `AmazonOpenSearchServiceRolePolicy`	Aggiunto il supporto per il tipo di risorsa `security-group` . La policy fornisce le autorizzazioni minime di Amazon EC2 ed Elastic Load Balancing necessarie per il ruolo collegato ai servizi per abilitare l'accesso VPC.	9 settembre 2021

Modifica	Descrizione	Data
• Aggiunto `AmazonOpenSearchServiceFullAccess` • Obsoleta `AmazonESFullAccess`	Questa nuova policy ha lo scopo di sostituire la vecchia policy. Entrambe le policy forniscono l'accesso completo all'API di configurazione del OpenSearch servizio e a tutti i metodi HTTP per le API. OpenSearch Il controllo granulare degli accessi e le policy basate sulle risorse possono comunque limitare l'accesso.	7 settembre 2021
• Aggiunto `AmazonOpenSearchServiceReadOnlyAccess` • Obsoleta `AmazonESReadOnlyAccess`	Questa nuova policy ha lo scopo di sostituire la vecchia policy. Entrambe le policy forniscono l'accesso in sola lettura all'API di configurazione del OpenSearch servizio (`es:Describe* ,es:List*`, and`es:Get*`) e nessun accesso ai metodi HTTP per le API. OpenSearch	7 settembre 2021
• Aggiunto `AmazonOpenSearchServiceCognitoAccess` • Obsoleta `AmazonESCognitoAccess`	Questa nuova policy ha lo scopo di sostituire la vecchia policy. Entrambe le policy forniscono le autorizzazioni minime di Amazon Cognito necessarie per abilitare l'autenticazione Cognito.	7 settembre 2021

Modifica	Descrizione	Data
• Aggiunto AmazonOpenSearchServiceRolePolicy • Obsoleta `AmazonElasticsearchServiceRolePolicy`	Questa nuova policy ha lo scopo di sostituire la vecchia policy. Entrambe le policy forniscono le autorizzazioni minime di Amazon EC2 ed Elastic Load Balancing necessarie per il ruolo collegato ai servizi per abilitare l'accesso VPC.	7 settembre 2021
Monitoraggio delle modifiche iniziato	Amazon OpenSearch Service ora tiene traccia delle modifiche alle politiche AWS gestite.	7 settembre 2021

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. In AWS, la rappresentazione cross-service può comportare il problema confused deputy. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Consigliamo di utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` nelle policy delle risorse per limitare le autorizzazioni con cui Amazon OpenSearch Service fornisce un altro servizio alla risorsa. Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali e il valore `aws:SourceArn` contiene l'ID account, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` deve utilizzare lo stesso ID

account nella stessa dichiarazione di policy. Utilizzare `aws:SourceArn` se si desidera consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizzare `aws:SourceAccount` se si desidera consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il valore di `aws:SourceArn` deve essere l'ARN del dominio di OpenSearch Service.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:es:*:123456789012:*`.

L'esempio seguente mostra il modo in cui puoi utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` in OpenSearch Service per prevenire il problema confused deputy.

```
{
   "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"
         }
      }
   }
}
```

Controllo granulare degli accessi in Amazon Service OpenSearch

Il controllo granulare degli accessi offre modi aggiuntivi per controllare l'accesso ai tuoi dati su Amazon Service. OpenSearch Ad esempio, a seconda di chi effettua la richiesta, è possibile che

una ricerca restituisca risultati da un solo indice. Potresti voler nascondere determinati campi nei tuoi documenti o escludere del tutto determinati documenti.

Il controllo granulare degli accessi offre i seguenti vantaggi:

- Controllo degli accessi basato sui ruoli
- Sicurezza a livello di indice, documento e campo
- OpenSearch Dashboard multi-tenancy
- Autenticazione di base HTTP per e dashboard OpenSearch OpenSearch

Argomenti

Il quadro generale: controllo granulare degli accessi e sicurezza dei servizi OpenSearch

La sicurezza di Amazon OpenSearch Service ha tre livelli principali:

Rete

Il primo livello di sicurezza è la rete, che determina se le richieste raggiungono un dominio OpenSearch di servizio. Se sceglisi sceglieAccesso pubblico quando creisi crea un dominio, le richieste provenienti da qualunquequalsiasi client connesso a Internet possono raggiungere l'endpoint del dominio. Se si sceglie Accesso VPC, i client devono connettersi al VPC (e i gruppi di sicurezza associati devono consentirlo) affinché una richiesta raggiunga l'endpoint. Per ulteriori informazioni, consultare the section called “Supporto per VPC”.

Policy di accesso al dominio

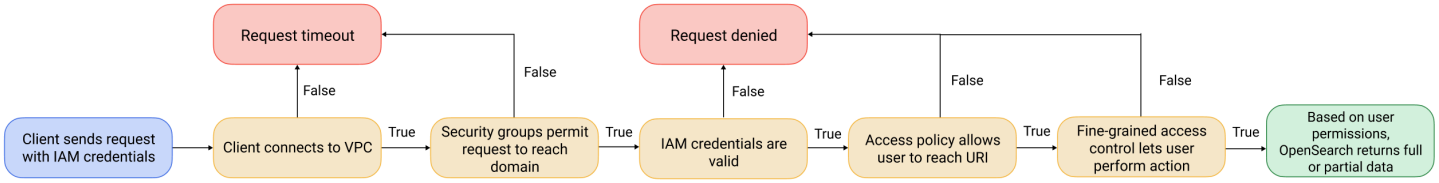
Il secondo livello di protezione è la policy di accesso al dominio. Dopo che una richiesta raggiunge un endpoint di dominio, la policy di accesso basato sulle risorse consente o nega la richiesta di accesso a un determinato URI. La politica di accesso accetta o rifiuta le richieste nella «periferia» del dominio, prima che raggiungano OpenSearch se stesse.

Controllo granulare degli accessi

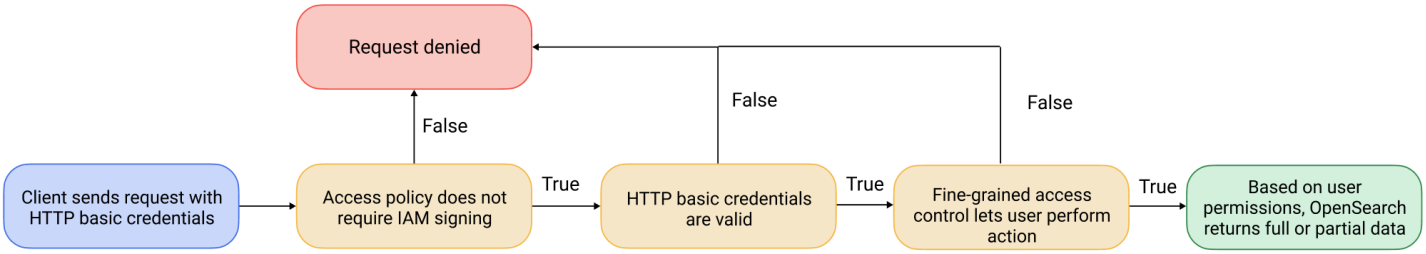
Il terzo e ultimo livello di sicurezza è il controllo granulare degli accessi. Dopo che una policy di accesso basata sulle risorse consente a una richiesta di raggiungere un endpoint di dominio, il controllo granulare degli accessi valuta le credenziali utente e autentica l'utente o nega la richiesta. Se il controllo granulare degli accessi autentica l'utente, recupera tutti i ruoli mappati a tale utente e utilizza il set completo di autorizzazioni per determinare come gestire la richiesta.

> **Note**
>
> Se una policy di accesso basata sulle risorse contiene ruoli o utenti IAM, i client devono inviare richieste firmate utilizzando AWS la versione 4 di Signature. Pertanto, le policy di accesso possono entrare in conflitto con il controllo granulare degli accessi, soprattutto se si utilizza il database utente interno e l'autenticazione di base HTTP. Non puoi firmare una richiesta con nome utente e password e credenziali IAM. In generale, se si abilita il controllo granulare degli accessi, si consiglia di utilizzare una policy di accesso al dominio che non richiede richieste firmate.

Questo primo diagramma illustra una configurazione comune: un dominio di accesso VPC con controllo granulare degli accessi abilitato, una policy di accesso basata su IAM e un utente principale IAM.



Il seguente diagramma illustra un'altra configurazione comune: un dominio di accesso pubblico con controllo granulare degli accessi abilitato, una policy di accesso che non utilizza i principal IAM e un utente master nel database utente interno.



Esempio

Considera una richiesta `GET` a `movies/_search?q=thor`. L'utente dispone delle autorizzazioni per cercare l'indice `movies`? In tal caso, l'utente dispone delle autorizzazioni per visualizzare tutti i documenti al suo interno? La risposta dovrebbe omettere o anonimizzare dei campi? Per l'utente master, la risposta potrebbe essere simile a questa:

```
{
  "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
        }
      },
      ...
    ]
  }
}
```

Se un utente con autorizzazioni più limitate emette esattamente la stessa richiesta, la risposta potrebbe essere simile a questa:

```
{
  "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 risposta ha meno hit e meno campi per ogni hit. Inoltre, il campo `release_date` è anonimizzato. Se un utente senza autorizzazioni effettua la stessa richiesta, il cluster restituisce un errore:

```
{
  "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
}
```

Se un utente fornisce credenziali non valide, il cluster restituisce un'eccezione `Unauthorized`.

Concetti chiave

Per iniziare a utilizzare un controllo granulare degli accessi, considera i seguenti concetti:

- Ruoli: il modo principale di utilizzare il controllo granulare degli accessi. In questo caso, i ruoli sono distinti dai ruoli IAM. I ruoli contengono qualsiasi combinazione di autorizzazioni: a livello di cluster, a livello di indice, a livello di documento e a livello di campo.
- Mappatura: dopo aver configurato un ruolo, lo si associa a uno o più utenti. Ad esempio, è possibile mappare tre ruoli a un singolo utente: un ruolo che fornisce l'accesso a Dashboards, uno che fornisce l'accesso in sola lettura a `index1` e uno che fornisce l'accesso in scrittura a `index2`. In alternativa, è possibile includere tutte queste autorizzazioni in un singolo ruolo.
- Utenti: persone o applicazioni che effettuano richieste al OpenSearch cluster. Gli utenti dispongono di credenziali, chiavi di accesso IAM o nome utente e password, che specificano quando effettuano richieste.

Informazioni sull'utente principale

L'utente principale in OpenSearch Service è una combinazione di nome utente e password o un principale IAM che dispone delle autorizzazioni complete per il OpenSearch cluster sottostante. Un utente è considerato un utente principale se ha tutti gli accessi al OpenSearch cluster e la possibilità di creare utenti interni, ruoli e mappature dei ruoli all'interno delle dashboard. OpenSearch

Un utente master creato nella console di OpenSearch servizio o tramite la CLI viene automaticamente mappato su due ruoli predefiniti:

- `all_access`— Fornisce l'accesso completo a tutte le operazioni a livello di cluster, l'autorizzazione alla scrittura su tutti gli indici del cluster e l'autorizzazione alla scrittura a tutti i tenant.
- `security_manager`— Fornisce l'accesso al plug-in di sicurezza e la gestione di utenti e autorizzazioni.

Con questi due ruoli, l'utente ottiene l'accesso alla scheda Sicurezza nelle OpenSearch dashboard, dove può gestire utenti e autorizzazioni. Se si crea un altro utente interno e lo si associa solo al **`all_access`** ruolo, l'utente non ha accesso alla scheda Sicurezza. È possibile creare utenti principali aggiuntivi mappandoli esplicitamente a entrambi `all_access` i `security_manager` ruoli. Per istruzioni, consulta the section called “Utenti principali aggiuntivi”.

Quando crei un utente master per il tuo dominio, puoi specificare un principale IAM esistente o creare un utente master all'interno del database utenti interno. Considera quanto segue quando decidi quale usare:

- Principal IAM: se scegli un principale IAM per il tuo utente principale, tutte le richieste al cluster devono essere firmate utilizzando AWS Signature Version 4.

  OpenSearch Il servizio non prende in considerazione nessuna delle autorizzazioni del responsabile IAM. L'utente o il ruolo IAM serve esclusivamente per l'autenticazione. Le politiche relative a quell'utente o ruolo non influiscono sull'autorizzazione dell'utente principale. L'autorizzazione viene gestita tramite le varie autorizzazioni del plug-in OpenSearch Security.

  Ad esempio, puoi assegnare zero autorizzazioni IAM a un principale IAM e, purché la macchina o la persona possa autenticarsi per quell'utente o ruolo, ha il potere dell'utente principale in Service. OpenSearch

Ti consigliamo IAM se desideri utilizzare gli stessi utenti su più cluster, se desideri utilizzare Amazon Cognito per accedere alle dashboard o se OpenSearch disponi di client che supportano la firma Signature versione 4.

- Database utenti interno: se crei un master nel database utenti interno (con una combinazione di nome utente e password), puoi utilizzare l'autenticazione di base HTTP (oltre alle credenziali IAM) per effettuare richieste al cluster. La maggior parte dei client supporta l'autenticazione di base, incluso curl, che supporta anche la versione 4 di AWS Signature con l'opzione --aws-sigv4. Il database utenti interno è memorizzato in un OpenSearch indice, quindi non è possibile condividerlo con altri cluster.

  È consigliabile utilizzare il database utente interno se non è necessario riutilizzare gli utenti in più cluster, se si desidera utilizzare l'autenticazione di base HTTP per accedere a Dashboards (anziché ad Amazon Cognito) o se si dispone di client che supportano solo l'autenticazione di base. Il database utenti interno è il modo più semplice per iniziare a usare OpenSearch Service.

Abilitazione del controllo granulare degli accessi

Abilita il controllo granulare degli accessi utilizzando la console o l'API di AWS CLI configurazione. Per le fasi, consulta Creazione e gestione dei domini.

Il controllo granulare degli accessi richiede OpenSearch Elasticsearch 6.7 o versione successiva. Richiede inoltre HTTPS per tutto il traffico verso il dominio, la crittografia dei dati inattivi e la crittografia. node-to-node A seconda di come configurate le funzionalità avanzate del controllo granulare degli accessi, l'ulteriore elaborazione delle richieste potrebbe richiedere risorse di calcolo e memoria su singoli nodi di dati. Dopo aver abilitato il controllo granulare degli accessi, non è più possibile disabilitarlo.

Abilitazione del controllo granulare degli accessi su domini esistenti

Puoi abilitare un controllo granulare degli accessi sui domini esistenti in esecuzione o su Elasticsearch 6.7 o versione successiva. OpenSearch

Per abilitare il controllo granulare degli accessi su un dominio esistente (console)

1. Seleziona il dominio e scegli Operazioni quindi Modifica configurazione di sicurezza.
2. True per abilitare il controllo granulare degli accessi.
3. Scegli come creare l'utente master:

- Se si desidera utilizzare IAM per la gestione degli utenti, scegliere Imposta ARN IAM come utente principale e specificare l'ARN per un ruolo IAM.
- Se desideri utilizzare il database utenti interno, scegli Crea utente principale e specifica un nome utente e una password.

4. (Opzionale) Seleziona Enable migration period for open/IP-based access policy (Abilita il periodo di migrazione per le policy di accesso open/basati su IP). Questa impostazione consente un periodo di transizione di 30 giorni durante il quale gli utenti esistenti possono continuare ad accedere al dominio senza interruzioni e Policy di accesso basate su IP aperte e esistenti continueranno a lavorare con il tuo dominio. Durante questo periodo di migrazione, consigliamo agli amministratori creare i ruoli necessari e mapparli agli utenti per il dominio. Se si utilizzano policy basate su identità anziché un criterio di accesso aperto o basato su IP, è possibile disabilitare questa impostazione.

   È inoltre necessario aggiornare i client per lavorare con un controllo granulare degli accessi durante il periodo di migrazione. Ad esempio, se mappi i ruoli IAM con un controllo di accesso granulare, devi aggiornare i tuoi client per iniziare a firmare le richieste con AWS Signature Version 4. Se si configura l'autenticazione di base HTTP con un controllo granulare degli accessi, è necessario aggiornare i client per fornire le credenziali di autenticazione di base appropriate nelle richieste.

   Durante il periodo di migrazione, gli utenti che accedono all'endpoint OpenSearch Dashboards per il dominio accederanno direttamente alla pagina Discover anziché alla pagina di accesso. Gli amministratori e gli utenti master possono scegliere Login per accedere con le credenziali di amministratore e configurare i mapping dei ruoli.

   > **Important**
   >
   > OpenSearch Il servizio disabilita automaticamente il periodo di migrazione dopo 30 giorni. Si consiglia di terminarlo non appena crei i ruoli necessari e li mappi agli utenti. Al termine del periodo di migrazione, non è possibile riattivarlo.

5. Scegliere Save changes (Salva modifiche).

Il cambiamento innesca una implementazione blu/verde durante la quale l'integrità del cluster diventa rossa, ma tutte le operazioni del cluster rimangono inalterate.

Per abilitare il controllo granulare degli accessi su un dominio esistente (CLI)

Imposta `AnonymousAuthEnabled` su `true` per abilitare il periodo di migrazione con un controllo granulare degli accessi:

```
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}'
```

Informazioni sul ruolo default

Un controllo granulare degli accessi richiede una mappatura dei ruoli. Se il tuo dominio utilizza politiche di accesso basate sull'identità, OpenSearch Service associa automaticamente gli utenti a un nuovo ruolo chiamato default_role per aiutarti a migrare correttamente gli utenti esistenti. Questa mappatura temporanea garantisce che gli utenti possano ancora inviare correttamente le richieste GET e PUT firmate IAM fino a quando non crei i tuoi mapping dei ruoli personalizzati.

Il ruolo non aggiunge vulnerabilità o difetti di sicurezza al dominio del servizio. OpenSearch Ti consigliamo di eliminare il ruolo predefinito non appena configuri i tuoi ruoli e di mapparli di conseguenza.

Scenari di migrazione

Nella tabella seguente viene descritto il comportamento di ciascun metodo di autenticazione prima e dopo aver abilitato il controllo granulare degli accessi su un dominio esistente e i passaggi che gli amministratori devono adottare per mappare correttamente i propri utenti ai ruoli:

Metodo di autentica zione	Prima dell'abil itazione del controllo dettagliato degli accessi	Dopo l'abilitazione del controllo dettagliato degli accessi	Attività amministrative
Policy basate su identità	Tutti gli utenti IAM che soddisfan o la policy IAM possono accedere al dominio.	Non è necessario abilitare il periodo di migrazione. OpenSearch Il servizio mappa automaticamente	1. Crea mappature di ruolo personali zzate sul dominio. 2. Elimina il default_role.

Metodo di autentica zione	Prima dell'abil itazione del controllo dettagliato degli accessi	Dopo l'abilitazione del controllo dettagliato degli accessi	Attività amministrative
		tutti gli utenti che soddisfano la policy IAM sul default_r ole in modo che possano continuar e ad accedere al dominio.	
Policy basate su IP	Tutti gli utenti degli indirizzi IP o dei blocchi CIDR consentit i possono accedere al dominio.	Durante il periodo di migrazione di 30 giorni, tutti gli utenti degli indirizzi IP o dei blocchi CIDR consentiti possono continuar e ad accedere al dominio.	1. Crea mappature di ruolo personali zzate sul dominio. 2. Aggiorna i tuoi client per fornire credenziali di autenticazione di base o credenziali IAM, a seconda della configurazione della mappatura dei ruoli. 3. Disabilitare il periodo di migrazione. Gli utenti degli indirizzi IP consentit i o dei blocchi CIDR che inviano richieste senza autenticazione di base o credenziali IAM perderanno l'accesso al dominio.

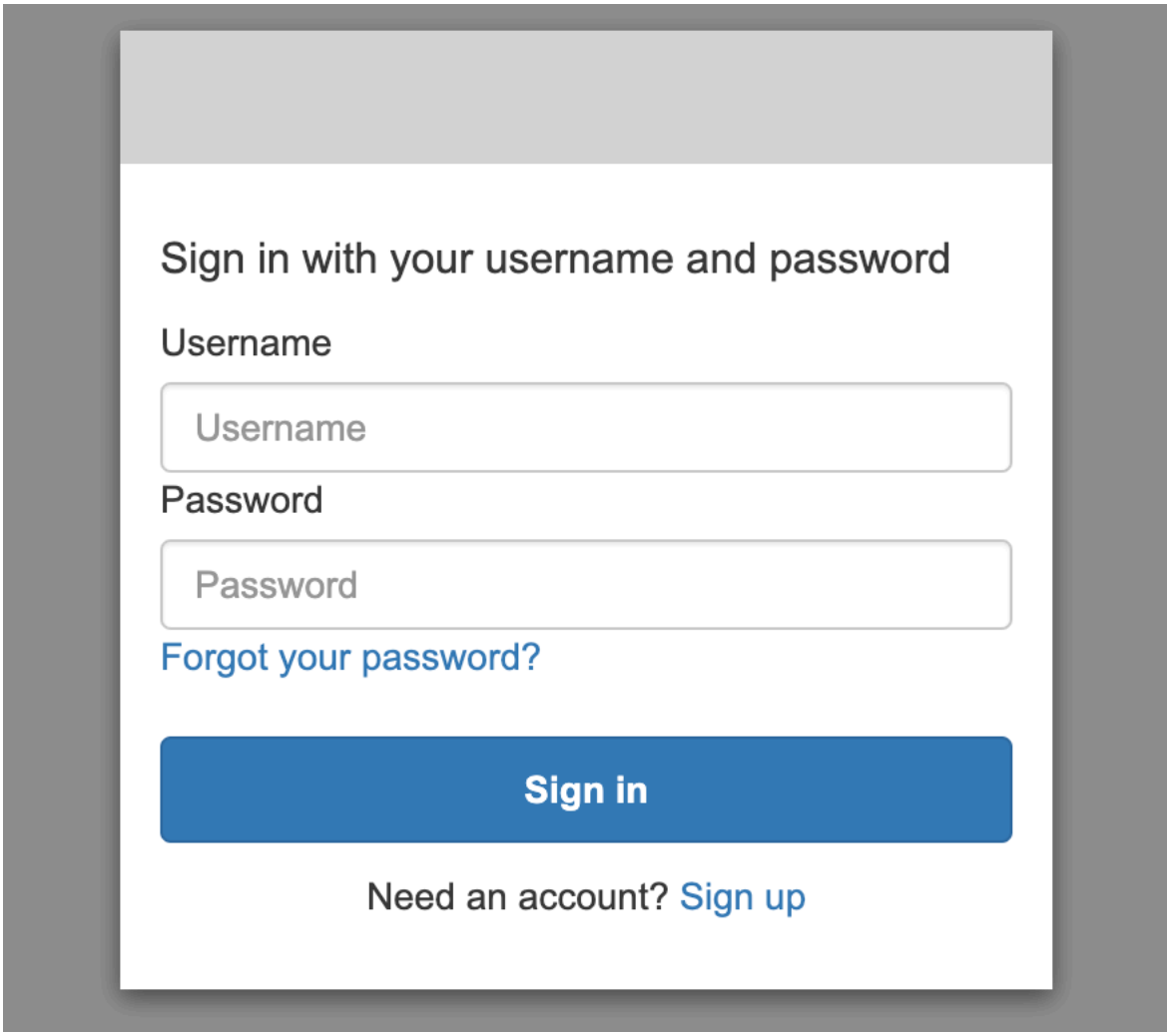
Metodo di autentica zione	Prima dell'abil itazione del controllo dettagliato degli accessi	Dopo l'abilitazione del controllo dettagliato degli accessi	Attività amministrative
Policy di accesso aperto	Tutti gli utenti su Internet possono accedere al dominio.	Durante il periodo di migrazione di 30 giorni, tutti gli utenti su Internet possono continuar e ad accedere al dominio.	1. Crea mappature dei ruoli sul dominio. 2. Aggiorna i tuoi client per fornire credenziali di autenticazione di base o credenziali IAM, a seconda della configurazione della mappatura dei ruoli. 3. Disabilitare il periodo di migrazione. Gli utenti che inviano richieste senza autenticazione di base o credenzia li IAM perderanno l'accesso al dominio.

Accesso alle OpenSearch dashboard come utente principale

Il controllo granulare degli accessi ha un plug-in OpenSearch Dashboards che semplifica le attività di gestione. È possibile utilizzare Dashboards per gestire utenti, ruoli, mappature, gruppi di operazioni e tenant. La pagina di accesso a OpenSearch Dashboards e il metodo di autenticazione sottostante differiscono, tuttavia, a seconda di come gestisci gli utenti e configuri il dominio.

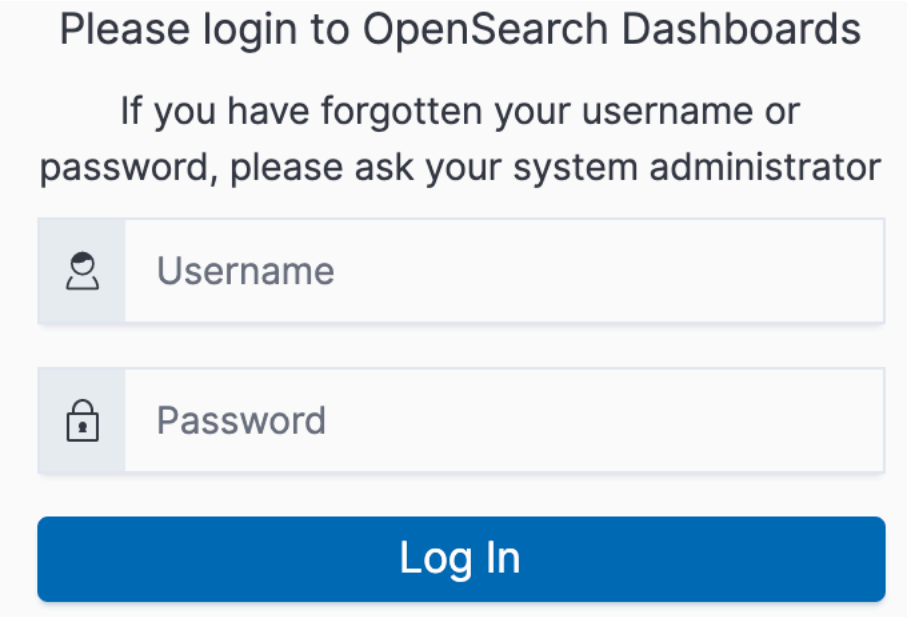
- Se si desidera utilizzare IAM per la gestione degli utenti, utilizzare the section called “Autenticazione Amazon Cognito per dashboard OpenSearch ” per accedere a Dashboards. Altrimenti, Dashboards mostra una pagina di accesso non funzionale. Per informazioni, consultare the section called “Limitazioni”.

  Con l'autenticazione di Amazon Cognito, uno dei ruoli assunti dal pool di identità deve corrispondere al ruolo IAM specificato per l'utente principale. Per ulteriori informazioni su questa configurazione, consulta the section called “(Facoltativo) Configurazione dell'accesso granulare” e the section called “Tutorial: controllo granulare degli accessi con autenticazione Cognito”.



- Se scegli di utilizzare il database utenti interno, puoi accedere a Dashboards con il nome utente e la password principali. È necessario accedere a Dashboards tramite HTTPS. L'autenticazione Amazon Cognito e SAML per Dashboards sostituiscono entrambe questa schermata di accesso.

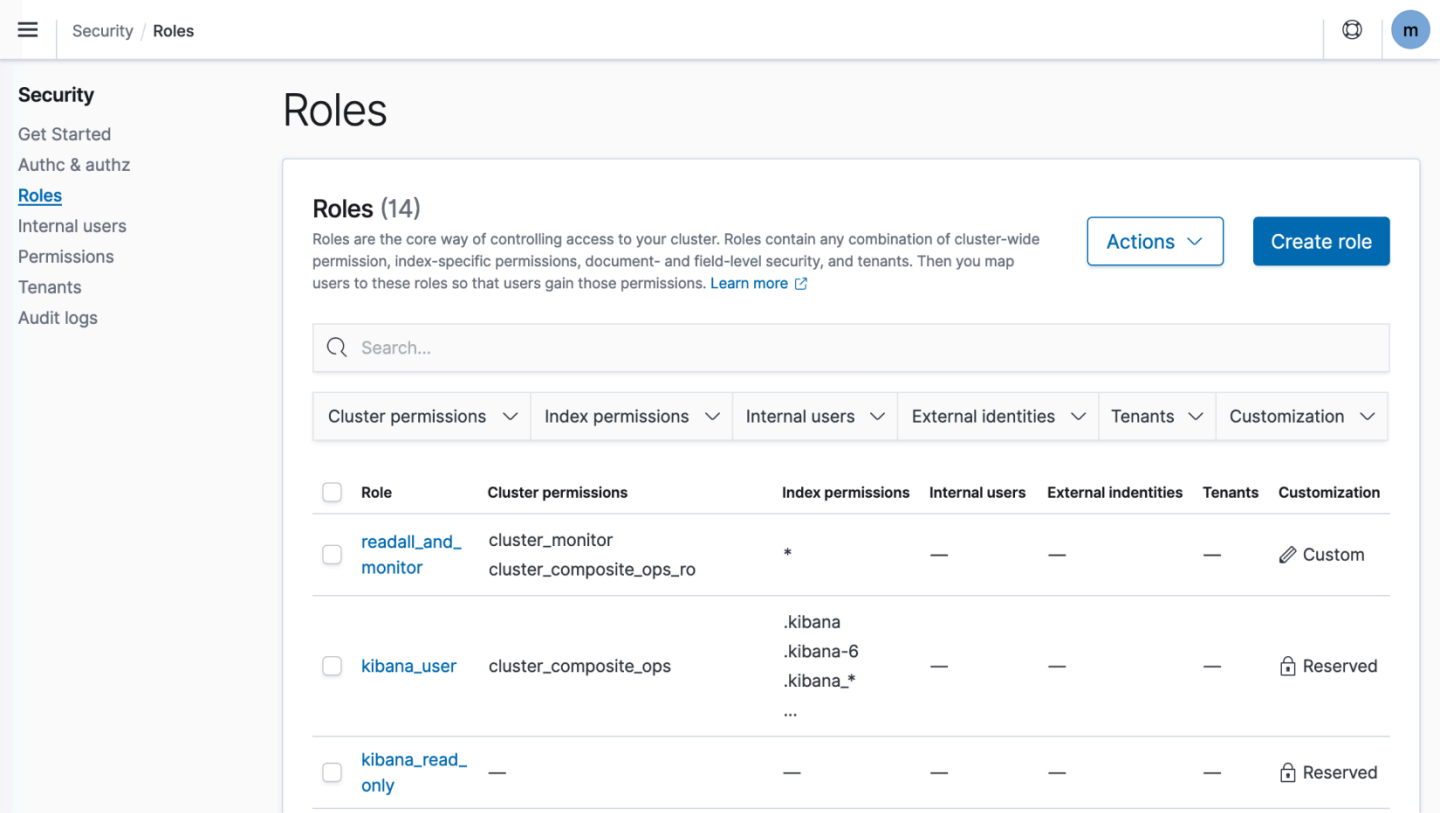
  Per ulteriori informazioni su questa configurazione, consulta the section called “Tutorial: Database utente interno e autenticazione di base”.



- Se si decide di utilizzare l'autenticazione SAML, è possibile accedere utilizzando le credenziali di un provider di identità esterno. Per ulteriori informazioni, consultare the section called “Autenticazione SAML per dashboard OpenSearch ”.

Gestione delle autorizzazioni

Come indicato in the section called “Concetti chiave”, è possibile gestire le autorizzazioni del controllo granulare degli accessi a utilizzando ruoli, utenti e mappature. In questa sezione viene descritto come creare e applicare tali risorse. Per eseguire queste operazioni si consiglia di accedere a Dashboards come utente principale.



> **Note**
>
> Le autorizzazioni che scegli di concedere agli utenti variano ampiamente in base al caso d'uso. Non possiamo coprire in maniera fattibile tutti gli scenari contenuti in questa documentazione. Mentre decidi quali autorizzazioni concedere ai tuoi utenti, assicurati di fare riferimento alle autorizzazioni per OpenSearch cluster e indice menzionate nelle sezioni seguenti e segui sempre il principio del privilegio minimo.

Creazione di ruoli

Puoi creare nuovi ruoli per il controllo granulare degli accessi utilizzando le OpenSearch dashboard o l'operazione nell'API REST. `_plugins/_security` Per ulteriori informazioni, consulta Creazione di ruoli.

Il controllo granulare degli accessi include anche numerosi ruoli predefiniti. Client come OpenSearch Dashboards e Logstash inviano un'ampia varietà di richieste OpenSearch, il che può rendere difficile la creazione manuale di ruoli con il set minimo di autorizzazioni. Ad esempio, il ruolo `opensearch_dashboards_user` include le autorizzazioni necessarie a un utente per utilizzare

modelli di indice, visualizzazioni, dashboard e tenant. Si consiglia di associarlo a qualsiasi ruolo utente o back-end che accede a Dashboards, insieme a ruoli aggiuntivi che consentono l'accesso ad altri indici.

Amazon OpenSearch Service non offre i seguenti OpenSearch ruoli:

- `observability_full_access`
- `observability_read_access`
- `reports_read_access`
- `reports_full_access`

Amazon OpenSearch Service offre diversi ruoli che non sono disponibili con OpenSearch:

- `ultrawarm_manager`
- `ml_full_access`
- `cold_manager`
- `notifications_full_access`
- `notifications_read_access`

Sicurezza a livello di cluster

Le autorizzazioni a livello di cluster includono la possibilità di eseguire richieste generiche quali `_mget`, `_msearch`, e `_bulk`, monitorare l'integrità, acquisire snapshot e altro ancora. Gestire queste autorizzazioni utilizzando la sezione Autorizzazioni cluster durante la creazione di un ruolo. Per l'elenco completo delle autorizzazioni a livello di cluster, consulta Autorizzazioni cluster.

Invece delle autorizzazioni individuali, spesso puoi ottenere la posizione di sicurezza desiderata utilizzando una combinazione di gruppi di azioni predefiniti. Per un elenco dei gruppi di operazioni a livello di cluster, consultare Livello di cluster.

Sicurezza a livello di indice

Le autorizzazioni a livello di indice includono la possibilità di creare nuovi indici, indici di ricerca, leggere e scrivere documenti, eliminare documenti, gestire alias e altro ancora. Gestire queste autorizzazioni utilizzando la sezione Autorizzazioni indice durante la creazione di un ruolo. Per l'elenco completo delle autorizzazioni a livello di indice, consulta Autorizzazioni indice.

Invece delle autorizzazioni individuali, spesso puoi ottenere la posizione di sicurezza desiderata utilizzando una combinazione di gruppi di azioni predefiniti. Per un elenco dei gruppi di operazioni a livello di indice, consultare Livello di indice.

Sicurezza a livello di documento

La sicurezza a livello di documento consente di limitare i documenti in un indice che un utente può visualizzare. Quando crei un ruolo, specifica uno schema di indice e una OpenSearch query. Tutti gli utenti che si associano a tale ruolo possono visualizzare solo i documenti corrispondenti alla query. La sicurezza a livello di documento influisce sul numero di visite ricevute durante la ricerca.

Per ulteriori informazioni, consultare Sicurezza a livello di documento.

Sicurezza a livello di campo

La sicurezza a livello di campo consente di controllare quali campi di documento possono essere visualizzati dall'utente. Quando si crea un ruolo, aggiungere un elenco di campi da includere o escludere. Se si includono campi, gli utenti per cui si esegue il mapping a tale ruolo possono visualizzare solo i campi. Se si escludono i campi, possono visualizzare tutti i campi tranne quelli esclusi. La sicurezza a livello di campo influisce sul numero di campi inclusi negli hit durante la ricerca.

Per ulteriori informazioni, consultare Sicurezza a livello di campo.

Mascheramento del campo

Il mascheramento dei campi è un'alternativa alla sicurezza a livello di campo che consente di anonimizzare i dati in un campo anziché rimuoverli del tutto. Quando si crea un ruolo, aggiungere un elenco di campi da mascherare. Il mascheramento dei campi influisce sulla possibilità di visualizzare il contenuto di un campo durante la ricerca.

> **Tip**
>
> Se applichi il mascheramento standard a un campo, OpenSearch Service utilizza un hash sicuro e casuale che può causare risultati di aggregazione imprecisi. Per eseguire aggregazioni su campi mascherati, utilizzare invece il mascheramento basato su modello.

Creazione di utenti

Se hai abilitato il database utenti interno, puoi creare utenti utilizzando le OpenSearch dashboard o l'`_plugins/_security`operazione nell'API REST. Per ulteriori informazioni, consultare Creazione di utenti.

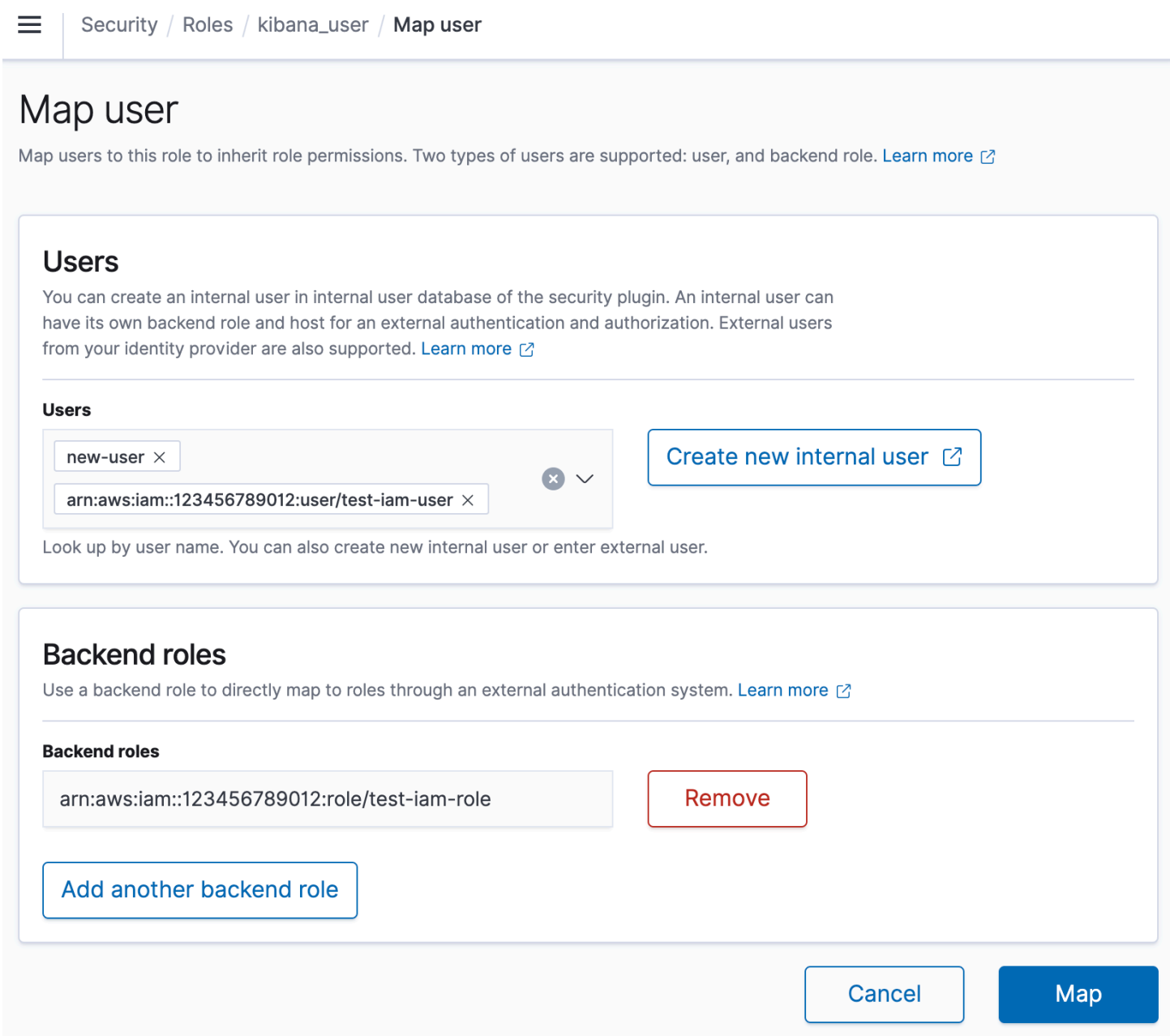
Se è stato scelto IAM per l'utente principale, ignorare questa parte di Dashboards. Creare invece ruoli IAM. Per ulteriori informazioni, consultare la Guida per l'utente IAM.

Mappatura dei ruoli agli utenti

La mappatura dei ruoli è l'aspetto più critico del controllo granulare degli accessi. Il controllo granulare degli accessi dispone di alcuni ruoli predefiniti che consentono di iniziare, ma a meno che non si esegua la mappatura dei ruoli agli utenti, ogni richiesta al cluster termina con un errore di autorizzazioni.

I ruoli di backend possono aiutare a semplificare il processo di mappatura dei ruoli. Invece di mappare lo stesso ruolo a 100 singoli utenti, puoi mappare il ruolo a un singolo ruolo di backend condiviso da tutti i 100 utenti. I ruoli di back-end possono essere ruoli IAM o stringhe arbitrarie.

- Nella sezione Users (Utenti), specifica utenti, ARN di utenti e stringhe utente di Amazon Cognito. Le stringhe utente di Cognito assumono la forma di `Cognito/`*`user-pool-id`*`/`*`username`*.
- Specificare i ruoli di back-end e gli ARN del ruolo IAM nella sezione Ruoli di back-end .



Puoi mappare i ruoli agli utenti utilizzando OpenSearch le dashboard o l'`_plugins/_security`operazione nell'API REST. Per ulteriori informazioni, consultare Mappa utenti ai ruoli.

Creazione di gruppi di operazioni

I gruppi di azioni sono insiemi di autorizzazioni che è possibile riutilizzare in diverse risorse. È possibile creare nuovi gruppi di azioni utilizzando OpenSearch le dashboard o l'`_plugins/_security`operazione nell'API REST, sebbene i gruppi di azioni predefiniti siano sufficienti per la

maggior parte dei casi d'uso. Per ulteriori informazioni sui gruppi di operazioni predefiniti, consultare Gruppi di operazioni predefiniti.

OpenSearch Dashboard multi-tenancy

I tenant sono spazi per salvare modelli di indici, visualizzazioni, pannelli di controllo e altri oggetti Dashboards. La funzionalità multi-tenancy di Dashboards ti consente di condividere in sicurezza il tuo lavoro con altri utenti di Dashboards (o di mantenerlo privato) e di configurare dinamicamente i tenant. È possibile controllare quali ruoli hanno accesso a un tenant e se tali ruoli hanno accesso in lettura o in scrittura. Il tenant globale è l'impostazione predefinita. Per ulteriori informazioni, consulta Dashboards multi-tenancy. OpenSearch

Per visualizzare il tenant corrente o modificare i tenant

1. Vai alle OpenSearch dashboard e accedi.
2. Seleziona l'icona utente in alto a destra e sceglie Cambia tenant.
3. Verificare il tenant prima di creare visualizzazioni o dashboard. Se si desidera condividere il proprio lavoro con tutti gli altri utenti di Dashboards, scegliere Globale. Per condividere il lavoro con un sottoinsieme di utenti di Dashboards, scegliere un tenant condiviso diverso. Altrimenti, scegli Privato.

> **Note**
>
> OpenSearch Dashboards mantiene un indice separato per ogni tenant e crea un modello di indice chiamato. `tenant_template` Non eliminate o modificate l'`tenant_template`indice, poiché se la mappatura dell'indice dei tenant non è configurata correttamente, ciò potrebbe causare il malfunzionamento dei OpenSearch dashboard.

Configurazioni consigliate

A causa del modo in cui il controllo granulare degli accessi interagisce con altre funzionalità di sicurezza, consigliamo diverse configurazioni di controllo granulare degli accessi che funzionano bene per la maggior parte dei casi d'uso.

Descrizione	Utente principale	Policy di accesso al dominio
Utilizza le credenziali IAM per le chiamate alle OpenSearch API e utilizza l'autenticazione SAML per accedere alle dashboard. Gestire i ruoli del controllo granulare degli accessi utilizzando Dashboards o la REST API.	Utente o ruolo IAM	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`
Utilizza le credenziali IAM o l'autenticazione di base per le chiamate alle API. OpenSearch Gestire i ruoli del controllo granulare degli accessi utilizzando Dashboards o la REST API. Questa configurazione offre molta flessibil ità, soprattutto se hai OpenSearch client che supportano solo l'autenti cazione di base. Se si dispone di un provider di identità esistente, utilizzare Autenticazione SAML per accedere a Dashboards.	Nome utente e password	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`

Descrizione	Utente principale	Policy di accesso al dominio
In caso contrario, gestire gli utenti di Dashboards nel database interno degli utenti.		

Usa le credenziali IAM per le chiamate alle OpenSearch API e usa Amazon Cognito per accedere alle dashboard. Gestire i ruoli del controllo granulare degli accessi utilizzando Dashboards o la REST API.	Utente o ruolo IAM	<pre>{
		  "Version": "2012-10-17",
		  "Statement": [
		  {
		  "Effect": "Allow",
		  "Principal": {
		  "AWS": "*"
		  },
		  "Action": "es:ESHttp*",
		  "Resource": " *domain-arn* /*"
		  }
		  ]
		}</pre>

Descrizione	Utente principale	Policy di accesso al dominio

Utilizza le credenziali IAM per le chiamate alle OpenSearch API e blocca la maggior parte degli accessi alle dashboard. Gestire i ruoli del controllo granulare degli accessi utilizzando la REST API.	Utente o ruolo IAM	<pre>{
		  "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*"
		    }
		  ]
		}</pre>

Limitazioni

Il controllo granulare degli accessi presenta diverse limitazioni importanti:

- L'aspetto `hosts` delle mappature dei ruoli, che associa i ruoli a nomi host o indirizzi IP, non funziona se il dominio è all'interno di un VPC. È comunque possibile mappare i ruoli agli utenti e ai ruoli di back-end.
- Se sceglisi sceglie IAM per l'utente principale e non abilitisi abilita l'autenticazione Amazon Cognito o SAML, Dashboards visualizza una pagina di accesso non funzionante.funzionale.
- Se si sceglie IAM per l'utente master, è comunque possibile creare utenti nel database utente interno. Poiché l'autenticazione di base HTTP non è abilitata in questa configurazione, tutte le richieste firmate con tali credenziali utente vengono rifiutate.

- Se si utilizza SQL per eseguire una query su un indice a cui non si ha accesso, viene visualizzato un errore "no permissions". Se l'indice non esiste, viene visualizzato un errore «tale indice è inesistente». Questa differenza nei messaggi di errore significa che puoi confermare l'esistenza di un indice se ti capita di indovinare il suo nome.

  Per ridurre al minimo il problema, non includere informazioni riservate nei nomi degli indici. Per negare tutti gli accessi a SQL, aggiungere il seguente elemento alla policy di accesso del dominio:

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": [
      "*"
    ]
  },
  "Action": [
    "es:*"
  ],
  "Resource": "arn:aws:es:us-east-1:123456789012:domain/my-domain/_plugins/_sql"
}
```

- Se la versione del tuo dominio è 2.3 o successiva e hai abilitato il controllo granulare degli accessi, l'impostazione su 1 causa problemi con `max_clause_count` il dominio. Ti consigliamo di impostare questo account su un numero più alto.
- Se stai abilitando il controllo granulare degli accessi in un dominio in cui non è impostato il controllo granulare degli accessi, per le fonti di dati create per l'interrogazione diretta, devi configurare tu stesso ruoli di controllo degli accessi granulari. Per ulteriori informazioni su come configurare ruoli di accesso granulari, consulta Creazione di integrazioni di origini dati Amazon OpenSearch Service con Amazon S3.

Modifica dell'utente principale

Se si dimenticano i dettagli dell'utente master, è possibile riconfigurarlo utilizzando la console, AWS CLI o l'API di configurazione.

Per modificare l'utente master (console)

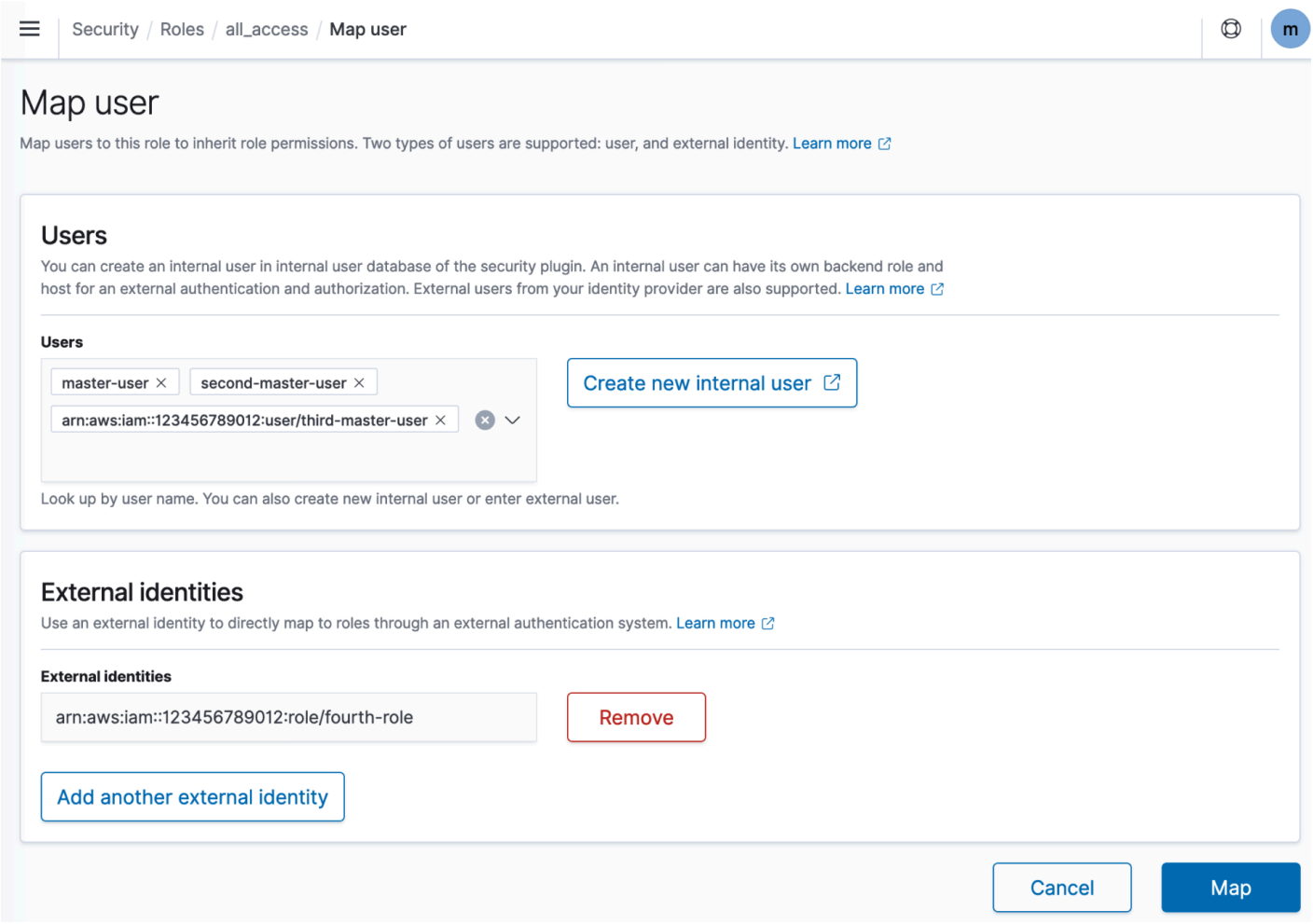
1. Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home/.

2. Seleziona il dominio e scegli Actions (Operazioni) quindi Edit security configuration (Modifica configurazione di sicurezza).
3. Scegliere Imposta ARN IAM come utente principale o Crea utente principale.
   - Se in precedenza è stato utilizzato un utente master IAM, il controllo granulare degli accessi esegue nuovamente la mappatura del ruolo `all_access` al nuovo ARN IAM specificato.
   - Se in precedenza è stato utilizzato il database utente interno, il controllo granulare degli accessi crea un nuovo utente principale. È possibile utilizzare il nuovo utente master per eliminare quello vecchio.
   - Il passaggio dal database utente interno a un utente principale IAM non elimina gli utenti dal database utente interno. Invece, disabilita semplicemente l'autenticazione di base HTTP. Eliminare manualmente gli utenti dal database utente interno o conservarli nel caso in cui sia necessario riabilitare l'autenticazione di base HTTP.
4. Seleziona Salvataggio delle modifiche.

Utenti principali aggiuntivi

Si designa un utente master quando si crea un dominio, ma se si desidera, è possibile utilizzare questo utente master per creare ulteriori utenti master. Hai due opzioni: OpenSearch dashboard o API REST.

- In Dashboards scegliere Sicurezza, Ruoli, quindi associare il nuovo utente principale ai ruoli `all_access` e `security_manager`.



- Per utilizzare la REST API, inviare le seguenti richieste:

```
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"
  ]
}
```

Queste richieste sostituiscono le mappature dei ruoli correnti, quindi eseguire prima le richieste `GET` in modo da poter includere tutti i ruoli correnti nelle richieste `PUT`. La REST API è particolarmente utile se non è possibile accedere a Dashboards e si desidera mappare un ruolo IAM da Amazon Cognito al ruolo `all_access`.

Snapshot manuali

Il controllo granulare degli accessi introduce alcune complicazioni aggiuntive con l'acquisizione di snapshot manuali. Per registrare un repository di snapshot, anche se si utilizza l'autenticazione di base HTTP per tutti gli altri scopi, è necessario associare il ruolo `manage_snapshots` a un ruolo IAM che dispone delle autorizzazioni `iam:PassRole` per assumere `TheSnapshotRole`, come definito in the section called “Prerequisiti”.

Utilizzare quindi il ruolo IAM per inviare una richiesta firmata al dominio, come descritto in the section called “Registrazione di un repository di snapshot manuali”.

Integrazioni

Se utilizzi altri AWS servizi con OpenSearch Service, devi fornire i ruoli IAM per tali servizi con le autorizzazioni appropriate. Ad esempio, i flussi di distribuzione di Firehose utilizzano spesso un ruolo IAM chiamato. `firehose_delivery_role` In Dashboards, creare un ruolo per il controllo granulare degli accessi e mappare il ruolo IAM a tale ruolo. In questo caso, il nuovo ruolo richiede le seguenti autorizzazioni:

```
{
  "cluster_permissions": [
    "cluster_composite_ops",
    "cluster_monitor"
  ],
```

```
  "index_permissions": [{
    "index_patterns": [
      "firehose-index*"
    ],
    "allowed_actions": [
      "create_index",
      "manage",
      "crud"
    ]
  }]
}
```

Le autorizzazioni variano in base alle azioni eseguite da ciascun servizio. Una AWS IoT regola o una AWS Lambda funzione che indicizza i dati richiede probabilmente autorizzazioni simili a quelle di Firehose, mentre una funzione Lambda che esegue solo ricerche può utilizzare un set più limitato.

Differenze della REST API

L'API REST per il controllo degli accessi a grana fine differisce leggermente a seconda della versione di /Elasticsearch. OpenSearch Prima di effettuare una richiesta PUT, effettuare una richiesta GET per verificare il corpo della richiesta previsto. Ad esempio, una richiesta GET per `_plugins/_security/api/user` restituisce tutti gli utenti, che è possibile modificare e utilizzare per effettuare richieste PUT valide.

In Elasticsearch 6.x, le richieste per creare utenti hanno il seguente aspetto:

```
PUT _opendistro/_security/api/user/new-user
{
  "password": "some-password",
  "roles": ["new-backend-role"]
}
```

Su OpenSearch o Elasticsearch 7.x, le richieste hanno questo aspetto (cambia se usi Elasticsearch): `_plugins` `_opendistro`

```
PUT _plugins/_security/api/user/new-user
{
  "password": "some-password",
  "backend_roles": ["new-backend-role"]
}
```

Inoltre, i tenant sono proprietà dei ruoli in Elasticsearch 6.x:

```
GET _opendistro/_security/api/roles/all_access

{
  "all_access": {
    "cluster": ["UNLIMITED"],
    "tenants": {
      "admin_tenant": "RW"
    },
    "indices": {
      "*": {
        "*": ["UNLIMITED"]
      }
    },
    "readonly": "true"
  }
}
```

In OpenSearch Elasticsearch 7.x, sono oggetti con un proprio URI (modificalo se usi Elasticsearch):: `_plugins` `_opendistro`

```
GET _plugins/_security/api/tenants

{
  "global_tenant": {
    "reserved": true,
    "hidden": false,
    "description": "Global tenant",
    "static": false
  }
}
```

Per la documentazione sull'API OpenSearch REST, consulta il riferimento all'API del plug-in di sicurezza.

Tip

Se si utilizza il database utente interno, è possibile utilizzare curl per effettuare richieste e testare il dominio. Provare i seguenti comandi di esempio:

```
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: configurazione di un dominio con un utente master IAM e autenticazione Amazon Cognito

Questo tutorial tratta un popolare caso d'uso di Amazon OpenSearch Service per il controllo granulare degli accessi: un utente master IAM con autenticazione Amazon Cognito per dashboard. OpenSearch

Nel tutorial configureremo un ruolo IAM master e un ruolo IAM limitato, che poi assoceremo agli utenti in Amazon Cognito. L'utente master può quindi accedere a OpenSearch Dashboards, mappare l'utente limitato a un ruolo e utilizzare un controllo granulare degli accessi per limitare le autorizzazioni dell'utente.

Sebbene questi passaggi utilizzino il bacino d'utenza di Amazon Cognito per l'autenticazione, questo stesso processo di base funziona per qualsiasi provider di autenticazione Cognito che consente di assegnare ruoli IAM differenti a utenti diversi.

In questo tutorial completerai le seguenti fasi:

1. Creazione di ruoli IAM master e limitati
2. Creazione di un dominio con l'autenticazione Cognito
3. Configurare un pool di utenti e un pool di identità di Cognito
4. Mappa i ruoli nelle dashboard OpenSearch
5. Test delle autorizzazioni

Fase1: Creazione di ruoli IAM master e limitati

Passa alla console AWS Identity and Access Management (IAM) e crea due ruoli separati:

- `MasterUserRole` - L'utente master, che disporrà di autorizzazioni complete per il cluster e gestirà ruoli e mappature dei ruoli.
- `LimitedUserRole` - Un ruolo più limitato, a cui come utente master concederai un accesso limitato.

Per istruzioni sulla creazione dei ruoli, consulta la pagina Creazione di un ruolo utilizzando policy di attendibilità personalizzate.

Entrambi i ruoli devono disporre della seguente policy di attendibilità che consente al pool di identità Cognito di assumere i ruoli:

```
{
  "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**
>
> Sostituzione di `identity-pool-id` con l'identificatore univoco del pool di identità Amazon Cognito. Ad esempio, `us-east-1:0c6cdba7-3c3c-443b-a958-fb9feb207aa6`.

Fase 2: Creazione di un dominio con l'autenticazione Cognito

Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home/ e crea un dominio con le seguenti impostazioni:

- OpenSearch 1.0 o versione successiva oppure Elasticsearch 7.8 o versione successiva
- Accesso pubblico
- Controllo granulare degli accessi abilitato con `MasterUserRole` come utente master (creato nella fase precedente)
- Autenticazione Amazon Cognito abilitata per le OpenSearch dashboard. Per le istruzioni sull'abilitazione dell'autenticazione Cognito e la selezione di un pool di utenti e identità, consulta the section called “Configurazione di un dominio per l'uso dell'autenticazione Amazon Cognito”.
- La seguente policy di accesso al dominio:

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

- HTTPS richiesto per tutto il traffico verso il dominio
- Nessuna crittografia ode-to-node
- Crittografia dei dati a riposo

Fase 3: Configurazione degli utenti di Cognito

Durante la creazione del dominio, configura gli utenti master e limitati all'interno di Amazon Cognito seguendo la procedura Crea un pool di utenti nella Amazon Cognito Developer Guide. Infine,

configura il tuo pool di identità seguendo i passaggi descritti in Creare un pool di identità in Amazon Cognito. Il bacino d'utenza e il pool di identità devono trovarsi nella stessa Regione AWS.

Fase 4: Mappa i ruoli nelle dashboard OpenSearch

Ora che gli utenti sono configurati, puoi accedere a OpenSearch Dashboards come utente principale e mappare gli utenti ai ruoli.

1. Torna alla console di OpenSearch servizio e vai all'URL delle OpenSearch dashboard per il dominio che hai creato. L'URL segue il seguente formato: *domain-endpoint*`/_dashboards/`.
2. Accedere con le credenziali `master-user`.
3. Scegliere Add sample data (Aggiungi dati di esempio) e aggiungere alcuni dati di volo di esempio.
4. Nel pannello di navigazione a sinistra, seleziona Security (Sicurezza), Roles (Ruoli) e Create role (Crea ruolo).
5. Denomina il ruolo `new-role`.
6. Per Index (Indice), specificare `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*` sui domini Elasticsearch).
7. Per Index permissions (Autorizzazioni relative all'indice), scegliere read (lettura).
8. Per Sicurezza a livello di documento, specificare la seguente query:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

9. Per la sicurezza a livello di campo, scegliere Escludi e specificare `FlightNum`.
10. Per Anonimizzazione, specificare `Dest`.
11. Scegliere Create (Crea) .
12. Scegliere Utenti mappati, Gestisci mappatura. Aggiungere il nome della risorsa Amazon (ARN) per `LimitedUserRole` come identità esterna e scegliere Map (Mappa).
13. Torna all'elenco di ruoli e scegli opensearch_dashboards_user. Scegliere Utenti mappati, Gestisci mappatura. Aggiungere l'ARN per `LimitedUserRole` come ruolo di back-end e scegliere Mappa.

Fase 5: Test delle autorizzazioni

Quando i ruoli sono mappati correttamente, puoi accedere come utente limitato e testare le autorizzazioni.

1. In una nuova finestra privata del browser, vai all'URL della OpenSearch dashboard per il dominio, accedi utilizzando le `limited-user` credenziali e scegli Esplora da solo.
2. Scegliere Strumenti di sviluppo ed eseguire la ricerca predefinita:

   ```
   GET _search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Notare l'errore di autorizzazioni. `limited-user` non dispone delle autorizzazioni per eseguire ricerche a livello di cluster.
3. Esegui un'altra ricerca:

   ```
   GET opensearch_dashboards_sample_data_flights/_search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Si noti che tutti i documenti corrispondenti hanno un campo `FlightDelay` di `true`, un campo `Dest` anonimizzato e nessun campo `FlightNum`.
4. Nella finestra del browser originale, accedere come `master-user`, scegliere Strumenti di sviluppo, e quindi eseguire le stesse ricerche. Nota la differenza tra autorizzazioni, numero di hit, documenti corrispondenti e campi inclusi.

Tutorial: Configurare un dominio con il database utente interno e l'autenticazione di base HTTP

Questo tutorial tratta un altro popolare caso d'uso dettagliato del controllo degli accessi: un utente principale nel database utenti interno e l'autenticazione di base HTTP per Dashboards. OpenSearch

L'utente master può quindi accedere alle OpenSearch dashboard, creare un utente interno, mappare l'utente a un ruolo e utilizzare un controllo granulare degli accessi per limitare le autorizzazioni dell'utente.

In questo tutorial completerai le seguenti fasi:

1. Crea un dominio con un utente principale
2. Configura un utente interno nelle OpenSearch dashboard
3. Mappa i ruoli nelle dashboard OpenSearch
4. Test delle autorizzazioni

Fase 1: Creazione di un dominio

Accedi alla console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home/ e crea un dominio con le seguenti impostazioni:

- OpenSearch 1.0 o versione successiva oppure Elasticsearch 7.9 o versione successiva
- Accesso pubblico
- Controllo granulare degli accessi con un utente principale nel database utente interno (`TheMasterUser` per il resto di questo tutorial)
- Autenticazione Amazon Cognito per Dashboards disabilitata
- La seguente policy di accesso:

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

- HTTPS richiesto per tutto il traffico verso il dominio
- Nessuna crittografia ode-to-node
- Crittografia dei dati a riposo

Fase 2: Creare un utente interno nelle OpenSearch dashboard

Ora che hai un dominio, puoi accedere alle OpenSearch dashboard e creare un utente interno.

1. Torna alla console di OpenSearch servizio e vai all'URL delle OpenSearch dashboard per il dominio che hai creato. L'URL segue il seguente formato: *domain-endpoint*`/_dashboards/`.
2. Accedi con. `TheMasterUser`
3. Scegliere Add sample data (Aggiungi dati di esempio) e aggiungere alcuni dati di volo di esempio.
4. Nel riquadro di navigazione a sinistra, scegli Sicurezza, Utenti interni, Crea utente interno.
5. Denominare l'utente `new-user` e specificare una password. Quindi, scegli Create (Crea).

Passaggio 3: mappare i ruoli nelle OpenSearch dashboard

Ora che l'utente è configurato, puoi mappare l'utente a un ruolo.

1. Resta nella sezione Sicurezza delle OpenSearch dashboard e scegli Ruoli, Crea ruolo.
2. Denomina il ruolo `new-role`.
3. Per Index, specifica `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*`sui domini Elasticsearch) il modello di indice.
4. Per il gruppo di operazioni, scegliere read.
5. Per Sicurezza a livello di documento, specificare la seguente query:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

6. Per la sicurezza a livello di campo, scegliere Escludi e specificare `FlightNum`.
7. Per Anonimizzazione, specificare `Dest`.
8. Scegliere Create (Crea) .

9. Scegliere Utenti mappati, Gestisci mappatura. Quindi aggiungere `new-user` a Utenti e scegliere Mappa.
10. Torna all'elenco di ruoli e scegli opensearch_dashboards_user. Scegliere Utenti mappati, Gestisci mappatura. Quindi aggiungere `new-user` a Utenti e scegliere Mappa.

Passaggio 4: Verifica le autorizzazioni

Quando i ruoli sono mappati correttamente, puoi accedere come utente limitato e testare le autorizzazioni.

1. In una nuova finestra privata del browser, vai all'URL della OpenSearch dashboard per il dominio, accedi utilizzando le `new-user` credenziali e scegli Esplora da solo.
2. Scegliere Strumenti di sviluppo ed eseguire la ricerca predefinita:

   ```
   GET _search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Notare l'errore di autorizzazioni. `new-user` non dispone delle autorizzazioni per eseguire ricerche a livello di cluster.
3. Esegui un'altra ricerca:

   ```
   GET dashboards_sample_data_flights/_search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Si noti che tutti i documenti corrispondenti hanno un campo `FlightDelay` di `true`, un campo `Dest` anonimizzato e nessun campo `FlightNum`.
4. Nella finestra del browser originale, accedere come `TheMasterUser`, scegliere Strumenti di sviluppo ed eseguire le stesse ricerche. Nota la differenza tra autorizzazioni, numero di hit, documenti corrispondenti e campi inclusi.

Convalida della conformità per Amazon Service OpenSearch

I revisori di terze parti valutano la sicurezza e la conformità del OpenSearch servizio Amazon nell'ambito di diversi programmi di AWS conformità. Questi programmi includono SOC, PCI e HIPAA.

Se hai requisiti di conformità, prendi in considerazione l'utilizzo di qualsiasi versione di Elasticsearch 6.0 OpenSearch o successiva. Le versioni precedenti di Elasticsearch non offrono una combinazione di crittografia dei dati archiviati e node-to-node crittografia ed è improbabile che soddisfino le tue esigenze. Potresti anche prendere in considerazione l'utilizzo di qualsiasi versione di Elasticsearch 6.7 OpenSearch o successiva se il controllo granulare degli accessi è importante per il tuo caso d'uso. Indipendentemente da ciò, la scelta di una versione particolare OpenSearch o di Elasticsearch quando si crea un dominio non garantisce la conformità.

Per sapere se una Servizio AWS rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Ambito per programma di conformitàServizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.

- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Amazon OpenSearch Service

L'infrastruttura globale di AWS è progettata attorno a Regioni AWS e zone di disponibilità. Regioni AWS fornisce più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire le applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, fault tolerant e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Oltre all'infrastruttura globale AWS, OpenSearch Service offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup.

- Domini Multi-AZ e partizioni di replica

- Snapshot automatiche e manuali

Autenticazione e autorizzazione JWT per Amazon Service OpenSearch

Amazon OpenSearch Service ora ti consente di utilizzare JSON Web Tokens (JWT) per l'autenticazione e l'autorizzazione. I JWT sono token di accesso basati su JSON utilizzati per concedere l'accesso Single Sign-On (SSO). Puoi utilizzare JWTS in OpenSearch Service per creare token Single Sign-on per convalidare le richieste al tuo dominio di servizio. OpenSearch Per utilizzare JWT, devi avere abilitato il controllo degli accessi a grana fine e devi fornire una chiave pubblica valida in formato RSA o ECDSA PEM. Per ulteriori informazioni sul controllo granulare degli accessi, consulta Controllo granulare degli accessi in Amazon Service. OpenSearch

Puoi configurare i token Web JSON utilizzando la console di OpenSearch servizio, il () o gli SDK. AWS Command Line Interface AWS CLI AWS

Considerazioni

Prima di utilizzare JWTS con Amazon OpenSearch Service, devi considerare quanto segue:

- A causa delle dimensioni delle chiavi pubbliche RSA in formato PEM, consigliamo di utilizzare la AWS console per configurare l'autenticazione e l'autorizzazione JWT.
- È necessario fornire utenti e ruoli validi quando si specificano i campi soggetti e ruoli per i JWT, altrimenti le richieste verranno rifiutate.

Modifica della policy di accesso al dominio

Prima di poter configurare il dominio per utilizzare l'autenticazione e l'autorizzazione JWT, è necessario aggiornare la politica di accesso al dominio per consentire agli utenti JWT di accedere al dominio. In caso contrario, tutte le richieste autorizzate JWT in entrata vengono rifiutate. La politica di accesso al dominio consigliata per fornire l'accesso completo alle risorse secondarie (/*) è:

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

```
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

Configurazione dell'autenticazione e dell'autorizzazione JWT

È possibile abilitare l'autenticazione e l'autorizzazione JWT durante il processo di creazione del dominio o aggiornando un dominio esistente. I passaggi di configurazione variano leggermente a seconda dell'opzione scelta.

I passaggi seguenti spiegano come configurare un dominio esistente per l'autenticazione e l'autorizzazione JWT nella console di OpenSearch servizio:

1. In Configurazione del dominio, vai su Autenticazione e autorizzazione JWT per OpenSearch, seleziona Abilita autenticazione e autorizzazione JWT.
2. Configura la chiave pubblica da utilizzare per il tuo dominio. Per fare ciò, puoi caricare un file PEM contenente una chiave pubblica o inserirlo manualmente.

   > **Note**
   >
   > Se la chiave caricata o inserita non è valida, verrà visualizzato un avviso sopra la casella di testo che specifica il problema.

3. (Facoltativo) In Impostazioni aggiuntive, puoi configurare i seguenti campi opzionali

   - Chiave dell'oggetto: puoi lasciare vuoto questo campo per utilizzare la `sub` chiave predefinita per i tuoi JWT.
   - Chiave dei ruoli: puoi lasciare vuoto questo campo per utilizzare la `roles` chiave predefinita per i tuoi JWT.

   Dopo aver apportato le modifiche, salva il dominio.

Utilizzo di un JWT per inviare una richiesta di test

Dopo aver creato un nuovo JWT con una coppia di soggetto e ruolo specificata, puoi inviare una richiesta di test. Per fare ciò, usa la chiave privata per firmare la tua richiesta tramite lo strumento che ha creato il JWT. OpenSearch Il servizio è in grado di convalidare la richiesta in arrivo verificando questa firma.

> **Note**
>
> Se hai specificato una chiave dell'oggetto o una chiave di ruolo personalizzata per il tuo JWT, devi utilizzare i nomi di claim corretti per il tuo JWT.

Di seguito è riportato un esempio di come utilizzare un token JWT per accedere al OpenSearch servizio tramite l'endpoint di ricerca del dominio:

```
curl -XGET "$search_endpoint" -H "Authorization: Bearer <JWT>"
```

Configurazione dell'autenticazione e dell'autorizzazione JWT ()AWS CLI

Il AWS CLI comando seguente abilita l'autenticazione e l'autorizzazione JWT a OpenSearch condizione che il dominio esista:

```
aws opensearch update-domain-config --domain-name <your_domain_name> --advanced-
security-options '{"JWTOptions":{"Enabled":true, "PublicKey": "<your_public_key>",
 "SubjectKey": "<your_subject_key>", "RolesKey": "<your_roles_key>"}}'
```

Configurazione dell'autenticazione e dell'autorizzazione JWT (configurazione tramite API)

La seguente richiesta all'API di configurazione abilita l'autenticazione e l'autorizzazione JWT OpenSearch su un dominio esistente:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "JWTOptions": {
      "Enabled": true,
      "PublicKey": "public-key",
      "RolesKey": "optional-roles-key",
      "SubjectKey": "optional-subject-key"
```

```
    }
  }
}
```

Generazione di una key pair

Per configurare JWT per il tuo OpenSearch dominio, dovrai fornire una chiave pubblica in formato Privacy-Enhanced Mail (PEM). Amazon OpenSearch Service attualmente supporta due algoritmi di crittografia asimmetrica quando si utilizzano JWT: RSA ed ECDSA.

Per creare una coppia di key pair RSA utilizzando la libreria openssl comune, segui questi passaggi:

1. `openssl genrsa -out privatekey.pem 2048`
2. `openssl rsa -in privatekey.pem -pubout -out publickey.pem`

In questo esempio, il `publickey.pem` file contiene la chiave pubblica da utilizzare con Amazon OpenSearch Service, mentre `privatekey.pem` contiene quella privata per la firma dei JWT inviati al servizio. Inoltre, hai la possibilità di convertire la chiave privata nel `pkcs8` formato comunemente usato se ne hai bisogno per generare i tuoi JWT.

Se utilizzi il pulsante di caricamento per aggiungere un file PEM direttamente alla console, il file deve avere un'`.pem`estensione o altre estensioni di file come `.crt.cert`, o non `.key` sono attualmente supportate.

Sicurezza dell'infrastruttura in Amazon OpenSearch Service

In quanto servizio gestito, Amazon OpenSearch Service è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Si utilizzano chiamate API AWS pubblicate per accedere al OpenSearch servizio attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Si utilizzano chiamate API AWS pubblicate per accedere all'API OpenSearch di configurazione del servizio tramite la rete. Per configurare la versione TLS minima richiesta da accettare, specificare il valore `TLSSecurityPolicy` nelle opzioni dell'endpoint di dominio:

```
aws opensearch update-domain-config --domain-name my-domain --domain-endpoint-options
 '{"TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"}'
```

Per maggiori dettagli, consulta la Guida di riferimento ai comandi dellaAWS CLI.

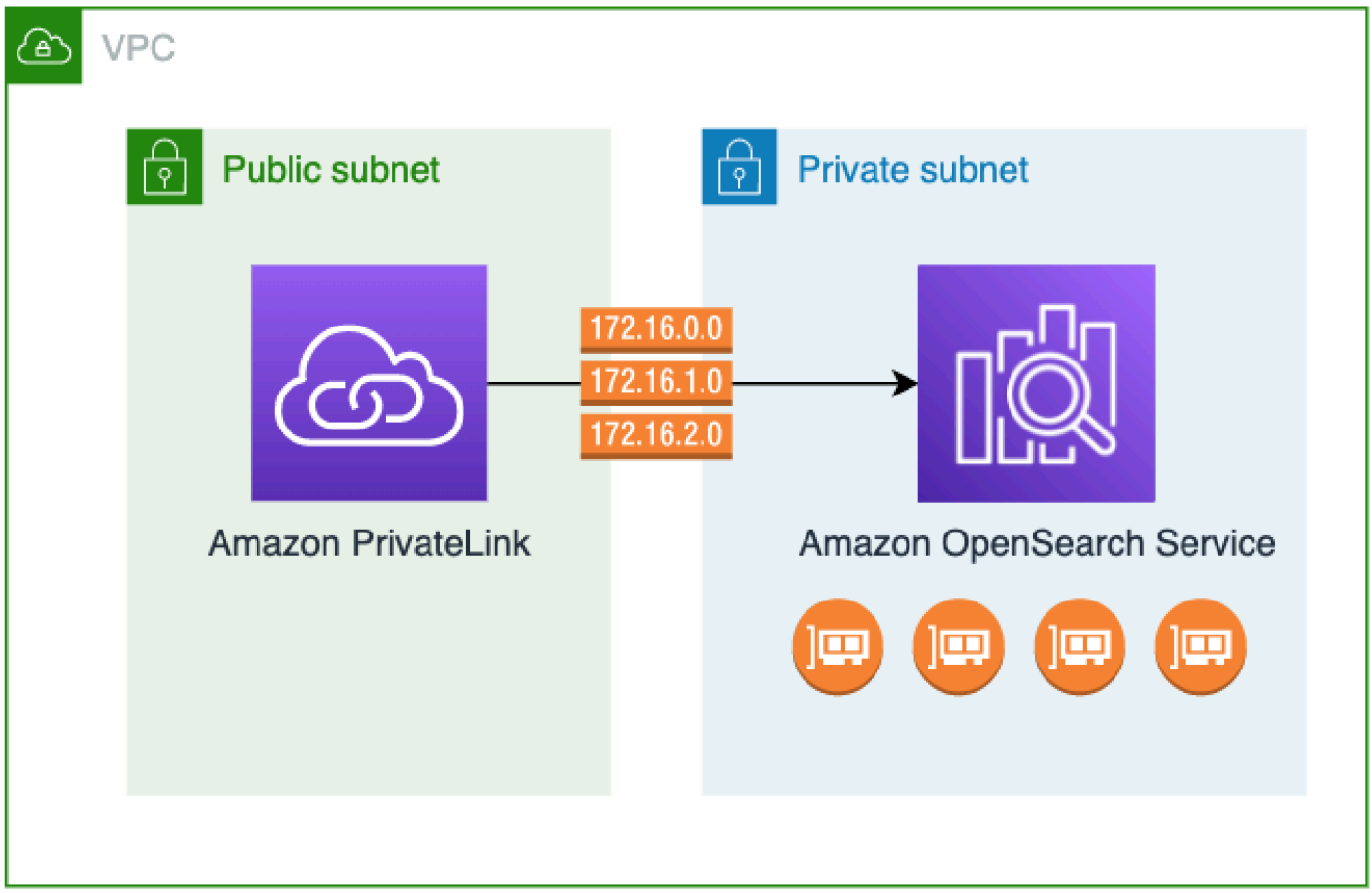
In base alla configurazione del dominio, potrebbe anche essere necessario firmare le richieste alle API OpenSearch . Per ulteriori informazioni, consulta the section called “Effettuazione e firma di richieste di servizio OpenSearch ”.

OpenSearch Il servizio supporta i domini di accesso pubblico, che possono ricevere richieste da qualsiasi dispositivo connesso a Internet, e i domini di accesso VPC, che sono isolati dalla rete Internet pubblica.

Accedi ad Amazon OpenSearch Service utilizzando un endpoint OpenSearch VPC gestito da Service ()AWS PrivateLink

Puoi accedere a un dominio Amazon OpenSearch Service configurando un endpoint OpenSearch VPC gestito dal servizio (fornito da). AWS PrivateLinkQuesti endpoint creano una connessione privata tra il tuo VPC e Amazon OpenSearch Service. Puoi accedere ai domini OpenSearch Service VPC come se fossero nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere al OpenSearch servizio.

Puoi configurare i domini OpenSearch di servizio per esporre endpoint aggiuntivi in esecuzione su sottoreti pubbliche o private all'interno dello stesso VPC, VPC diverso o diverso. Account AWSCiò consente di aggiungere un ulteriore livello di sicurezza per accedere ai domini indipendentemente da dove vengono eseguiti, senza alcuna infrastruttura da gestire. Il diagramma seguente illustra gli endpoint VPC OpenSearch gestiti dal servizio all'interno dello stesso VPC:



Si stabilisce questa connessione privata creando un endpoint VPC OpenSearch con interfaccia gestita dal servizio, alimentato da. AWS PrivateLinkIn ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint VPC dell'interfaccia. Si tratta di interfacce di rete gestite dal servizio che fungono da punto di ingresso per il traffico destinato al Servizio. OpenSearch I prezzi degli endpoint conAWS PrivateLink interfaccia standard si applicano agli endpoint VPC OpenSearch gestiti dal servizio fatturati a un prezzo inferiore. AWS PrivateLink

Puoi creare endpoint VPC per domini che eseguono tutte le versioni precedenti di OpenSearch Elasticsearch. Per ulteriori informazioni, consulta la sezione Accesso a Servizi AWS tramite AWS PrivateLink nella Guida diAWS PrivateLink .

Considerazioni e limitazioni per il servizio OpenSearch

Prima di configurare un endpoint VPC di interfaccia per il OpenSearch servizio, consulta le considerazioni nella Guida.AWS PrivateLink

Quando utilizzi gli endpoint OpenSearch VPC gestiti dal servizio, considera quanto segue:

- È possibile utilizzare solo gli endpoint VPC dell'interfaccia per connettersi ai domini VPC. I domini pubblici non sono supportati.
- Gli endpoint VPC possono connettersi solo ai domini all'interno della stessa Regione AWS.
- HTTPS è l'unico protocollo supportato per gli endpoint VPC. HTTP non è consentito.
- OpenSearch Il servizio supporta l'effettuazione di chiamate a tutte le operazioni OpenSearch API supportate tramite un endpoint VPC di interfaccia.
- Puoi configurare un massimo di 50 endpoint per account e un massimo di 10 endpoint per dominio. Un singolo dominio può avere un massimo di 10 principali autorizzati.
- Al momento non è possibile utilizzare AWS CloudFormation per creare endpoint VPC di interfaccia.
- È possibile creare endpoint VPC di interfaccia solo tramite la console di OpenSearch servizio o utilizzando l'OpenSearch API di servizio. Non puoi creare endpoint VPC di interfaccia per OpenSearch Service utilizzando la console Amazon VPC.
- OpenSearch Gli endpoint VPC gestiti dal servizio non sono accessibili da Internet. Un endpoint OpenSearch VPC gestito dai servizi è accessibile solo all'interno del VPC in cui viene fornito l'endpoint o di qualsiasi VPC collegato al VPC in cui viene fornito l'endpoint, come consentito dalle tabelle di routing e dai gruppi di sicurezza.
- Le policy degli endpoint VPC non sono supportate per Service. OpenSearch È possibile associare un gruppo di sicurezza alle interfacce di rete degli endpoint per controllare il traffico verso il OpenSearch servizio tramite l'interfaccia VPC endpoint.
- Il tuo ruolo collegato al servizio deve trovarsi nello stesso AWS account che usi per creare l'endpoint VPC.
- Per creare, aggiornare ed eliminare l'endpoint OpenSearch Service VPC, devi disporre delle seguenti autorizzazioni Amazon EC2 oltre alle autorizzazioni Amazon Service: OpenSearch
  - `ec2:CreateVpcEndpoint`
  - `ec2:DescribeVpcEndpoints`
  - `ec2:ModifyVpcEndpoint`
  - `ec2:DeleteVpcEndpoints`
  - `ec2:CreateTags`
  - `ec2:DescribeTags`
  - `ec2:DescribeSubnets`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeVpcs`

> **Note**
>
> Al momento, non puoi limitare la creazione di endpoint VPC a Service. OpenSearch Stiamo lavorando per renderlo possibile in un futuro aggiornamento.

Fornitura dell'accesso a un dominio

Se il VPC a cui desideri accedere al tuo dominio si trova in un altro Account AWS, devi autorizzarlo dall'account del proprietario prima di poter creare un endpoint VPC di interfaccia.

Per consentire a un VPC di un altro di accedere Account AWS al tuo dominio

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home/.
2. Nel pannello di navigazione, scegli Domains (Domini) e apri il dominio a cui desideri fornire l'accesso.
3. Vai alla scheda Endpoint VPC, che mostra gli account e i VPC corrispondenti che hanno accesso al dominio.
4. Scegli Authorize principal (Autorizza principale).
5. Inserisci l' Account AWS ID dell'account che accederà al tuo dominio. In questa fase autorizzi l'account specificato a creare endpoint VPC sul dominio.
6. Seleziona Authorize (Autorizza).

Creazione di un endpoint VPC dell'interfaccia per un dominio VPC

È possibile creare un endpoint VPC di interfaccia per OpenSearch Service utilizzando la console di OpenSearch servizio o (). AWS Command Line Interface AWS CLI

Per creare un endpoint VPC di interfaccia per un dominio di servizio OpenSearch

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home/.
2. Nel pannello di navigazione a sinistra, scegli Endpoint VPC.
3. Seleziona Crea endpoint.
4. Seleziona se connettere un dominio nell'attuale Account AWS o in un altro Account AWS.

5. Seleziona il dominio a cui ti connetti con questo endpoint. Se il dominio è nell'attuale Account AWS, usa il menu a discesa per scegliere il dominio. Se il dominio si trova in un altro account, immetti il nome della risorsa Amazon (ARN) del dominio a cui connettersi. Per scegliere un dominio in un altro account, il proprietario deve fornirti l'accesso al dominio.
6. Per VPC, seleziona il VPC da cui accederai a Service. OpenSearch
7. Per le sottoreti, seleziona una o più sottoreti da cui accedere al servizio. OpenSearch
8. Per Security groups (Gruppi di sicurezza), seleziona i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint. Si tratta di una fase fondamentale per limitare le porte, i protocolli e le origini per il traffico in ingresso che si sta autorizzando per l'endpoint. Le regole del gruppo di sicurezza devono consentire alle risorse che utilizzeranno l'endpoint VPC di comunicare con il OpenSearch Servizio di comunicare con l'interfaccia di rete dell'endpoint.
9. Seleziona Crea endpoint. L'endpoint dovrebbe essere attivo entro 2-5 minuti.

Utilizzo degli endpoint OpenSearch VPC gestiti dal servizio utilizzando l'API di configurazione

Utilizza le seguenti operazioni API per creare e gestire endpoint OpenSearch VPC gestiti dal servizio.

- CreateVpcEndpoint
- ListVpcEndpoints
- UpdateVpcEndpoint
- DeleteVpcEndpoint

Utilizza le seguenti operazioni API per gestire l'accesso degli endpoint ai domini VPC:

- AuthorizeVpcEndpointAccess
- ListVpcEndpointAccess
- ListVpcEndpointsForDomain
- RevokeVpcEndpointAccess

Autenticazione SAML per dashboard OpenSearch

L'autenticazione SAML per OpenSearch dashboard ti consente di utilizzare il tuo provider di identità esistente per offrire Single Sign-On (SSO) per dashboard su domini Amazon OpenSearch Service

in esecuzione o Elasticsearch 6.7 o versione successiva. OpenSearch Per utilizzare l'autenticazione SAML, è necessario abilitare il controllo granulare degli accessi.

Invece di eseguire l'autenticazione tramite Amazon Cognito o il database utenti interno, l'autenticazione SAML OpenSearch per dashboard consente di utilizzare provider di identità di terze parti per accedere alle dashboard, gestire il controllo granulare degli accessi, cercare i dati e creare visualizzazioni. OpenSearch Il servizio supporta provider che utilizzano lo standard SAML 2.0, come Okta, Keycloak, Active Directory Federation Services (ADFS), Auth0 e. AWS IAM Identity Center

L'autenticazione SAML per le dashboard consente solo l'accesso alle dashboard tramite un browser Web. OpenSearch Le tue credenziali SAML non ti consentono di effettuare richieste HTTP dirette alle API o Dashboards. OpenSearch

Panoramica della configurazione SAML

Questa documentazione presuppone che si disponga di un fornitore di identità esistente e che si abbia una certa familiarità con esso. Non possiamo fornire passaggi di configurazione dettagliati per il tuo provider esatto, ma solo per il tuo dominio di servizio. OpenSearch

Il flusso di accesso a OpenSearch Dashboards può assumere una delle due forme seguenti:

- Avviato da provider di servizi (SP): si passa a Dashboards (ad esempio `https://my-domain.us-east-1.es.amazonaws.com/_dashboards`), che reindirizza alla schermata di accesso. Dopo aver effettuato l'accesso, il provider di identità reindirizza l'utente da Dashboards.
- Provider di identità (IdP) avviato: accedi al tuo provider di identità, accedi e scegli OpenSearch Dashboard da una directory di applicazioni.

OpenSearch Il servizio fornisce due URL Single Sign-On, inizializzati da SP e avviati da IdP, ma è necessario solo quello che corrisponde al flusso di accesso desiderato per Dashboards. OpenSearch

Indipendentemente dal tipo di autenticazione utilizzato, l'obiettivo è quello di accedere tramite il provider di identità e ricevere un'asserzione SAML contenente il nome utente (obbligatorio) e qualsiasi ruolo di back-end (facoltativo, ma consigliato). Queste informazioni consentono il controllo granulare degli accessi per assegnare le autorizzazioni agli utenti SAML. Nei provider di identità esterni, i ruoli back-end sono in genere denominati "ruoli" o "gruppi".

Considerazioni

Durante la configurazione dell'autenticazione SAML tieni presente quanto segue:

- A causa delle dimensioni del file di metadati IdP, per configurare l'autenticazione SAML si consiglia vivamente di utilizzare la console AWS .
- I domini supportano solo un metodo di autenticazione Dashboards alla volta. Se hai abilitato l'autenticazione Amazon Cognito per OpenSearch dashboard, devi disabilitarla prima di poter abilitare l'autenticazione SAML.
- Se utilizzi un sistema di bilanciamento del carico di rete con SAML, devi prima creare un endpoint personalizzato. Per ulteriori informazioni, consulta ???.

Autenticazione SAML per domini VPC

SAML non richiede una comunicazione diretta tra il fornitore di identità e il provider di servizi. Pertanto, anche se il tuo OpenSearch dominio è ospitato all'interno di un VPC privato, puoi comunque utilizzare SAML purché il tuo browser sia in grado di comunicare sia con il tuo OpenSearch cluster che con il tuo provider di identità. Il browser agisce essenzialmente come intermediario tra il provider di identità e il provider di servizi. Per un diagramma utile che spiega il flusso di autenticazione SAML, consulta la Documentazione Okta.

Modifica della policy di accesso al dominio

Prima di configurare l'autenticazione SAML è necessario aggiornare la policy di accesso al dominio per consentire agli utenti SAML di accedervi. Altrimenti, saranno restituiti errori di accesso negato.

Consigliamo la seguente policy di accesso al dominio, che fornisce l'accesso completo alle risorse secondarie (`/*`) del dominio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

Per rendere la politica più restrittiva, puoi aggiungere una condizione relativa all'indirizzo IP alla politica. Questa condizione limita l'accesso solo all'intervallo di indirizzi IP o alla sottorete specificati. Ad esempio, la seguente politica consente l'accesso solo dalla sottorete 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 politica di accesso al dominio aperta richiede l'attivazione di un controllo granulare degli accessi sul dominio, altrimenti viene visualizzato il seguente errore:
> `To protect domains with public access, a restrictive policy or fine-grained access control is required.`
> Se hai un utente principale o un utente interno configurato con una password robusta, mantenere aperta la policy utilizzando un controllo granulare degli accessi potrebbe essere accettabile dal punto di vista della sicurezza. Per ulteriori informazioni, consulta ???.

Configurazione dell'autenticazione avviata da SP o da IdP

Questi passaggi spiegano come abilitare l'autenticazione SAML con l'autenticazione avviata da SP o IdP per i dashboard. OpenSearch Per il passaggio aggiuntivo richiesto per abilitare entrambi, consulta Configurazione dell'autenticazione avviata da SP e avviata da IdP.

Fase 1: Abilitazione dell'autenticazione SAML

Puoi abilitare l'autenticazione SAML durante la creazione del dominio o scegliendo Actions (Operazioni), Edit security configuration (Modifica configurazione di sicurezza) su un dominio esistente. I seguenti passaggi variano leggermente a seconda della scelta effettuata.

All'interno della configurazione del dominio, in Autenticazione SAML per Dashboards/Kibana, seleziona Abilita l'autenticazione SAML. OpenSearch

Fase 2: Configurazione del fornitore di identità

Esegui i seguenti passaggi a seconda di quando viene configurata l'autenticazione SAML.

Se stai creando un nuovo dominio

Se stai creando un nuovo dominio, Service non è ancora in grado di generare un ID di entità del OpenSearch fornitore di servizi o un URL SSO. Il tuo fornitore di identità richiede questi valori per abilitare correttamente l'autenticazione SAML, ma possono essere generati solo dopo la creazione del dominio. Per ovviare a questa interdipendenza durante la creazione del dominio, puoi fornire valori temporanei nella configurazione dell'IdP per generare i metadati richiesti e quindi aggiornarli una volta che il dominio è attivo.

Se utilizzi un endpoint personalizzato, puoi dedurre quali saranno gli URL. Ad esempio, se l'endpoint personalizzato è `www.custom-endpoint.com`, l'ID dell'entità del fornitore di servizi sarà `www.custom-endpoint.com`, l'URL SSO avviato dall'IDP sarà `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs/idpinitiated` e l'URL SSO avviato da SP sarà `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs`. Puoi utilizzare i valori per configurare il tuo fornitore di identità prima della creazione del dominio. Per gli esempi consultare la prossima sezione.

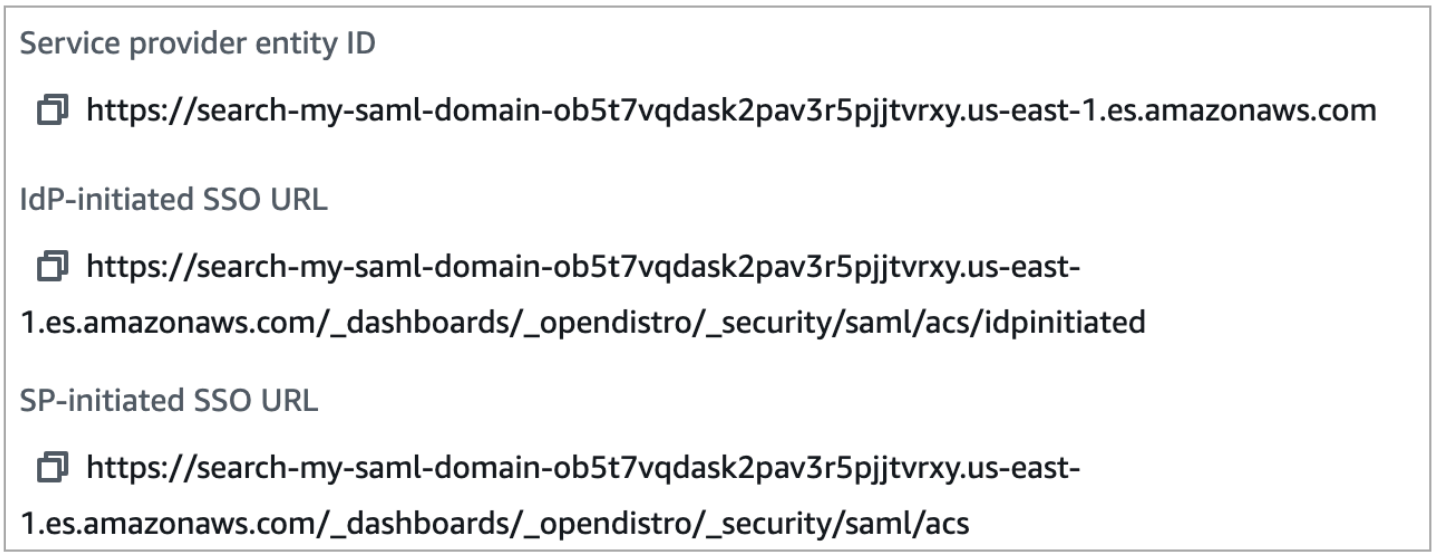
Se non utilizzi un endpoint personalizzato, puoi inserire valori temporanei nel tuo IdP per generare i metadati richiesti e quindi aggiornarli in un secondo momento dopo l'attivazione del dominio.

Ad esempio, all'interno di Okta, puoi inserire `https://temp-endpoint.amazonaws.com` nei campi Single sign on URL (URL Single Sign On) e Audience URI (SP Entity ID) (URI del pubblico

[ID entità SP]), che consentono di generare i metadati. Quindi, dopo che il dominio è attivo, puoi recuperare i valori corretti da OpenSearch Service e aggiornarli in Okta. Per istruzioni, consulta the section called “Fase 6: Aggiornamento degli URL dell'IdP”.

Se stai modificando un dominio esistente

Se stai abilitando l'autenticazione SAML su un dominio esistente, copia l'ID dell'entità del fornitore di servizi e uno degli URL SSO. Per indicazioni sull'URL da utilizzare, consulta the section called “Panoramica della configurazione SAML”.



Utilizzare questi valori per configurare il fornitore di identità. Questa è la parte più complessa del processo e, sfortunatamente, la terminologia e i passaggi variano notevolmente a seconda del provider. Consultare la documentazione del provider.

In Okta, ad esempio, crei un'applicazione web SAML 2.0. Per Single sign on URL (URL Single Sign-On), specifica l'URL SSO. Per URI di destinazione (ID entità SP), specificare l'ID entità SP.

Piuttosto che utenti e ruoli di back-end, Okta utilizza utenti e gruppi. Per Group Attribute Statements (Istruzioni degli attributi di gruppo), consigliamo di aggiungere `role` al campo Name (Nome) e l'espressione regolare `.+` al campo Filter (Filtro). Questa istruzione indica al provider di identità Okta di includere tutti i gruppi di utenti sotto il campo `role` dell'asserzione SAML dopo l'autenticazione di un utente.

In IAM Identity Center, si specifica l'ID dell'entità SP come audience SAML dell'applicazione. È inoltre necessario specificare le seguenti mappature degli attributi: e. `Subject=${user:subject}:format=unspecified` `Role=${user:groups}:format=uri`

In Auth0, crei una normale applicazione web e abiliti il componente aggiuntivo SAML 2.0. In Keycloak, crei un client.

Fase 3: Importazione dei metadati dell'IdP

Dopo aver configurato il provider di identità, viene generato un file di metadati IdP. Questo file XML contiene informazioni sul provider, ad esempio un certificato TLS, endpoint Single Sign-On e l'ID entità del provider di identità.

Copia il contenuto del file di metadati IdP e incollalo nel campo Metadati da IdP della console di servizio. OpenSearch In alternativa, scegliere Importa da file XML e caricare il file. Il file dei metadati dovrebbe avere un aspetto simile al seguente:

```
<?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>
```

Fase 4: Configurazione dei campi SAML

Dopo aver inserito i metadati IdP, configura i seguenti campi aggiuntivi nella OpenSearch console di servizio:

- IdP entity ID (ID entità IdP): copiare il valore della proprietà `entityID` dal file di metadati e incollarlo in questo campo. Molti provider di identità visualizzano questo valore anche come parte di un riepilogo successivo alla configurazione. Alcuni fornitori lo chiamano "emittente".
- Nome utente principale SAML e ruolo di backend principale SAML: l'utente e/o il ruolo di backend specificato riceve le autorizzazioni complete per il cluster, equivalenti a quelle di un nuovo utente master, ma può utilizzare tali autorizzazioni solo all'interno delle dashboard. OpenSearch

  Ad esempio, in Okta è possibile avere un utente `jdoe` che appartiene al gruppo `admins`. Se si aggiunge `jdoe` al campo Nome utente master SAML, solo quell'utente riceverà le autorizzazioni complete. Se si aggiunge `admins` al campo SAML master backend role (Ruolo back-end master SAML), qualsiasi utente che appartiene al gruppo `admins` riceverà le autorizzazioni complete.

> **Note**
>
> Il contenuto dell'asserzione SAML deve corrispondere esattamente alle stringhe utilizzate per il nome utente master SAML e/o il ruolo di master SAML. Alcuni provider di identità aggiungono un prefisso prima dei nomi utente, il che può causare una mancata corrispondenza. hard-to-diagnose Nell'interfaccia utente del provider di identità, è possibile che venga visualizzato `jdoe`, ma l'asserzione SAML potrebbe contenere `auth0|jdoe`. Utilizzare sempre la stringa dall'asserzione SAML.

Molti provider di identità consentono di visualizzare un'asserzione di esempio durante il processo di configurazione e strumenti come Tracer SAML possono aiutare a esaminare e risolvere i problemi del contenuto di asserzioni reali. Le asserzioni hanno il seguente aspetto:

```
<?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>
```

Fase 5: (facoltativo) configurazione delle impostazioni aggiuntive

In Additional settings (Impostazioni aggiuntive), configura i seguenti campi facoltativi:

- Subject key (Chiave oggetto): è possibile lasciare questo campo vuoto in modo da utilizzare l'elemento `NameID` dell'asserzione SAML per il nome utente. Se l'asserzione non utilizza questo elemento standard e include invece il nome utente come attributo personalizzato, specificare tale attributo qui.
- Roles key)Chiave ruoli): Se si desidera utilizzare i ruoli back-end (scelta consigliata), specificare un attributo dall'asserzione in questo campo, ad esempio `role` o `group`. Questa è un'altra situazione in cui strumenti come i tracer SAML possono aiutare.
- Durata della sessione: per impostazione predefinita, OpenSearch Dashboards disconnette gli utenti dopo 24 ore. È possibile configurare questo valore su qualsiasi numero compreso tra 60 e 1.440 (24 ore) specificando un nuovo valore.

Se la configurazione ti soddisfa, salva il dominio.

Fase 6: Aggiornamento degli URL dell'IdP

Se hai abilitato l'autenticazione SAML durante la creazione di un dominio, hai specificato URL temporanei all'interno dell'IdP per generare il file di metadati XML. Dopo il passaggio del dominio allo stato `Active`, potrai ottenere gli URL corretti e modificare l'IdP.

Per richiamare gli URL, seleziona il dominio e scegli Actions (Operazioni) quindi Edit security configuration (Modifica configurazione di sicurezza). In Autenticazione SAML per OpenSearch Dashboards/Kibana, puoi trovare l'ID dell'entità del fornitore di servizi e gli URL SSO corretti. Copia i valori e usali per configurare il tuo fornitore di identità, sostituendo gli URL temporanei che hai fornito nella fase 2.

Fase 7: Associazione degli utenti SAML ai ruoli

Una volta che lo stato del dominio è Attivo e il tuo IdP è configurato correttamente, accedi a OpenSearch Dashboards.

- Se è stato scelto l'URL avviato da SP, passare a *`domain-endpoint`*`/_dashboards`. Per accedere direttamente a un tenant specifico, aggiungere `?security_tenant=`*`tenant-name`* all'URL.
- Se è stato scelto l'URL avviato dall'IdP, passare alla directory dell'applicazione del provider di identità.

In entrambi i casi, accedere come utente principale SAML o come utente appartenente al ruolo back-end principale SAML. Per continuare l'esempio dalla fase 7, accedere come `jdoe` o come membro del gruppo `admins`.

Dopo il caricamento di OpenSearch Dashboards, scegli Sicurezza, Ruoli. Quindi, mappa i ruoli per consentire ad altri utenti di accedere alle OpenSearch dashboard.

Ad esempio, è possibile mappare il collega fidato `jroe` ai ruoli `all_access` e `security_manager`. È inoltre possibile mappare il ruolo back-end `analysts` ai ruoli `readall` e `opensearch_dashboards_user`.

Se preferisci utilizzare l'API anziché le OpenSearch dashboard, consulta la seguente richiesta di esempio:

```
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"] }
  }
]
```

Configurazione dell'autenticazione avviata da SP e avviata da IdP

Se si desidera configurare sia l'autenticazione avviata da SP che quella avviata da IdP, è necessario farlo tramite il provider di identità. Ad esempio, in Okta, puoi eseguire le operazioni seguenti:

1. All'interno dell'applicazione SAML, vai su General (Generale), SAML settings (Impostazioni SAML).
2. Per Single sign on URL (URL Single Sign On), fornisci l'URL SSO avviato da IdP. Ad esempio, `https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs/idpinitiated`.
3. Abilita Allow this app to request other SSO URLs (Consenti a questa app di richiedere altri URL SSO).
4. In Requestable SSO URLs (URL SSO richiedibili), aggiungi uno o più URL SSO avviati da SP. Ad esempio, `https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs`.

Configurazione dell'autenticazione SAML (AWS CLI)

Il AWS CLI comando seguente abilita l'autenticazione SAML per le OpenSearch dashboard su un dominio esistente:

```
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"}}'
```

È necessario eseguire l'escape di tutte le virgolette e i caratteri newline nel file XML dei metadati. Ad esempio, utilizzare `<KeyDescriptor use=\"signing\">\n` invece di `<KeyDescriptor use="signing">` e un'interruzione di riga. Per informazioni dettagliate sull'utilizzo di AWS CLI, consulta il AWS CLI Command Reference.

Configurazione dell'autenticazione SAML (API di configurazione)

La seguente richiesta all'API di configurazione abilita l'autenticazione SAML per le OpenSearch dashboard su un dominio esistente:

```
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"
    }
  }
}
```

È necessario eseguire l'escape di tutte le virgolette e i caratteri newline nel file XML dei metadati. Ad esempio, utilizzare `<KeyDescriptor use=\"signing\">\n` invece di `<KeyDescriptor use="signing">` e un'interruzione di riga. Per informazioni dettagliate sull'utilizzo dell'API di configurazione, consulta il riferimento all'API OpenSearch di servizio.

Risoluzione dei problemi SAML

Errore	Informazioni
La richiesta: '*/some/path* ' non è consentita.	Verificare di aver fornito al provider di identità l'URL SSO corretto (fase 3).
Fornisci un documento valido per i metadati del provider di identità per abilitare SAML.	Il file di metadati IdP non è conforme allo standard SAML 2.0. Verificare la presenza di errori utilizzando uno strumento di convalida.
Le opzioni di configurazione SAML non sono visibili nella console.	Effettuare l'aggiornamento alla versione più recente del software di assistenza.
Errore di configurazione SAML: si è verificato un errore durante il recupero della configurazione SAML, controlla le impostazioni.	Questo errore generico può verificarsi per molti motivi. • Verificare di aver fornito al provider di identità l'ID entità SP e l'URL SSO corretti. • Rigenerare il file di metadati IdP e verificare l'ID entità IdP. Aggiungere tutti i metadati aggiornati nella console AWS . • Verifica che la politica di accesso al dominio consenta l'accesso a OpenSearch dashboard `e_plugins/_security/*` . In generale, per domini che utilizzano un controllo granulare degli accessi è preferibile utilizzare una policy di accesso aperta. • Consultare la documentazione del provider di identità per le istruzioni sulla configurazione di SAML.
Ruolo mancante: nessun ruolo disponibi le per questo utente, contatta l'amminis tratore di sistema.	L'autenticazione è stata eseguita correttamente, ma il nome utente e gli eventuali ruoli back-end dell'asse rzione SAML non sono mappati ad alcun ruolo e quindi non dispongono di autorizzazioni. Queste mappature distinguono tra maiuscole e minuscole.

Errore	Informazioni
	L'amministratore di sistema può verificare il contenuto dell'asserzione SAML utilizzando uno strumento come SAML-Tracer, quindi verificare la mappatura dei ruoli utilizzando la seguente richiesta: `GET _plugins/_security/api/rolesmapping`
Il browser reindirizza o riceve continuamente errori HTTP 500 quando tenta di accedere alle dashboard. OpenSearch	Questi errori possono verificarsi se l'asserzione SAML contiene un numero elevato di ruoli per un totale di circa 1.500 caratteri. Ad esempio, se si superano 80 ruoli, la cui lunghezza media è di 20 caratteri, è possibile che il limite di dimensione per i cookie nel browser Web venga superato. A partire dalla OpenSearch versione 2.7, l'asserzione SAML supporta ruoli fino a 5000 caratteri.
Non è possibile disconnettersi da ADFS.	ADFS richiede che tutte le richieste di disconnessione siano firmate, cosa che OpenSearch Service non supporta. Rimuovi `<SingleLogoutService />` dal file di metadati IdP per forzare il OpenSearch servizio a utilizzare il proprio meccanismo di disconnessione interno.
`Could not find entity descriptor for __PATH__.`	L'ID dell'entità dell'IdP fornito nei metadati XML to OpenSearch Service è diverso da quello nella risposta SAML. Per risolvere questo problema, assicurati che corrispondano. Abilita i log degli errori dell'applicazione CW sul tuo dominio per trovare il messaggio di errore per il debug del problema di integrazione SAML.

Errore	Informazioni
`Signature validation failed. SAML response rejected.`	OpenSearch Il servizio non è in grado di verificare la firma nella risposta SAML utilizzando il certificato dell'IdP fornito nei metadati XML. Potrebbe trattarsi di un errore manuale o il certificato del tuo IdP potrebbe aver modificato il certificato. Aggiorna il certificato più recente del tuo IdP nei metadati XML forniti al OpenSearch Servizio tramite. AWS Management Console
`__PATH__ is not a valid audience for this response.`	Il campo audience nella risposta SAML non corrispon de all'endpoint del dominio. Per correggere questo errore, aggiorna il campo SP audience in modo che corrisponda all'endpoint del tuo dominio. Se hai abilitato gli endpoint personalizzati, il campo audience deve corrispondere al tuo endpoint personalizzato. Abilita i registri degli errori dell'applicazione CW sul tuo dominio per trovare il messaggio di errore per eseguire il debug del problema di integrazione SAML.
Il tuo browser riceve un errore HTTP 400 nella risposta. `Invalid Request Id`	Questo errore si verifica in genere se hai configura to l'URL avviato dall'IdP con il formato. *<DashboardsURL>* `/_opendistro/_security/saml/acs` Configura invece l'URL con il formato. *<DashboardsURL>* `/_opendistro/_security/saml/acs/idpinitiated`

Errore	Informazioni
La risposta è stata ricevuta al `__PATH__` posto di`__PATH__`.	Il campo di destinazione nella risposta SAML non corrisponde a uno dei seguenti formati URL: • *<DashboardsURL>* `/_opendistro/_security/saml/acs` • *<DashboardsURL>* `/_opendistro/_security/saml/acs/idpinitiated` . A seconda del flusso di accesso utilizzato (avviato da SP o avviato da IDP), inserisci un campo di destinazione che corrisponda a uno degli URL. OpenSearch
La risposta ha un `InResponseTo` attributo, mentre non era previsto. `InResponseTo`	Stai utilizzando l'URL avviato dall'IdP per un flusso di accesso avviato da SP. Utilizza invece l'URL avviato da SP.

Disabilitazione dell'autenticazione SAML

Per disabilitare l'autenticazione SAML per OpenSearch Dashboards (console)

1. Scegli il dominio, Operazioni quindi Modifica configurazione di sicurezza.
2. Deselezionare Abilita autenticazione SAML.
3. Seleziona Salvataggio delle modifiche.
4. Al termine dell'elaborazione del dominio, verificare la mappatura dei ruoli del controllo granulare degli accessi con la seguente richiesta:

   ```
   GET _plugins/_security/api/rolesmapping
   ```

   La disabilitazione dell'autenticazione SAML per Dashboards non rimuove le mappature per il nome utente principale SAML e/o il ruolo backend principale SAML. Se si desidera rimuovere queste mappature, accedere a Dashboards utilizzando il database utente interno (se abilitato) oppure l'API:

   ```
   PUT _plugins/_security/api/rolesmapping/all_access
   ```

```
{
  "users": [
    "master-user"
  ]
}
```

Configurazione dell'autenticazione Amazon Cognito per dashboard OpenSearch

Puoi autenticare e proteggere l'installazione predefinita di OpenSearch dashboard di Amazon OpenSearch Service utilizzando Amazon Cognito. L'autenticazione Amazon Cognito è facoltativa e disponibile solo per i domini che utilizzano Elasticsearch 5.1 OpenSearch o versione successiva. Se non si configura l'autenticazione Amazon Cognito, è comunque possibile proteggere Dashboards usando una policy di accesso basata su IP e un server proxy, autenticazione di base HTTP o SAML.

Gran parte del processo di autenticazione avviene in Amazon Cognito, ma questa sezione offre linee guida e requisiti per configurare le risorse di Amazon Cognito in modo che funzionino con i domini di servizio. OpenSearch A tutte le risorse Amazon Cognito si applicano i prezzi standard.

> **Tip**
>
> La prima volta che configuri un dominio per utilizzare l'autenticazione Amazon Cognito per le OpenSearch dashboard, ti consigliamo di utilizzare la console. Le risorse Amazon Cognito sono estremamente personalizzabili e la console può aiutare a identificare e comprendere le funzionalità importanti più adatte al proprio caso specifico.

Argomenti

- Test
- Quote
- Problemi di configurazione comuni
- Disattivazione dell'autenticazione Amazon Cognito per dashboard OpenSearch
- Eliminazione di domini che utilizzano l'autenticazione Amazon Cognito per dashboard OpenSearch

Prerequisiti

Prima di poter configurare l'autenticazione Amazon Cognito per le OpenSearch dashboard, devi soddisfare diversi prerequisiti. La console OpenSearch di servizio aiuta a semplificare la creazione di queste risorse, ma la comprensione dello scopo di ciascuna risorsa aiuta nella configurazione e nella risoluzione dei problemi. L'autenticazione Amazon Cognito per Dashboards richiede le risorse seguenti:

- Bacino d'utenza di Amazon Cognito
- Pool di identità di Amazon Cognito
- Ruolo IAM a cui è collegata la policy `AmazonOpenSearchServiceCognitoAccess` (`CognitoAccessForAmazonOpenSearch`)

> **Note**
>
> Il bacino d'utenza e il pool di identità devono trovarsi nella stessa Regione AWS. Puoi utilizzare lo stesso pool di utenti, pool di identità e ruolo IAM per aggiungere l'autenticazione Amazon Cognito per dashboard a più OpenSearch domini di servizio. Per ulteriori informazioni, consulta the section called “Quote”.

Informazioni sul bacino d'utenza

I pool di utenti hanno due caratteristiche principali: creano e gestiscono una directory di utenti e permettono agli utenti di registrarsi e accedere. Per istruzioni su come creare un bacino d'utenza, consulta Creazione di un bacino d'utenza nella Guida per gli sviluppatori di Amazon Cognito.

Quando crei un pool di utenti da utilizzare con OpenSearch Service, considera quanto segue:

- Il bacino d'utenza di Amazon Cognito deve avere un nome di dominio. OpenSearch Il servizio utilizza questo nome di dominio per reindirizzare gli utenti a una pagina di accesso per accedere alle dashboard. Oltre a un nome di dominio, il pool di utenti non richiede altre configurazioni non predefinite.
- È necessario specificare gli attributi standard obbligatori del pool, ovvero attributi come nome, data di nascita, indirizzo e-mail e numero di telefono. Poiché non puoi modificare questi attributi dopo che crei il pool di utenti, scegli quelli più importanti a questo punto.
- Durante la creazione del pool di utenti, scegli se gli utenti possono creare i propri account, la complessità minima delle password per gli account e se abilitare l'autenticazione a più fattori. Se prevedi di usare un provider di identità esterno, queste impostazioni non si escludono a vicenda. Tecnicamente, puoi abilitare il pool di utenti come provider di identità e abilitare un provider di identità esterno, ma la maggior parte degli utenti preferisce scegliere solo uno dei due approcci.

Gli ID pool di utenti hanno il formato *region*`_`*ID*. Se prevedi di utilizzare la AWS CLI o un AWS SDK per configurare il OpenSearch servizio, prendi nota dell'ID.

Informazioni sul pool di identità

I pool di identità permettono di assegnare ruoli temporanei con privilegi limitati agli utenti dopo che questi accedono. Per istruzioni su come creare un pool di identità, consultare Pool di identità nella Guida per gli sviluppatori di Amazon Cognito. Quando crei un pool di identità da utilizzare con OpenSearch Service, considera quanto segue:

- Se si utilizza la console Amazon Cognito, è necessario selezionare la casella di controllo Consenti l'accesso a identità non autenticate per creare il pool di identità. Dopo aver creato il pool di identità e configurato il dominio del OpenSearch servizio, Amazon Cognito disabilita questa impostazione.
- Non devi aggiungere provider di identità esterni al pool di identità. Quando configuri OpenSearch Service per utilizzare l'autenticazione Amazon Cognito, configura il pool di identità per utilizzare il pool di utenti che hai appena creato.
- Dopo aver creato il pool di identità, devi scegliere i ruoli IAM non autenticati e autenticati. Questi ruoli specificano le policy d'accesso associate agli utenti prima e dopo l'accesso. Se si utilizza la console Amazon Cognito, questa può creare i ruoli per conto dell'utente. Dopo aver creato il ruolo autenticato, annota l'ARN, che usa il formato `arn:aws:iam::`*123456789012*`:role/Cognito_`*identitypoolname*`Auth_Role`.

Gli ID pool di identità hanno il formato *region*:*ID*-*ID*-*ID*-*ID*-*ID*. Se prevedi di utilizzare la AWS CLI o un AWS SDK per configurare il OpenSearch servizio, prendi nota dell'ID.

Informazioni sul ruolo CognitoAccessForAmazonOpenSearch

OpenSearch Il servizio richiede le autorizzazioni per configurare i pool di utenti e identità di Amazon Cognito e utilizzarli per l'autenticazione. È possibile utilizzare`AmazonOpenSearchServiceCognitoAccess`, che è una politica AWS gestita, per questo scopo. `AmazonESCognitoAccess`è una politica precedente che è stata sostituita da `AmazonOpenSearchServiceCognitoAccess` quando il servizio è stato rinominato Amazon OpenSearch Service. Entrambe le policy forniscono le autorizzazioni minime di Amazon Cognito necessarie per abilitare l'autenticazione Cognito. Per la policy JSON, consultare Console IAM.

Se utilizzi la console per creare o configurare il tuo dominio di OpenSearch servizio, questa crea per te un ruolo IAM e allega la `AmazonOpenSearchServiceCognitoAccess` policy (o la `AmazonESCognitoAccess` policy se si tratta di un dominio Elasticsearch) al ruolo. Il nome predefinito per questo ruolo è `CognitoAccessForAmazonOpenSearch`.

`AmazonESCognitoAccess`Entrambe le politiche `AmazonOpenSearchServiceCognitoAccess` relative alle autorizzazioni dei ruoli consentono a OpenSearch Service di completare le seguenti azioni su tutti i pool di identità e utenti:

- Operazione: `cognito-idp:DescribeUserPool`
- Operazione: `cognito-idp:CreateUserPoolClient`
- Operazione: `cognito-idp:DeleteUserPoolClient`
- Operazione: `cognito-idp:UpdateUserPoolClient`
- Operazione: `cognito-idp:DescribeUserPoolClient`
- Operazione: `cognito-idp:AdminInitiateAuth`
- Operazione: `cognito-idp:AdminUserGlobalSignOut`
- Operazione: `cognito-idp:ListUserPoolClients`
- Operazione: `cognito-identity:DescribeIdentityPool`
- Operazione: `cognito-identity:SetIdentityPoolRoles`
- Operazione: `cognito-identity:GetIdentityPoolRoles`

Se utilizzi lo AWS CLI o uno degli AWS SDK, devi creare il tuo ruolo, allegare la policy e specificare l'ARN per questo ruolo quando configuri il OpenSearch tuo dominio di servizio. Il ruolo deve avere la relazione di trust seguente:

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

Per le istruzioni, consultare Creazione di un ruolo per delegare autorizzazioni a un servizio AWS e Collegamento e scollegamento di policy IAM nella Guida per l'utente di IAM.

Configurazione di un dominio per l'uso dell'autenticazione Amazon Cognito

Dopo aver completato i prerequisiti, puoi configurare un dominio di OpenSearch servizio per utilizzare Amazon Cognito for Dashboards.

> **Note**
>
> Amazon Cognito non è disponibile in tutte le Regioni AWS. Per un elenco delle regioni e degli endpoint supportati, consultare Regioni AWS ed endpoint. Non è necessario utilizzare la stessa regione per Amazon Cognito utilizzata per OpenSearch Service.

Configurazione dell'autenticazione Amazon Cognito (console)

Poiché crea il CognitoAccessForAmazonOpenSearchruolo per te, la console offre l'esperienza di configurazione più semplice. Oltre alle autorizzazioni standard del OpenSearch Servizio, è necessario il seguente set di autorizzazioni per utilizzare la console per creare un dominio che utilizza l'autenticazione Amazon Cognito per le dashboard. OpenSearch

```
{
  "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"
    }
  ]
}
```

Per istruzioni per aggiungere autorizzazioni per un'identità (utente, gruppo di utenti o ruolo), consulta Aggiunta di autorizzazioni per identità IAM (console).

Se `CognitoAccessForAmazonOpenSearch` esiste già, è necessario un numero minore di autorizzazioni:

```
{
  "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"
    }
  ]
}
```

Come configurare l'autenticazione Amazon Cognito per Dashboards (console)

1. Apri la console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home/.
2. In Domini, seleziona il dominio che desideri configurare.
3. Scegli Operazioni, quindi Modifica configurazione di sicurezza.
4. SelezionaAbilitare l'autenticazione Amazon Cognito.
5. Per Regione selezionare la Regione AWS che contiene il pool di utenti e il pool di identità di Amazon Cognito.
6. Per Bacino d'utenza Cognito, seleziona un pool di utenti o creane uno. Per le linee guida, consulta the section called “Informazioni sul bacino d'utenza”.
7. Per Pool di identità Cognito, seleziona un pool di identità o creane uno. Per le linee guida, consulta the section called “Informazioni sul pool di identità”.

   > **Note**
   >
   > I link Crea bacino d'utenza e Crea pool di identità reindirizzano alla console Amazon Cognito e richiedono la creazione manuale di queste risorse. Il processo non è automatico. Per ulteriori informazioni, consulta the section called “Prerequisiti”.

8. Per Nome ruolo IAM, utilizza il valore di default `CognitoAccessForAmazonOpenSearch` (consigliato) o specifica un nuovo nome. Per ulteriori informazioni sullo scopo di questo ruolo, consultare the section called “Informazioni sul ruolo CognitoAccessForAmazonOpenSearch”.
9. Sceglie Save changes (Salva modifiche).

Al termine dell'elaborazione del dominio, consulta the section called “Concessione del ruolo autenticato” e the section called “Configurazione dei provider di identità” per informazioni sulle altre fasi di configurazione.

Configurazione dell'autenticazione Amazon Cognito (AWS CLI)

Usa il `--cognito-options` parametro per configurare il tuo dominio OpenSearch di servizio. La sintassi seguente viene usata dai comandi `create-domain` e `update-domain-config`:

```
--cognito-options Enabled=true,UserPoolId="user-pool-id",IdentityPoolId="identity-pool-id",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

Esempio

Nell'esempio seguente viene creato un dominio nella regione `us-east-1` che abilita l'autenticazione Amazon Cognito per Dashboards tramite il ruolo `CognitoAccessForAmazonOpenSearch` e fornisce a `Cognito_Auth_Role` l'accesso al dominio:

```
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"
```

Al termine dell'elaborazione del dominio, consulta the section called “Concessione del ruolo autenticato” e the section called “Configurazione dei provider di identità” per informazioni sulle altre fasi di configurazione.

Configurazione dell'autenticazione Amazon Cognito (SDK AWS)

Gli AWS SDK (eccetto gli SDK per Android e iOS) supportano tutte le operazioni definite nell'Amazon OpenSearch Service API Reference, incluso il `CognitoOptions` parametro per le operazioni `CreateDomain` and`UpdateDomainConfig`. Per ulteriori informazioni sull'installazione e sull'uso degli SDK AWS, consultare Software Development Kit AWS.

Al termine dell'elaborazione del dominio, consulta the section called “Concessione del ruolo autenticato” e the section called “Configurazione dei provider di identità” per informazioni sulle altre fasi di configurazione.

Concessione del ruolo autenticato

Per impostazione predefinita, il ruolo IAM autenticato che hai configurato seguendo le linee guida contenute the section called “Informazioni sul pool di identità” non dispone dei privilegi necessari per accedere alle dashboard. OpenSearch Devi fornire al ruolo autorizzazioni aggiuntive.

> **Note**
>
> Se hai configurato un controllo granulare degli accessi e utilizzi una policy di accesso aperta o basata su IP, puoi saltare questo passaggio.

È possibile includere queste autorizzazioni in una policy basata sull'identità, ma a meno che non si desideri che gli utenti autenticati abbiano accesso a tutti i domini di OpenSearch servizio, una policy basata sulle risorse collegata a un singolo dominio è l'approccio migliore.

Per `Principal`, specifica l'ARN del ruolo autenticato di Cognito che hai configurato con le linee guida in the section called “Informazioni sul pool di identità”.

```
{
   "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/*"
      }
   ]
}
```

Per istruzioni sull'aggiunta di una politica basata sulle risorse a un dominio di servizio, consulta. OpenSearch the section called “Configurazione delle policy di accesso”

Configurazione dei provider di identità

Quando configuri un dominio per utilizzare l'autenticazione Amazon Cognito per dashboard, OpenSearch Service aggiunge un client di app al pool di utenti e aggiunge il pool di utenti al pool di identità come provider di autenticazione.

> **Warning**
>
> Non rinominare o eliminare il client app.

A seconda di come hai configurato il pool di utenti, potresti dover creare gli account utente manualmente oppure gli utenti potrebbero essere in grado di creare i propri account. Se queste impostazioni sono accettabili, non devi eseguire altre operazioni. Molte persone, tuttavia, preferiscono usare provider di identità esterni.

Per abilitare un provider di identità SAML 2.0, devi fornire un documento di metadati SAML. Per abilitare provider di identità social come Login with Amazon, Facebook e Google, devi ottenere un ID app e un segreto dell'app da questi provider. Puoi abilitare qualsiasi combinazione di provider di identità.

Il metodo più semplice per configurare il bacino d'utenza è usare la console Amazon Cognito. Per istruzioni, consultare Utilizzo della federazione da un bacino d'utenza e Specifica delle impostazioni del provider di identità per l'app del bacino d'utenza nella Guida per gli sviluppatori di Amazon Cognito.

(Facoltativo) Configurazione dell'accesso granulare

Le impostazioni di default del pool di identità assegnano a ogni utente che accede lo stesso ruolo IAM (`Cognito_identitypoolAuth_Role`) e questo significa che ogni utente può accedere alle stesse risorse AWS. Se, ad esempio, si desidera utilizzare il controllo granulare degli accessi con Amazon Cognito, ad esempio se si desidera che gli analisti dell'organizzazione abbiano accesso in sola lettura a diversi indici, ma gli sviluppatori abbiano accesso in scrittura a tutti gli indici, sono disponibili due opzioni:

- Puoi creare gruppi di utenti e configurare il provider di identità in modo da scegliere il ruolo IAM in base al token di autenticazione dell'utente (consigliato).
- Puoi configurare il provider di identità in modo da scegliere il ruolo IAM in base a uno o più ruoli.

Per una procedura dettagliata che include il controllo granulare degli accessi, consultare the section called “Tutorial: controllo granulare degli accessi con autenticazione Cognito”.

> **Important**
>
> Proprio come il ruolo di default, Amazon Cognito deve far parte della relazione di trust di ogni ruolo aggiuntivo. Per maggiori dettagli, consultare Creazione dei ruoli per la mappatura dei ruoli nella Guida per gli sviluppatori di Amazon Cognito.

Gruppi di utenti e token

Quando crei un gruppo di utenti, devi scegliere un ruolo IAM per i membri del gruppo. Per informazioni su come creare i gruppi, consultare Gruppi di utenti nella Guida per gli sviluppatori di Amazon Cognito.

Dopo aver creato uno o più gruppi di utenti, puoi configurare il provider di autenticazione in modo da assegnare agli utenti i ruoli dei rispettivi gruppi anziché il ruolo predefinito del pool di identità. Selezionare Scegli ruolo da token, quindi selezionare Usa ruolo autenticato predefinito o DENY per specificare il modo in cui il pool di identità gestisce gli utenti che non fanno parte di un gruppo.

Regolamento

Le regole sono essenzialmente una serie di istruzioni `if` che Amazon Cognito valuta in sequenza. Ad esempio, se l'indirizzo e-mail di un utente contiene `@corporate`, Amazon Cognito assegna all'utente il ruolo `Role_A`. Se l'indirizzo e-mail di un utente contiene `@subsidiary`, assegna all'utente il ruolo `Role_B`. In caso contrario, assegna all'utente il ruolo autenticato predefinito.

Per ulteriori informazioni, consultare Utilizzo della mappatura basata su regole per assegnare ruoli agli utenti nella Guida per gli sviluppatori di Amazon Cognito.

(Facoltativo) Personalizzazione della pagina di accesso

Puoi utilizzare la console Amazon Cognito per caricare un logo personalizzato e apportare modifiche CSS alla pagina di accesso. Per istruzioni e un elenco completo delle proprietà CSS, consultare Configurazione delle impostazioni di personalizzazione dell'interfaccia utente dell'app per il bacino d'utenza nella Guida per gli sviluppatori di Amazon Cognito.

(Facoltativo) Configurazione della sicurezza avanzata

I bacini d'utenza di Amazon Cognito supportano funzionalità di sicurezza avanzate quali l'autenticazione a più fattori, la verifica di credenziali compromesse e l'autenticazione adattiva. Per ulteriori informazioni, consultare Gestione della sicurezza nella Guida per gli sviluppatori di Amazon Cognito.

Test

Quando la configurazione sembra soddisfacente, verificare che l'esperienza utente soddisfi le aspettative.

Per accedere alle dashboard OpenSearch

1. Passare `https://`*`opensearch-domain`*`/_dashboards` in un Web browser. Per accedere direttamente a un tenant specifico, aggiungere `?security_tenant=`*`tenant-name`* all'URL.
2. Accedere usando le credenziali preferite.
3. Dopo il caricamento di OpenSearch Dashboards, configura almeno un modello di indice. Dashboards usa questi modelli per identificare gli indici da analizzare. Immettere `*`, scegliere Next step (Fase successiva) e quindi Create index pattern (Crea modello di indice).
4. Per cercare o esplorare i dati, scegliere Discover (Individua).

Se qualsiasi fase di questo processo non riesce, consulta the section called “Problemi di configurazione comuni” per informazioni sulla risoluzione dei problemi.

Quote

Amazon Cognito applica limiti flessibili a molte delle risorse. Se desideri abilitare l'autenticazione delle dashboard per un gran numero di domini di OpenSearch servizio, consulta Quotas in Amazon Cognito e richiedi l'aumento dei limiti, se necessario.

Ogni dominio OpenSearch di servizio aggiunge un client di app al pool di utenti, che aggiunge un provider di autenticazione al pool di identità. Se OpenSearch abiliti l'autenticazione Dashboards per più di 10 domini, potresti incontrare il limite del «numero massimo di provider del pool di utenti di Amazon Cognito per pool di identità». Se superi un limite, tutti i domini di OpenSearch servizio che tenti di configurare per utilizzare l'autenticazione Amazon Cognito per dashboard possono rimanere bloccati in uno stato di configurazione di Elaborazione.

Problemi di configurazione comuni

La tabella seguente elenca i problemi di configurazione più comuni e le relative soluzioni.

Servizio di configurazione OpenSearch

Problema	Soluzione
`OpenSearch Service can't create the role` (console)	Non devi avere le autorizzazioni IAM corrette. Aggiungi le autorizzazioni specificate in the section called “Configurazione dell'autenticazione Amazon Cognito (console)”.
`User is not authorized to perform: iam:PassRole on resource CognitoAccessForAmazonOpenSearch` (console)	Non disponi `iam:PassRole` delle autorizzazioni per il CognitoAccessForAmazonOpenSearchruolo. Collega la policy seguente al tuo account: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:PassRole" ], "Resource": "arn:aws:iam:: 123456789012:role/service-role/CognitoAccessForAmazonOpenSearch " } ] }` In alternativa, puoi collegare la policy `IAMFullAccess` .
`User is not authorized to perform: cognito-identity:ListIdentityPools on resource`	Non è necessario disporre di autorizzazioni di lettura per Amazon Cognito. Collega la policy `AmazonCognitoReadOnly` al tuo account.
`An error occurred (ValidationException) when calling the CreateDomain operation`	OpenSearch Il servizio non è specificato nella relazione di fiducia del `CognitoAccessForAmazonOpenSearch` ruolo. Controlla che il ruolo usi la relazione di

Problema	Soluzione
`: OpenSearch Service must be allowed to use the passed role`	trust specificata in the section called “Informazioni sul ruolo CognitoAccessForAmazonOpenSearch”. In alternativa, per configurare l'autenticazione Amazon Cognito utilizzare la console. La console crea un ruolo per te.
`An error occurred (ValidationException) when calling the CreateDomain operation: User is not authorized to perform: cognito-idp: action on resource: user pool`	Il ruolo specificato in `--cognito-options` non ha le autorizzazioni per accedere ad Amazon Cognito. Verificare che al ruolo sia collegata la policy `AmazonOpenSearchServiceCognitoAccess` gestita da AWS. In alternativa, per configurare l'autenticazione Amazon Cognito utilizzare la console. La console crea un ruolo per te.
`An error occurred (ValidationException) when calling the CreateDomain operation: User pool does not exist`	OpenSearch Il servizio non riesce a trovare il pool di utenti. Conferma di averne creato uno e di avere l'ID corretto. Per trovare l'ID, è possibile usare la console Amazon Cognito o il seguente comando della 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 Il servizio non riesce a trovare il pool di identità. Conferma di averne creato uno e di avere l'ID corretto. Per trovare l'ID, è possibile usare la console Amazon Cognito o il seguente comando della 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`	Il pool di utenti non ha un nome di dominio. È possibile configurarne uno tramite la console Amazon Cognito o con il seguente comando della AWS CLI: `aws cognito-idp create-user-pool-domain --domain name --user-pool-id id`

Accesso ai OpenSearch pannelli di controllo

Problema	Soluzione
La pagina di accesso non mostra i provider di identità preferiti.	Verifica di aver abilitato il provider di identità per il client dell'app OpenSearch Service come specificato inthe section called “Configurazione dei provider di identità”.
La pagina di accesso non sembra associata all'organizzazione.	Consultare the section called “(Facoltativo) Personalizzazione della pagina di accesso”.
Le credenziali di accesso non funzionano.	Verifica di aver configurato il provider di identità come indicato in the section called “Configurazione dei provider di identità”. Se utilizzi il pool di utenti come provider di identità, verifica che l'account esista nella console Amazon Cognito.
OpenSearch Le dashboard non si caricano affatto o non funzionano correttamente.	Il ruolo autenticato con Amazon Cognito deve disporre delle autorizzazioni `es:ESHttp*` per il dominio (`/*`) per poter accedere e utilizzare Dashboards. Verifica di aver aggiungo una policy d'accesso come indicato in the section called “Concessione del ruolo autenticato”.
Quando esco dai OpenSearch dashboard da una scheda, nelle schede rimanenti viene visualizzato un messaggio che indica che il token di aggiornamento è stato revocato.	Quando esci da una sessione di OpenSearch Dashboards mentre utilizzi l'autenticazione Amazon Cognito OpenSearch , Service esegue AdminUserGlobalSignOutun'operazione che ti disconnette da tutte le sessioni di Dashboards OpenSearch attive.
`Invalid identity pool configuration. Check assigned IAM roles for this pool.`	Amazon Cognito non dispone delle autorizzazioni per assumere il ruolo IAM per conto dell'utente autenticato. Modificare la relazione di trust per il ruolo per includere: `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": {`

Problema	Soluzione
	"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.`	Questo errore poco comune può verificarsi quando rimuovi il client app dal pool di utenti. Provare ad aprire Dashboards in una nuova sessione del browser.

Disattivazione dell'autenticazione Amazon Cognito per dashboard OpenSearch

Usa la procedura seguente per disabilitare l'autenticazione Amazon Cognito per Dashboards.

Come disabilitare l'autenticazione Amazon Cognito per Dashboards (console)

1. Apri la console di Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home/.
2. In Domini, scegli il dominio che desideri configurare.
3. Scegli Operazioni, quindi Modifica configurazione di sicurezza.
4. Deselezionare Abilita autenticazione Amazon Cognito.
5. Sceglie Save changes (Salva modifiche).

> **Important**
>
> Se il bacino d'utenza e il pool di identità di Amazon Cognito non sono più necessari, è possibile eliminarli. Altrimenti, continuano a esserti addebitati i costi.

Eliminazione di domini che utilizzano l'autenticazione Amazon Cognito per dashboard OpenSearch

Per evitare che i domini che utilizzano l'autenticazione Amazon Cognito per dashboard rimangano bloccati in uno stato di configurazione di Elaborazione, OpenSearch elimina i domini di servizio prima di eliminare i pool di utenti e identità di Amazon Cognito associati.

Utilizzo di ruoli collegati ai servizi per Amazon Service OpenSearch

Amazon OpenSearch Service utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente al servizio. OpenSearch I ruoli collegati ai servizi sono predefiniti da OpenSearch Service e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione del OpenSearch servizio perché non è necessario aggiungere manualmente le autorizzazioni necessarie. OpenSearch Il servizio definisce le autorizzazioni dei suoi ruoli collegati al servizio e, se non diversamente definito, solo OpenSearch il servizio può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM. Per gli aggiornamenti ai ruoli collegati ai servizi e alle politiche di autorizzazione, consulta la Cronologia dei documenti per Amazon Service. OpenSearch

Per informazioni sugli altri servizi che supportano i ruoli collegati al servizio, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruoli collegati al servizio. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Argomenti

- Utilizzo di ruoli collegati ai servizi per creare domini VPC
- Utilizzo di ruoli collegati ai servizi per creare raccolte Serverless OpenSearch
- Utilizzo di ruoli collegati ai servizi per creare pipeline di ingestione OpenSearch

Utilizzo di ruoli collegati ai servizi per creare domini VPC

Amazon OpenSearch Service utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente al servizio. OpenSearch I ruoli collegati ai servizi sono predefiniti da OpenSearch Service e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

OpenSearch Il servizio utilizza il ruolo collegato al servizio denominato AWSServiceRoleForAmazonOpenSearchService, che fornisce le autorizzazioni minime di Amazon EC2 ed Elastic Load Balancing necessarie affinché il ruolo abiliti l'accesso VPC a un dominio.

Ruolo di Elasticsearch legacy

Amazon OpenSearch Service utilizza un ruolo collegato al servizio chiamato. `AWSServiceRoleForAmazonOpenSearchService` Gli account potrebbero anche contenere un ruolo collegato al servizio legacy denominato `AWSServiceRoleForAmazonElasticsearchService`, che funziona con gli endpoint dell'API Amazon Elasticsearch Service obsoleti.

Se il ruolo legacy di Elasticsearch non esiste nel tuo account, OpenSearch Service crea automaticamente un nuovo ruolo OpenSearch collegato al servizio la prima volta che crei un dominio. OpenSearch In caso contrario, l'account continua a utilizzare il ruolo Elasticsearch. Perché questa operazione di creazione automatica riesca, devi disporre delle autorizzazioni per l'operazione `iam:CreateServiceLinkedRole`.

Autorizzazioni

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForAmazonOpenSearchService` considera attendibili i seguenti servizi:

- `opensearchservice.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AmazonOpenSearchServiceRolePolicy`consente a OpenSearch Service di completare le seguenti azioni sulle risorse specificate:

- Operazione: `acm:DescribeCertificate` su `*`
- Operazione: `cloudwatch:PutMetricData` su `*`

- Operazione: `ec2:CreateNetworkInterface` su *
- Operazione: `ec2:DeleteNetworkInterface` su *
- Operazione: `ec2:DescribeNetworkInterfaces` su *
- Operazione: `ec2:ModifyNetworkInterfaceAttribute` su *
- Operazione: `ec2:DescribeSecurityGroups` su *
- Operazione: `ec2:DescribeSubnets` su *
- Operazione: `ec2:DescribeVpcs` su *
- Azione: `ec2:CreateTags` su tutte le interfacce di rete e gli endpoint VPC
- Operazione: `ec2:DescribeTags` su *
- Azione: `ec2:CreateVpcEndpoint` su tutti i VPC, i gruppi di sicurezza, le sottoreti e le tabelle di instradamento, nonché su tutti gli endpoint VPC quando la richiesta contiene il tag `OpenSearchManaged=true`
- Azione: `ec2:ModifyVpcEndpoint` su tutti i VPC, i gruppi di sicurezza, le sottoreti e le tabelle di instradamento, nonché su tutti gli endpoint VPC quando la richiesta contiene il tag `OpenSearchManaged=true`
- Azione: `ec2:DeleteVpcEndpoints` su tutti gli endpoint quando la richiesta contiene il tag `OpenSearchManaged=true`
- Operazione: `ec2:AssignIpv6Addresses` su *
- Operazione: `ec2:UnAssignIpv6Addresses` su *
- Operazione: `elasticloadbalancing:AddListenerCertificates` su *
- Operazione: `elasticloadbalancing:RemoveListenerCertificates` su *

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato ai servizi

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un dominio abilitato per VPC utilizzando AWS Management Console, OpenSearch Service crea automaticamente il ruolo collegato al servizio. Perché questa operazione di creazione automatica riesca, devi disporre delle autorizzazioni per l'operazione `iam:CreateServiceLinkedRole`.

Per creare manualmente un ruolo collegato ai servizi, è possibile utilizzare la console IAM, la CLI IAM o l'API IAM. Per ulteriori informazioni, consultare Creazione di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Modifica del ruolo collegato ai servizi

OpenSearch Il servizio non ti consente di modificare il ruolo collegato al servizio. `AWSServiceRoleForAmazonOpenSearchService` Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato ai servizi

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia del ruolo collegato ai servizi

Prima di utilizzare IAM per eliminare un ruolo collegato ai servizi, devi innanzitutto verificare che il ruolo non abbia sessioni attive ed eliminare tutte le risorse utilizzate dal ruolo.

Per verificare se il ruolo collegato ai servizi dispone di una sessione attiva nella console IAM

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM seleziona Ruoli. Quindi, scegli il nome (non la casella di controllo) del ruolo `AWSServiceRoleForAmazonOpenSearchService`.
3. Nella pagina Summary (Riepilogo) per il ruolo selezionato, scegliere la scheda Access Advisor (Consulente accessi).
4. Nella scheda Access Advisor (Consulente accessi), esamina l'attività recente per il ruolo collegato ai servizi.

> **Note**
>
> Se non sei sicuro che OpenSearch Service stia utilizzando il `AWSServiceRoleForAmazonOpenSearchService` ruolo, puoi provare a eliminare

il ruolo. Se il servizio sta utilizzando il ruolo, l'eliminazione non riesce e si possono visualizzare le risorse che utilizzano il ruolo. Se il ruolo è in uso, è necessario attendere il termine della sessione prima di poter eliminare il ruolo e/o cancellare le risorse che lo utilizzano. Non puoi revocare la sessione per un ruolo collegato al servizio.

Eliminazione manuale di un ruolo collegato ai servizi

Elimina i ruoli collegati ai servizi dalla console IAM, dall'API o dalla CLI AWS . Per le istruzioni, consultare Eliminazione di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per creare raccolte Serverless OpenSearch

OpenSearch Serverless utilizza ruoli collegati ai AWS Identity and Access Management servizi (IAM). Un ruolo collegato al servizio è un tipo unico di ruolo IAM collegato direttamente al servizio. OpenSearch I ruoli collegati ai servizi sono predefiniti da OpenSearch Service e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

OpenSearch Serverless utilizza il ruolo collegato al servizio denominato AWSServiceRoleForAmazonOpenSearchServerless, che fornisce le autorizzazioni necessarie al ruolo per pubblicare metriche relative al server sull'account dell'utente. CloudWatch La politica di autorizzazione dei ruoli associata a è denominata. AWSServiceRoleForAmazonOpenSearchServerless `AmazonOpenSearchServerlessServiceRolePolicy` Per ulteriori informazioni sulla policy, consulta AmazonOpenSearchServerlessServiceRolePolicyla AWS Managed Policy Reference Guide.

Autorizzazioni di ruolo collegate ai servizi per Serverless OpenSearch

OpenSearch Serverless utilizza il ruolo collegato al servizio denominato AWSServiceRoleForAmazonOpenSearchServerless, che consente a OpenSearch Serverless di chiamare i servizi per tuo conto. AWS

Il ruolo AWSServiceRoleForAmazonOpenSearchServerless collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `observability.aoss.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AmazonOpenSearchServerlessServiceRolePolicy` consente a OpenSearch Serverless di completare le seguenti azioni sulle risorse specificate:

- Azione: `cloudwatch:PutMetricData` su tutte le risorse AWS

> **Note**
>
> La policy include la chiave di condizione`{"StringEquals": {"cloudwatch:namespace": "AWS/AOSS"}}`, il che significa che il ruolo collegato al servizio può inviare solo dati metrici al namespace. `AWS/AOSS` CloudWatch

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato al servizio per Serverless OpenSearch

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei una raccolta OpenSearch Serverless nella AWS Management Console, nella o nell' AWS API AWS CLI, OpenSearch Serverless crea automaticamente il ruolo collegato al servizio.

> **Note**
>
> La prima volta che si crea una raccolta, è necessario ottenere l'assegnazione del ruolo `iam:CreateServiceLinkedRole` in una policy basata sull'identità.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei una raccolta Serverless, OpenSearch OpenSearch Serverless crea nuovamente il ruolo collegato al servizio per te.

Puoi anche utilizzare la console IAM per creare un ruolo collegato ai servizi con lo use case Amazon OpenSearch Serverless. Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio: `observability.aoss.amazonaws.com`

```
aws iam create-service-linked-role --aws-service-name
 "observability.aoss.amazonaws.com"
```

Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente di IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica del ruolo collegato al servizio per Serverless OpenSearch

OpenSearch Serverless non consente di modificare il ruolo collegato al servizio. AWSServiceRoleForAmazonOpenSearchServerless Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato al servizio per Serverless OpenSearch

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. Ciò impedisce di avere un'entità inutilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Per eliminare il AWSServiceRoleForAmazonOpenSearchServerless, devi prima eliminare tutte le raccolte OpenSearch Serverless presenti nel tuo. Account AWS

> **Note**
>
> Se OpenSearch Serverless utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForAmazonOpenSearchServerless servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per ruoli OpenSearch Serverless collegati ai servizi

OpenSearch Serverless supporta l'utilizzo del ruolo AWSServiceRoleForAmazonOpenSearchServerless collegato al servizio in tutte le regioni in cui è disponibile Serverless. OpenSearch Per un elenco delle regioni supportate, consulta Endpoint e quote Amazon OpenSearch Serverless nel. Riferimenti generali di AWS

Utilizzo di ruoli collegati ai servizi per creare pipeline di ingestione OpenSearch

Amazon OpenSearch Ingestion utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Ingestion. OpenSearch I ruoli collegati ai servizi sono predefiniti da OpenSearch Ingestion e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per conto dell'utente. AWS

OpenSearch Ingestion utilizza il ruolo collegato al servizio denominato AWSServiceRoleForAmazonOpenSearchIngestionService, tranne quando si utilizza un VPC autogestito, nel qual caso utilizza il ruolo collegato al servizio denominato. AWSServiceRoleForOpensearchIngestionSelfManagedVpce La policy allegata fornisce le autorizzazioni necessarie al ruolo per creare un cloud privato virtuale (VPC) tra il tuo account OpenSearch e Ingestion e per CloudWatch pubblicare le metriche sul tuo account.

Autorizzazioni

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForAmazonOpenSearchIngestionService` considera attendibili i seguenti servizi:

- `osis.amazon.com`

La politica di autorizzazione dei ruoli denominata `AmazonOpenSearchIngestionServiceRolePolicy` consente a OpenSearch Ingestion di completare le seguenti azioni sulle risorse specificate:

- Operazione: `ec2:DescribeSubnets` su `*`
- Operazione: `ec2:DescribeSecurityGroups` su `*`
- Operazione: `ec2:DeleteVpcEndpoints` su `*`

- Operazione: `ec2:CreateVpcEndpoint` su `*`
- Operazione: `ec2:DescribeVpcEndpoints` su `*`
- Operazione: `ec2:CreateTags` su `arn:aws:ec2:*:*:network-interface/*`
- Operazione: `cloudwatch:PutMetricData` su `cloudwatch:namespace": "AWS/OSIS"`

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForOpensearchIngestionSelfManagedVpce` considera attendibili i seguenti servizi:

- `self-managed-vpce.osis.amazon.com`

La politica di autorizzazione dei ruoli denominata `OpenSearchIngestionSelfManagedVpcePolicy` consente a OpenSearch Ingestion di completare le seguenti azioni sulle risorse specificate:

- Operazione: `ec2:DescribeSubnets` su `*`
- Operazione: `ec2:DescribeSecurityGroups` su `*`
- Operazione: `ec2:DescribeVpcEndpoints` su `*`
- Operazione: `cloudwatch:PutMetricData` su `cloudwatch:namespace": "AWS/OSIS"`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato al servizio per Ingestion OpenSearch

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando create una pipeline di OpenSearch Ingestion nell'API, nella o nell' AWS API AWS Management Console, OpenSearch Ingestion crea automaticamente il ruolo collegato al servizio. AWS CLI

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei una pipeline di Ingestion, OpenSearch Ingestion crea nuovamente il ruolo collegato al servizio per te. OpenSearch

Modifica del ruolo collegato al servizio per Ingestion OpenSearch

OpenSearch Ingestion non consente di modificare il ruolo collegato al servizio. `AWSServiceRoleForAmazonOpenSearchIngestionService` Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato al servizio per Ingestion OpenSearch

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo.

> **Note**
>
> Se OpenSearch Ingestion utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse OpenSearch di Ingestion utilizzate dal ruolo or **`AWSServiceRoleForAmazonOpenSearchIngestionServiceAWSServiceRoleForOpensearchInge`**

1. Vai alla console di Amazon OpenSearch Service e scegli Ingestion.
2. Elimina tutte le pipeline. Per istruzioni, consulta the section called “Eliminazione delle tubazioni”.

Eliminare il ruolo collegato al servizio per Ingestion OpenSearch

È possibile utilizzare la console OpenSearch Ingestion per eliminare un ruolo collegato al servizio.

Per eliminare un ruolo collegato ai servizi (console)

1. Passare alla IAM console (Console IAM).

2. Scegli Ruoli e cerca il ruolo o. AWSServiceRoleForAmazonOpenSearchIngestionServiceAWSServiceRoleForOpensearchIngestionSel
3. Seleziona il ruolo e scegli Elimina.

Codice di esempio per AmazonOpenSearchServizio

Questo capitolo contiene un codice di esempio comune per lavorare con AmazonOpenSearchServizio: firma di richieste HTTP in una varietà di linguaggi di programmazione, compressione dei corpi delle richieste HTTP e utilizzo delAWSSDK per creare domini.

Argomenti

Compatibilità con i client Elasticsearch

Le versioni più recenti dei client Elasticsearch potrebbero includere controlli di licenza o versione che violano artificialmente la compatibilità. La tabella seguente include consigli sulle versioni di tali client da utilizzare per una migliore compatibilità conOpenSearchServizio.

> **Important**
>
> Queste versioni client non sono aggiornate e non sono aggiornate con le ultime dipendenze, incluso Log4j. Consigliamo vivamente di utilizzareOpenSearchversioni dei client quando possibile.

Client	Versioni suggerite
Client REST Java di basso livello	7.13.4
Client REST Java di livello elevato	7.13.4
Client Elasticsearch Python	7.13.4
Client Elasticsearch Ruby	7.13.3
Client Elasticsearch Node.js	7.13.0

Compressione delle richieste HTTP in Amazon OpenSearch Service

Puoi comprimere le richieste e le risposte HTTP nei domini Amazon OpenSearch Service utilizzando la compressione gzip. La compressione gzip consente di ridurre le dimensioni dei documenti e di ridurre l'utilizzo della larghezza di banda e la latenza, migliorando così la velocità di trasferimento.

La compressione Gzip è supportata per tutti i domini che eseguono Elasticsearch 6.0 OpenSearch o versioni successive. Alcuni OpenSearch client dispongono del supporto integrato per la compressione gzip e molti linguaggi di programmazione dispongono di librerie che semplificano il processo.

Abilitazione della compressione gzip

Da non confondere con OpenSearch impostazioni simili, `http_compression.enabled` è specifico di OpenSearch Service e abilita o disabilita la compressione gzip su un dominio. Domini in esecuzione OpenSearch o Elasticsearch 7. x hanno la compressione gzip abilitata per impostazione predefinita, mentre i domini che eseguono Elasticsearch 6. x l'hanno disabilitata per impostazione predefinita.

Per abilitare la compressione gzip, inviare la seguente richiesta:

```
PUT _cluster/settings
{
  "persistent" : {
    "http_compression.enabled": true
  }
}
```

Le richieste a `_cluster/settings` devono essere decompresse, quindi potrebbe essere necessario utilizzare un client separato o una richiesta HTTP standard per aggiornare le impostazioni del cluster.

Per confermare di aver abilitato correttamente la compressione gzip, invia la seguente richiesta:

```
GET _cluster/settings?include_defaults=true
```

Assicurati di vedere la seguente impostazione nella risposta:

```
...
```

```
"http_compression": {
  "enabled": "true"
}
...
```

Intestazioni richieste

Quando si include un corpo di richiesta compresso con gzip, mantenere l'intestazione `Content-Type: application/json` standard e aggiungere l'intestazione `Content-Encoding: gzip`. Per accettare una risposta gzip compressa, aggiungere anche l'intestazione `Accept-Encoding: gzip`. Se un OpenSearch client supporta la compressione gzip, probabilmente include queste intestazioni automaticamente.

Codice di esempio (Python 3)

Nell'esempio seguente viene utilizzato opensearch-py per eseguire la compressione e inviare la richiesta. Questo codice firma la richiesta utilizzando le credenziali 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))
```

In alternativa, è possibile specificare le intestazioni corrette, comprimere il corpo della richiesta da soli e utilizzare una libreria HTTP standard come Requests. Questo codice firma la richiesta utilizzando le credenziali di base HTTP, che il dominio potrebbe supportare se si utilizza il controllo granulare degli accessi.

```
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)
```

Usando ilAWSSDK per interagire con AmazonOpenSearchServizio

Questa sezione include esempi di come utilizzareAWSSDK per interagire con AmazonOpenSearchAPI di configurazione del servizio. Questi esempi di codice mostrano come creare, aggiornare ed eliminareOpenSearchDomini di servizio.

Java

Questa sezione include esempi per le versioni 1 e 2 del AWS SDK for Java.

Version 2

Questo esempio utilizzaOpenSearchClientBuildercostruttore della versione 2 delAWS SDK for Javaper creare unOpenSearchdominio, aggiorna la sua configurazione ed eliminalo. Rimuovere il commento dalle chiamate a `waitForDomainProcessing` (e commentare la chiamata a `deleteDomain`) per fare in modo che il dominio sia online e utilizzabile.

```
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

Questo esempio utilizzaAWSElasticsearchClientBuildercostruttore della versione 1 delAWS SDK for Javaper creare un dominio Elasticsearch obsoleto, aggiornarne la configurazione ed eliminarlo. Rimuovere il commento dalle chiamate a `waitForDomainProcessing` (e commentare la chiamata a `deleteDomain`) per fare in modo che il dominio sia online e utilizzabile.

```
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

Questo esempio utilizzaOpenSearchServiceclient Python di basso livello delAWS SDK for Python (Boto)per creare un dominio, aggiornarne la configurazione ed 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

Questo esempio utilizza la versione 3 dell'SDK perJavaScriptin Node.jsOpenSearchclienteper creare un dominio, aggiornarne la configurazione ed 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.');
            }
    };
}
```

Indicizzazione dei dati in Amazon Service OpenSearch

Poiché Amazon OpenSearch Service utilizza un'API REST, esistono numerosi metodi per indicizzare i documenti. Puoi utilizzare client standard come curl o qualsiasi linguaggio di programmazione in grado di inviare richieste HTTP. Per semplificare ulteriormente il processo di interazione con essa, OpenSearch Service dispone di client per molti linguaggi di programmazione. Gli utenti esperti possono passare direttamente a the section called “Caricamento di dati di streaming in OpenSearch Service”.

Ti consigliamo vivamente di utilizzare Amazon OpenSearch Ingestion per importare dati, un raccoglitore di dati completamente gestito integrato in Service. OpenSearch Per ulteriori informazioni, consulta Amazon OpenSearch Ingestion.

Per un'introduzione all'indicizzazione, consulta la documentazione. OpenSearch

Limitazioni di denominazione per gli indici

OpenSearch Gli indici dei servizi presentano le seguenti restrizioni di denominazione:

- Tutte le lettere devono essere minuscole.
- I nomi degli indici non possono iniziare con `_` o `-`.
- I nomi degli indici non possono contenere spazi, virgole, `:`, `"`, `*`, `+`, `/`, `\`, `|`, `?`, `#`, `>` o `<`.

Non includere informazioni riservate nei nomi degli indici, dei tipi o degli ID dei documenti. OpenSearch Il servizio utilizza questi nomi nei suoi Uniform Resource Identifiers (URI). I server e le applicazioni registrano spesso le richieste HTTP, il che può causare un'inutile esposizione dei dati se gli URI contengono informazioni sensibili.

```
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"
```

Anche se non si dispone delle autorizzazioni per visualizzare il documento JSON associato, è possibile dedurre da questa riga fittizia del log che uno dei pazienti del Dr. Doe con numero di telefono 202-555-0100 ha avuto l'influenza nel 2018.

Se OpenSearch Service rileva un indirizzo IP reale o percepito in un nome di indice (ad esempio,`my-index-12.34.56.78.91`), maschera l'indirizzo IP. Una chiamata a `_cat/indices` produce la risposta seguente:

```
green open my-index-x.x.x.x.91    soY19tBERoKo71WcEScidw 5 1 0 0   2kb  1kb
```

Per evitare inutili confusioni, evitare di includere indirizzi IP nei nomi di indice.

Riduzione delle dimensioni della risposta

Le risposte dalle API `_index` e `_bulk` contengono diverse informazioni. Queste informazioni possono essere utili per le richieste di risoluzione dei problemi o per l'implementazione della logica dei tentativi, ma possono utilizzare una larghezza di banda considerevole. In questo esempio, l'indicizzazione di un documento a 32 byte genera una risposta a 339 byte (incluse le intestazioni):

```
PUT opensearch-domain/more-movies/_doc/1
{"title": "Back to the Future"}
```

Risposta

```
{
  "_index": "more-movies",
  "_type": "_doc",
  "_id": "1",
  "_version": 4,
  "result": "updated",
  "_shards": {
    "total": 2,
    "successful": 2,
    "failed": 0
  },
  "_seq_no": 3,
  "_primary_term": 1
}
```

Questa dimensione della risposta potrebbe sembrare minima, ma se si indicizza 1.000.000 di documenti al giorno, circa 11,5 documenti al secondo, 339 byte per risposta sono 10,17 GB di traffico di download al mese.

Se i costi di trasferimento dei dati sono un problema, utilizzate il `filter_path` parametro per ridurre le dimensioni della risposta del OpenSearch Servizio, ma fate attenzione a non filtrare i campi necessari per identificare o riprovare le richieste non riuscite. Questi campi possono variare a seconda del client. Il `filter_path` parametro funziona per tutte le API REST del OpenSearch servizio, ma è particolarmente utile con le API che chiamate frequentemente, come le `_index` API and: `_bulk`

```
PUT opensearch-domain/more-movies/_doc/1?filter_path=result,_shards.total
{"title": "Back to the Future"}
```

Risposta

```
{
  "result": "updated",
  "_shards": {
    "total": 2
  }
}
```

Invece di includere i campi, puoi escluderli con un prefisso `-`. `filter_path` supporta anche i caratteri jolly:

```
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"}
```

Risposta

```
{
  "errors": false,
  "items": [
    {
      "index": {
        "result": "updated",
        "status": 200
      }
    },
    {
      "index": {
```

```
        "result": "updated",
        "status": 200
      }
    }
  ]
}
```

Codec indicizzati

I codec di indice determinano il modo in cui i campi memorizzati in un indice vengono compressi e archiviati su disco. Il codec dell'indice è controllato dall'`index.codec`impostazione statica, che specifica l'algoritmo di compressione. Questa impostazione influisce sulla dimensione del frammento di indice e sulle prestazioni operative.

Per un elenco dei codec supportati e delle relative caratteristiche prestazionali, consultate Codec supportati nella documentazione. OpenSearch

Quando scegliete un codec di indice, tenete presente quanto segue:

- Per evitare i problemi legati alla modifica dell'impostazione del codec di un indice esistente, testate un carico di lavoro rappresentativo in un ambiente non di produzione prima di utilizzare una nuova impostazione del codec. Per ulteriori informazioni, consultate Modifica di un codec di indice.
- Non puoi utilizzare i codec di compressione Zstandard (`"index.codec": "zstd"o"index.codec": "zstd_no_dict"`) per gli indici k-NN o Security Analytics.

Caricamento di dati di streaming in Amazon OpenSearch Service

Puoi utilizzare OpenSearch Ingestion per caricare direttamente i dati di streaming nel tuo dominio Amazon OpenSearch Service, senza dover utilizzare soluzioni di terze parti. Per inviare dati a OpenSearch Ingestion, configuri i produttori di dati e il servizio consegna automaticamente i dati al dominio o alla raccolta specificati. Per iniziare a usare OpenSearch Ingestion, consulta. the section called “Tutorial: inserisci dati in una raccolta”

Puoi comunque utilizzare altre fonti per caricare dati in streaming, come Amazon Data Firehose e Amazon CloudWatch Logs, che dispongono del supporto integrato per Service. OpenSearch Altre, come Amazon S3, Amazon Kinesis Data Streams e Amazon DynamoDB, utilizzano le funzioni AWS Lambda come gestori di eventi. Le funzioni Lambda rispondono ai nuovi dati elaborandoli ed eseguendone lo streaming nel dominio.

> **Note**
>
> Lambda supporta diversi linguaggi di programmazione tra i più diffusi ed è disponibile in gran parte delle Regioni AWS. Per ulteriori informazioni, consulta Getting started with Lambda nella AWS Lambda Developer Guide e AWS Service Endpoints nel. Riferimenti generali di AWS

Argomenti

Caricamento di dati di streaming da Ingestion OpenSearch

Puoi usare Amazon OpenSearch Ingestion per caricare dati in un dominio di OpenSearch servizio. Puoi configurare i produttori di dati per inviare dati a OpenSearch Ingestion, che li invia automaticamente alla raccolta specificata. Puoi anche configurare OpenSearch Ingestion per trasformare i dati prima di consegnarli. Per ulteriori informazioni, consulta OpenSearch Ingestione di Amazon.

Caricamento di dati in streaming da Amazon S3

Puoi usare Lambda per inviare dati al tuo dominio di OpenSearch servizio da Amazon S3. I nuovi dati che arrivano in un bucket S3 attivano una notifica eventi per Lambda, che quindi esegue il codice personalizzato per eseguire l'indicizzazione.

Questo metodo per lo streaming dei dati è estremamente flessibile. Puoi indicizzare i metadati degli oggetti oppure, se l'oggetto è un testo normale, analizzare e indicizzare alcuni elementi del corpo dell'oggetto. Questa sezione include alcuni semplici codici Python di esempio in cui sono utilizzate espressioni regolari per analizzare un file di log e indicizzare le corrispondenze.

Prerequisiti

Prima di procedere, devi disporre delle risorse indicate di seguito.

Prerequisito	Descrizione
Bucket Amazon S3	Per ulteriori informazioni, consulta Creazione del primo bucket S3 nella Guida per l'utente di Amazon Simple Storage Service. Il bucket deve risiedere nella stessa regione del dominio di servizio. OpenSearch
OpenSearch Dominio di servizio	La destinazione dei dati dopo che la funzione Lambda li ha elaborati. Per ulteriori informazioni, consultare the section called “ Creazione di domini OpenSearch di servizio”.

Creazione il pacchetto di implementazione Lambda

I pacchetti di distribuzione sono file ZIP o JAR che includono codice ed eventuali dipendenze. In questa sezione è incluso codice di esempio Python. Per altri linguaggi di programmazione, consultare Pacchetti di implementazione Lambda nella Guida per gli sviluppatori diAWS Lambda .

1. Crea una directory. In questo esempio utilizziamo il nome `s3-to-opensearch`.
2. Creare un file nella directory denominata `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)
```

Modifica le variabili per `region` e `host`.

3. Installare pip, se non è già stato fatto, quindi installare le dipendenze in una nuova directory `package`:

```
cd s3-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

In tutti gli ambienti di esecuzione Lambda è installato Boto3, perciò non è necessario includerlo nel pacchetto di implementazione.

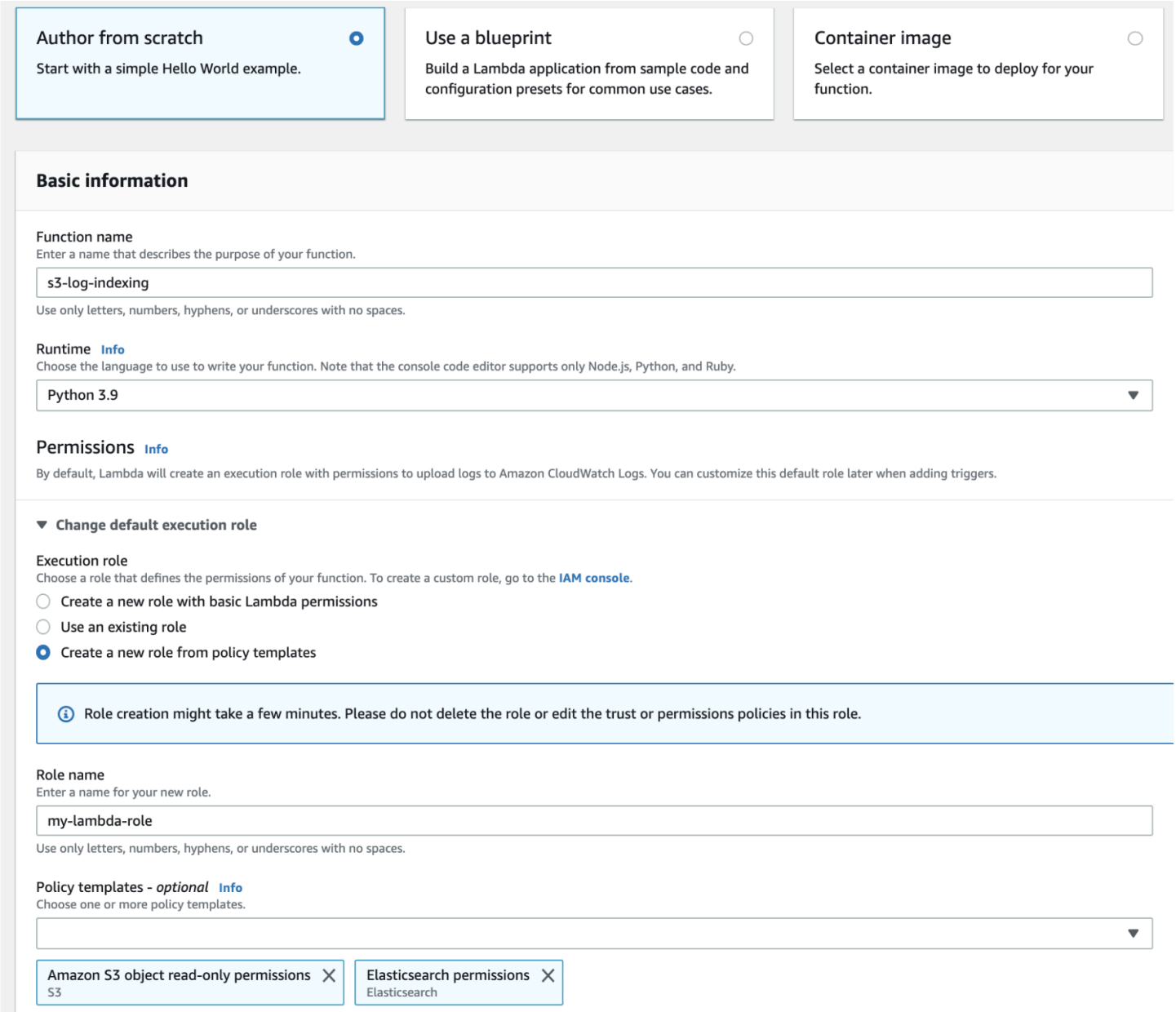
4. Crea un pacchetto con il codice dell'applicazione e le dipendenze:

```
cd package
zip -r ../lambda.zip .

cd ..
zip -g lambda.zip sample.py
```

Creazione della funzione Lambda

Dopo aver creato il pacchetto di implementazione, è possibile creare la funzione Lambda. Quando si crea una funzione, scegliere nome, runtime (ad esempio, Python 3.8) e ruolo IAM. Il ruolo IAM definisce le autorizzazioni per la tua funzione. Per istruzioni dettagliate, consultare Creazione di una funzione Lambda con la console nella Guida per gli sviluppatori diAWS Lambda .

Questo esempio presuppone l'utilizzo della console. Scegli Python 3.9 e un ruolo con autorizzazioni di lettura S3 e autorizzazioni di scrittura del OpenSearch servizio, come mostrato nella schermata seguente:



Una volta creata la funzione, devi aggiungere un trigger. In questo esempio, vogliamo che il codice venga eseguito ogni volta che un file di log arriva in un bucket S3:

1. Scegliere Aggiungi trigger e selezionare S3.
2. Scegli il bucket.
3. Per Event type (Tipo di evento), seleziona PUT.
4. In Prefix (Prefisso), digita `logs/`.
5. Per Suffisso, digitare `.log`.
6. Confermare l'avviso di chiamata ricorsiva e scegliere Aggiungi.

Puoi infine caricare il pacchetto di implementazione:

1. Scegliere Carica da e File .zip, quindi seguire i prompt su schermo per caricare il pacchetto di implementazione.
2. Al termine del caricamento, modificare il campo Impostazioni runtime e cambiare il gestore in `sample.handler`. Questa impostazione indica a Lambda il file (`sample.py`) e il metodo (`handler`) da eseguire dopo un trigger.

A questo punto, hai un set completo di risorse: un bucket per i file di registro, una funzione che viene eseguita ogni volta che viene aggiunto un file di registro al bucket, codice che esegue l'analisi e l'indicizzazione e un dominio di servizio per la ricerca e la visualizzazione. OpenSearch

Test della funzione Lambda

Una volta creata la funzione, è possibile eseguirne il test caricando un file nel bucket Amazon S3. Crea un file denominato `sample.log` utilizzando le righe di log di esempio indicate di seguito:

```
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"
```

Carica il file nella cartella `logs` del bucket S3. Per le istruzioni, consulta Caricamento di un oggetto nel bucket nella Guida per l'utente di Amazon Simple Storage Service.

Utilizza quindi la console di OpenSearch servizio o le OpenSearch dashboard per verificare che l'indice contenga due documenti. `lambda-s3-index` Puoi anche effettuare una richiesta di ricerca standard:

```
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"
        }
      }
    ]
  }
}
```

Caricamento dei dati in streaming in Amazon Kinesis Data Streams

È possibile caricare dati di streaming da Kinesis Data OpenSearch Streams to Service. I nuovi dati che arrivano nel flusso di dati attivano una notifica eventi per Lambda, che quindi esegue il codice personalizzato per eseguire l'indicizzazione. In questa sezione è incluso un semplice codice di esempio Python.

Prerequisiti

Prima di procedere, devi disporre delle risorse indicate di seguito.

Prerequisito	Descrizione
Amazon Kinesis Data Streams	L'origine dell'evento per la funzione Lambda. Per ulteriori informazioni, consultare Kinesis Data Streams.
OpenSearch Dominio di servizio	La destinazione dei dati dopo che la funzione Lambda li ha elaborati. Per ulteriori informazioni, consultare the section called “ Creazione di domini OpenSearch di servizio”
Ruolo IAM	Questo ruolo deve avere le autorizzazioni di base OpenSearch Service, Kinesis e Lambda, come le seguenti:

Prerequisito	Descrizione

```
{
  "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": "*"
    }
  ]
}
```

Il ruolo deve avere la relazione di trust seguente:

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

Per ulteriori informazioni, consultare Creazione di ruoli IAM nella Guida per l'utente di IAM.

Creazione della funzione Lambda

Procedi come descritto in the section called “Creazione il pacchetto di implementazione Lambda”, ma crea una directory denominata `kinesis-to-opensearch` e utilizza il codice seguente per `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.'
```

Modifica le variabili per `region` e `host`.

Installare pip, se non è già stato fatto, quindi utilizzare i seguenti comandi per installare le dipendenze:

```
cd kinesis-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Procedi quindi come descritto in the section called “Creazione della funzione Lambda”, ma specifica il ruolo IAM dai the section called “Prerequisiti” e le impostazioni seguenti per il trigger:

- Flusso Kinesis: il flusso di Kinesis.
- Batch size (Dimensione batch): 100
- Starting position (Posizione di inizio): orizzonte di taglio

Per ulteriori informazioni, consultare Cos'è Amazon Kinesis Data Streams? nella Guida per gli sviluppatori di Amazon Kinesis Data Streams.

A questo punto, hai a disposizione un set completo di risorse: un flusso di dati Kinesis, una funzione che viene eseguita dopo che il flusso riceve nuovi dati e li indicizza e un dominio di OpenSearch servizio per la ricerca e la visualizzazione.

Test della funzione Lambda

Una volta creata la funzione, puoi provarla aggiungendo un nuovo record al flusso di dati utilizzando l' AWS CLI:

```
aws kinesis put-record --stream-name test --data "My test data." --partition-key
 partitionKey1 --region us-west-1
```

Quindi utilizza la console di OpenSearch servizio o le OpenSearch dashboard per verificare che contenga un documento. `lambda-kine-index` Puoi inoltre utilizzare la seguente richiesta:

```
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"
      }
    }
  ]
}
```

Caricamento di dati in streaming da una tabella Amazon DynamoDB

Puoi utilizzarlo AWS Lambda per inviare dati al tuo dominio di OpenSearch servizio da Amazon DynamoDB. I nuovi dati che arrivano nella tabella di database attivano una notifica eventi per Lambda, che quindi esegue il codice personalizzato per eseguire l'indicizzazione.

Prerequisiti

Prima di procedere, devi disporre delle risorse indicate di seguito.

Prerequisito	Descrizione
DynamoDB tabella	La tabella contiene i dati di origine. Per ulteriori informazioni, consultare Operazioni di base sulle tabelle DynamoDB nella Guida per gli sviluppat ori di Amazon DynamoDB. La tabella deve risiedere nella stessa regione del dominio di OpenSearc h servizio e avere uno stream impostato su Nuova immagine. Per ulteriori informazioni, consultare Abilitazione di un flusso.
OpenSearch Dominio di servizio	La destinazione dei dati dopo che la funzione Lambda li ha elaborati. Per ulteriori informazioni, consultare the section called “ Creazione di domini OpenSearch di servizio”.
Ruolo IAM	Questo ruolo deve disporre delle autorizzazioni di esecuzione di base di OpenSearch Service, DynamoDB e Lambda, come le seguenti:

Prerequisito	Descrizione

```
{
  "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": "*"
    }
  ]
}
```

Il ruolo deve avere la relazione di trust seguente:

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

Per ulteriori informazioni, consultare Creazione di ruoli IAM nella Guida per l'utente di IAM.

Creazione della funzione Lambda

Procedi come descritto in the section called “Creazione il pacchetto di implementazione Lambda”, ma crea una directory denominata `ddb-to-opensearch` e utilizza il codice seguente per `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.'
```

Modifica le variabili per `region` e `host`.

Installare pip, se non è già stato fatto, quindi utilizzare i seguenti comandi per installare le dipendenze:

```
cd ddb-to-opensearch
```

```
pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Procedi quindi come descritto in the section called “Creazione della funzione Lambda”, ma specifica il ruolo IAM dai the section called “Prerequisiti” e le impostazioni seguenti per il trigger:

- Tabella: la tabella DynamoDB
- Batch size (Dimensione batch): 100
- Starting position (Posizione di inizio): orizzonte di taglio

Per ulteriori informazioni, consultare Elaborazione di nuovi elementi con DynamoDB Streams e Lambdanella Guida per gli sviluppatori di Amazon DynamoDB.

A questo punto, hai a disposizione un set completo di risorse: una tabella DynamoDB per i dati di origine, un flusso DynamoDB di modifiche alla tabella, una funzione che viene eseguita dopo le modifiche dei dati di origine e indicizza tali modifiche e un dominio di servizio per la ricerca e la visualizzazione. OpenSearch

Test della funzione Lambda

Una volta creata la funzione, è possibile eseguirne il test aggiungendo un nuovo elemento alla tabella DynamoDB utilizzando 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
```

Utilizzate quindi la console di OpenSearch servizio o le OpenSearch dashboard per verificare che contenga un documento. `lambda-index` Puoi inoltre utilizzare la seguente richiesta:

```
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"
        }
    }
}
```

Caricamento di dati di streaming da Amazon Data Firehose

Firehose supporta il OpenSearch Servizio come destinazione di consegna. Per istruzioni su come caricare i dati di streaming in OpenSearch Service, consulta Creating a Kinesis Data Firehose Delivery Stream OpenSearch e Choose Service for Your Destination nella Amazon Data Firehose Developer Guide.

Prima di caricare i dati in OpenSearch Service, potrebbe essere necessario eseguire delle trasformazioni sui dati. Per ulteriori informazioni su come usare le funzioni Lambda per completare questa attività, consultare Trasformazione dei dati di Amazon Kinesis Data Firehose nella stessa guida.

Durante la configurazione di un flusso di distribuzione, Firehose offre un ruolo IAM «one-click» che gli fornisce l'accesso alle risorse di cui ha bisogno per inviare dati a OpenSearch Service, eseguire il backup dei dati su Amazon S3 e trasformarli utilizzando Lambda. Poiché creare un ruolo simile manualmente sarebbe molto complesso, è consigliabile utilizzare il ruolo fornito.

Caricamento di dati di streaming da Amazon CloudWatch

Puoi caricare dati di streaming da CloudWatch Logs al tuo dominio OpenSearch di servizio utilizzando un abbonamento CloudWatch Logs. Per informazioni sugli CloudWatch abbonamenti Amazon, consulta Elaborazione in tempo reale dei dati di registro con gli abbonamenti. Per informazioni sulla configurazione, consulta Streaming CloudWatch Logs data to Amazon OpenSearch Service nell'Amazon CloudWatch Developer Guide.

Caricamento di dati in streaming da AWS IoT

Puoi inviare dati AWS IoT utilizzando regole. Per ulteriori informazioni, consulta l'OpenSearchazione nella Guida per gliAWS IoT sviluppatori.

Caricamento dei dati in Amazon OpenSearch Service con Logstash

La versione open source di Logstash (Logstash OSS) fornisce un modo conveniente per utilizzare l'API bulk per caricare i dati nel dominio Amazon OpenSearch Service. Il servizio supporta tutti i plug-in di input Logstash standard, incluso il plug-in di input Amazon S3. OpenSearch Il servizio supporta il plug-in logstash-output-opensearchdi output, che supporta sia l'autenticazione di base che le credenziali IAM. Il plug-in funziona con la versione 8.1 e precedenti di Logstash OSS.

Configurazione

La configurazione di Logstash varia in base al tipo di autenticazione utilizzata dal dominio.

Indipendentemente dal metodo di autenticazione utilizzato, è necessario impostare `ecs_compatibility` a `disabled` nella sezione di output del file di configurazione. Logstash 8.0 ha introdotto un cambiamento rivoluzionario in cui vengono eseguiti tutti i plug-in in Modalità di compatibilità ECS per impostazione predefinita. È necessario sostituire il valore di default per mantenere il comportamento legacy.

Configurazione dettagliata dei controlli degli accessi

Se il dominio OpenSearch Service utilizza il controllo granulare degli accessi con l'autenticazione di base HTTP, la configurazione è simile a quella di qualsiasi altro OpenSearch cluster. Questo file di configurazione di esempio prende il suo input dalla versione open source di 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 configurazione varia in base all'applicazione Beats e al caso d'uso, ma la configurazione di Filebeat OSS potrebbe essere simile a questa:

```
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"]
```

Configurazione IAM

Se il dominio utilizza una policy di accesso al dominio basata su IAM o un controllo granulare degli accessi con un utente principale, è necessario firmare tutte le richieste per OpenSearch Service tramite le credenziali IAM. La seguente policy basata su identità concede tutte le richieste ad alcune o a tutte le risorse del dominio.

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

Per la configurazione di Logstash, modifica il file di configurazione per utilizzare il plug-in per il suo output. Questo file di configurazione di esempio prende il suo input dai file in un bucket 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
  }
}
```

Se non si desidera fornire le credenziali IAM all'interno del file di configurazione, è possibile esportarle (o eseguirle `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"
```

Se il dominio OpenSearch Service è in un VPC, la macchina di Logstash OSS deve essere in grado di connettersi al VPC e accedere al dominio tramite i gruppi di sicurezza del VPC. Per ulteriori informazioni, consulta the section called “Informazioni sulle policy d'accesso nei domini VPC”.

Ricerca di dati in Amazon OpenSearch Service

Esistono diversi metodi comuni per la ricerca di documenti in Amazon OpenSearch Service, tra cui ricerche URI e ricerche nel corpo della richiesta. OpenSearch Il servizio offre funzionalità aggiuntive che migliorano l'esperienza di ricerca, come pacchetti personalizzati, supporto SQL e ricerca asincrona. Per un riferimento completo all'API OpenSearch di ricerca, consulta la documentazione. OpenSearch

> **Note**
>
> Le seguenti richieste di esempio funzionano con le OpenSearch API. Alcune richieste potrebbero non funzionare con versioni precedenti di Elasticsearch.

Argomenti

Ricerche negli URI

Le ricerche URI (Universal Resource Identifier) sono la forma di ricerca più semplice. In una ricerca URI, si specifica la query come un parametro di richiesta HTTP:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/_search?q=house
```

L'aspetto di una risposta di esempio è simile al seguente:


```
{
  "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"
        }
      },
      ...
    ]
  }
}
```

Per impostazione predefinita, questa query ricerca il termine house in tutti i campi di tutti gli indici. Per restringere la ricerca, specifica un indice (`movies`) e un campo di documento (`title`) nell'URI:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?q=title:house
```

È possibile includere parametri aggiuntivi nella richiesta, ma i parametri supportati forniscono solo un piccolo sottoinsieme delle opzioni di OpenSearch ricerca. La seguente richiesta restituisce 20 risultati (anziché il numero predefinito di 10) ordinati per anno (anziché per `_score`):

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?
q=title:house&size=20&sort=year:desc
```

Ricerche nel corpo della richiesta

Per eseguire ricerche più complesse, utilizzate il corpo della richiesta HTTP e il linguaggio OpenSearch specifico del dominio (DSL) per le query. La query DSL consente di specificare l'intera gamma di opzioni di ricerca. OpenSearch

> **Note**
>
> Non è possibile includere caratteri speciali Unicode nel valore di un campo di testo, altrimenti il valore verrà analizzato come valori multipli separati dal carattere speciale. Questa analisi errata può portare a un filtraggio involontario dei documenti e persino compromettere il controllo sul loro accesso. Per ulteriori informazioni, vedere Una nota sui caratteri speciali Unicode nei campi di testo nella OpenSearch documentazione.

La seguente query `match` è simile all'esempio di ricerca URI finale:

```
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**
>
> L'API `_search` accetta `GET` e `POST` HTTP per ricerche del corpo della richiesta, ma non tutti i client HTTP supportano l'aggiunta di un corpo della richiesta a una richiesta `GET`. `POST` è la scelta più universale.

In molti casi, potrebbe essere necessario eseguire la ricerca in diversi campi, ma non in tutti. Utilizza la query `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"]
    }
  }
}
```

Campi di boosting

Puoi migliorare la rilevanza della ricerca "potenziando" alcuni campi. I boost sono moltiplicatori che valutano le corrispondenze in un campo più pesantemente rispetto alle corrispondenze in altri campi. Nel seguente esempio, una corrispondenza per john nel campo `title` influenza `_score` il doppio di una corrispondenza nel campo `plot` e quattro volte di più di una corrispondenza nei campi `actors` o `directors`. Ne risulta che film come John Wick e John Carter sono vicini alla parte alta dei risultati della ricerca e film con protagonista John Travolta sono nella parte bassa.

```
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"]
    }
  }
}
```

Evidenziazione dei risultati della ricerca

L'`highlight`opzione indica OpenSearch di restituire un oggetto aggiuntivo all'interno dell'`hits`array se la query corrisponde a uno o più campi:

```
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": {}
    }
  }
}
```

Se la query corrisponde al contenuto del campo `plot`, l'aspetto di un'occorrenza è simile al seguente:


```
{
  "_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>."
    ]
  }
}
```


Per impostazione predefinita, OpenSearch racchiude la stringa corrispondente nei tag, fornisce fino a 100 caratteri di contesto attorno alla corrispondenza e suddivide il contenuto in frasi

identificando segni di punteggiatura, spazi, tabulazioni e interruzioni di riga. Tutte queste impostazioni sono personalizzabili:

```
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 conteggio

Se non sei interessato ai contenuti dei documenti e desideri solo conoscere il numero di corrispondenze, puoi utilizzare l'API `_count` anziché l'API `_search`. La seguente richiesta utilizza la query `query_string` per identificare commedie romantiche:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_count
{
  "query": {
    "query_string": {
      "default_field": "genres",
      "query": "romance AND comedy"
    }
  }
}
```

L'aspetto di una risposta di esempio è simile al seguente:

```
{
```

```
  "count": 564,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  }
}
```

Paginazione dei risultati della ricerca

Se è necessario visualizzare un gran numero di risultati di ricerca, è possibile implementare l'impaginazione utilizzando diversi metodi.

Punto nel tempo

La funzionalità point in time (PIT) è un tipo di ricerca che consente di eseguire diverse query su un set di dati fisso nel tempo. Questo è il metodo di impaginazione preferito in OpenSearch, specialmente per l'impaginazione profonda. È possibile utilizzare PIT con OpenSearch Service versione 2.5 e successive. Per ulteriori informazioni su PIT, vedere???.

I `size` parametri `from` e

Il modo più semplice per impaginare è con i `size` parametri `from` and. La richiesta seguente restituisce i risultati 20-39 dell'elenco indicizzato su zero dei risultati della ricerca:

```
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"]
    }
  }
}
```

Per ulteriori informazioni sull'impaginazione della ricerca, consulta Impaginare i risultati nella documentazione. OpenSearch

Linguaggio query dashboard

Puoi utilizzare il Dashboards Query Language (DQL) per cercare dati e visualizzazioni nelle dashboard. OpenSearch DQL utilizza quattro tipi di query principali: termini, booleano, data e intervallo e campo nidificata.

Query di termine

Una query di termini richiede di specificare il termine che si sta cercando.

Per eseguire una query di termini, inserisci quanto segue:

```
host:www.example.com
```

Query booleano

Puoi utilizzare gli operatori booleani `AND`, `or` e `not` per combinare più query.

Per eseguire una query booleana, incollare quanto segue:

```
host.keyword:www.example.com and response.keyword:200
```

Query di data e intervallo

È possibile utilizzare una query di data e intervallo per trovare una data prima o dopo la query.

- > indica una ricerca di una data successiva alla data specificata.
- < indica una ricerca di una data precedente alla data specificata.

```
@timestamp > "2020-12-14T09:35:33"
```

Query di campi nidificati

Se hai un documento con campi nidificati, devi specificare quali parti del documento desideri recuperare. Di seguito è riportato un documento di esempio che contiene campi nidificati:

```
{"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"
    }
  ]
}
```

Per recuperare un campo specifico utilizzando DQL, incollare quanto segue:

```
NBA players: {player-name: Lebron James}
```

Per recuperare più oggetti dal documento nidificato, incollare quanto segue:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo}
```

Per eseguire una ricerca all'interno di un intervallo, incolla quanto segue:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo and < 30}
```

Se il documento ha un oggetto nidificato all'interno di un altro oggetto, è comunque possibile recuperare i dati specificando tutti i livelli. A tale scopo, copia quanto segue:

```
Top-Power-forwards.NBA players: {player-name:Lebron James}
```

Pacchetti personalizzati per Amazon OpenSearch Service

Amazon OpenSearch Service ti consente di caricare file di dizionario personalizzati, come parole chiave e sinonimi, e fornisce anche diversi plugin opzionali preconfezionati che puoi associare al tuo dominio. Il termine generico per entrambi questi tipi di file è pacchetti.

I file di dizionario migliorano i risultati della ricerca indicando di OpenSearch ignorare determinate parole ad alta frequenza o di trattare termini come «crema pasticcera surgelata», «gelato» e «gelato» come equivalenti. Possono anche migliorare lo stemming, come nel plugin di analisi del giapponese (kuromoji).

I plugin opzionali possono fornire funzionalità aggiuntive al tuo dominio. Ad esempio, puoi utilizzare il plug-in Amazon Personalize per ottenere risultati di ricerca personalizzati. I plugin opzionali utilizzano il tipo di `ZIP-PLUGIN` pacchetto. Per ulteriori informazioni sui plugin opzionali, consulta. the section called “Plug-in per versione motore”

Argomenti

- Requisiti di autorizzazioni per i pacchetti
- Caricamento di pacchetti in Amazon S3
- Importazione e associazione di pacchetti
- Utilizzo di pacchetti con OpenSearch
- Aggiornamento dei pacchetti
- Aggiornamenti manuali degli indici per i dizionari
- Dissociazione e rimozione dei pacchetti

Requisiti di autorizzazioni per i pacchetti

Gli utenti senza accesso come amministratore richiedono determinate azioni AWS Identity and Access Management (IAM) per gestire i pacchetti:

- `es:CreatePackage`- creare un pacchetto in una regione OpenSearch di servizio
- `es:DeletePackage`- eliminare un pacchetto da un'area OpenSearch di servizio
- `es:AssociatePackage`: associazione di un pacchetto a un dominio
- `es:DissociatePackage`: dissociazione di un pacchetto da un dominio

Sono necessarie anche le autorizzazioni per il percorso del bucket Amazon S3 o l'oggetto in cui si trova il pacchetto personalizzato.

Concedere tutte le autorizzazioni all'interno di IAM, non nella policy di accesso al dominio. Per ulteriori informazioni, consultare the section called “Identity and Access Management”.

Caricamento di pacchetti in Amazon S3

Questa sezione spiega come caricare pacchetti di dizionari personalizzati, poiché i pacchetti di plug-in opzionali sono già preinstallati. Prima di poter associare un dizionario personalizzato al tuo dominio, devi caricarlo in un bucket Amazon S3. Per le istruzioni, consulta Caricamento di oggetti nella Guida per l'utente di Amazon Simple Storage Service. I plugin supportati non devono essere caricati.

Se il dizionario contiene informazioni sensibili, specifica la crittografia lato server con chiavi gestite da S3 al momento del caricamento. OpenSearch Il servizio non può accedere ai file su S3 che proteggi utilizzando una chiave. AWS KMS

Dopo aver caricato il file, prendere nota del suo percorso S3. Il formato del percorso è `s3://`*`bucket-name`*`/`*`file-path`*`/`*`file-name`*.

È possibile utilizzare il seguente file di sinonimi per scopi di test. Salvalo come `synonyms.txt`.

```
danish, croissant, pastry
ice cream, gelato, frozen custard
sneaker, tennis shoe, running shoe
basketball shoe, hightop
```

Alcuni dizionari, come i dizionari Hunspell, utilizzano più file e richiedono le proprie directory nel file system. Al momento, OpenSearch Service supporta solo dizionari a file singolo.

Importazione e associazione di pacchetti

La console è il modo più semplice per importare un dizionario personalizzato in Service. OpenSearch Quando importi un dizionario da Amazon S3, OpenSearch Service archivia la propria copia del pacchetto e la crittografa automaticamente utilizzando AES-256 con chiavi gestite dal servizio. OpenSearch

I plug-in opzionali sono già preinstallati in OpenSearch Service, quindi non è necessario caricarli personalmente, ma è necessario associare un plug-in a un dominio. I plugin disponibili sono elencati nella schermata Pacchetti della console.

Importa e associa un pacchetto a un dominio con AWS Management Console

1. Nella console di Amazon OpenSearch Service, scegli Pacchetti.

2. Scegli Importa pacchetto.
3. Assegna al dizionario personalizzato un nome descrittivo.
4. Fornisci il percorso S3 del file e quindi scegli Invia.
5. Tornare alla schermata Pacchetti .
6. Quando lo stato del pacchetto è disponibile, selezionarlo. I plugin opzionali saranno automaticamente disponibili.
7. Scegli Associa a un dominio.
8. Seleziona un dominio, quindi scegli Associate (Associa).
9. Nel pannello di navigazione, scegliere il dominio e passare alla scheda Pacchetti.
10. Se il pacchetto è un dizionario personalizzato, annota l'ID quando il pacchetto diventa Disponibile. Utilizza `analyzers/id` come percorso del file nelle richieste di OpenSearch.

In alternativa, utilizza gli AWS CLI SDK o l'API di configurazione per importare e associare i pacchetti. Per ulteriori informazioni, consulta AWS CLI Command Reference e Amazon OpenSearch Service API Reference.

Utilizzo di pacchetti con OpenSearch

Questa sezione spiega come utilizzare entrambi i tipi di pacchetti: dizionari personalizzati e plugin opzionali.

Usare dizionari personalizzati

Dopo aver associato un file a un dominio, è possibile utilizzarlo in parametri quali `synonyms_path`, `stopwords_path` e `user_dictionary` durante la creazione di tokenizer e filtri token. Il parametro esatto varia in base all'oggetto. Diversi oggetti supportano `synonyms_path` e `stopwords_path`, ma `user_dictionary` è esclusivo per il plugin kuromoji.

Per il plug-in IK (Chinese) Analysis, è possibile caricare un file di dizionario personalizzato come pacchetto personalizzato e associarlo a un dominio e il plug-in lo raccoglie automaticamente senza richiedere un parametro `user_dictionary`. Se il file è un file di sinonimi, usa il parametro `synonyms_path`.

Nel seguente esempio viene aggiunto un file di sinonimi a un nuovo indice:

```
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"
      }
    }
  }
}
```

Questa richiesta crea un analizzatore personalizzato per l'indice che utilizza il tokenizer standard e un filtro token sinonimo.

- I tokenizer scompongono i flussi di caratteri in token (in genere parole) in base ad alcune regole. L'esempio più semplice è il tokenizer di whitespace, che scompone i caratteri precedenti in un token ogni volta che incontra un carattere di whitespace. Un esempio più complesso è il tokenizer standard, che utilizza un insieme di regole grammaticali per lavorare in molte lingue.
- I filtri token aggiungono, modificano o eliminano token. Ad esempio, un filtro token sinonimo aggiunge token quando trova una parola nell'elenco dei sinonimi. Il filtro token di arresto rimuove i token quando trova una parola nell'elenco di parole stop.

Questa richiesta aggiunge anche un campo di testo (`description`) alla mappatura e indica di OpenSearch utilizzare il nuovo analizzatore come analizzatore di ricerca. Si può vedere che come analizzatore di indice è utilizzato ancora l'analizzatore standard.

Infine, prendere nota della riga `"updateable": true` nel filtro token. Questo campo si applica solo agli analizzatori di ricerca non agli analizzatori di indice, ed è critico se in seguito si desidera aggiornare l'analizzatore di ricerca automaticamente.

A scopo di test, aggiungere alcuni documenti all'indice:

```
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" }
```

Quindi cercarli usando un sinonimo:

```
GET my-index/_search
{
  "query": {
    "match": {
      "description": "gelato"
    }
  }
}
```

In questo caso, OpenSearch restituisce la seguente risposta:

```
{
  "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**
>
> I file di dizionario utilizzano lo spazio heap Java proporzionale alle loro dimensioni. Ad esempio, un file di dizionario a 2 GiB potrebbe consumare su un nodo 2 GiB di spazio heap. Se si utilizzano file di grandi dimensioni, assicurarsi che i nodi dispongano di spazio heap sufficiente per contenerli. Monitorare il parametro `JVMMemoryPressure` e dimensionare il cluster in base alle esigenze.

Utilizzo di plugin opzionali

OpenSearch Il servizio consente di associare OpenSearch plug-in opzionali preinstallati da utilizzare al dominio. Un pacchetto di plug-in opzionale è compatibile con una OpenSearch versione specifica e può essere associato solo a domini con quella versione. L'elenco dei pacchetti disponibili per il tuo dominio include tutti i plugin supportati compatibili con la versione del tuo dominio. Dopo aver associato un plug-in a un dominio, inizia un processo di installazione sul dominio. Quindi, puoi fare riferimento e utilizzare il plug-in quando effettui richieste al OpenSearch Servizio.

L'associazione e la dissociazione di un plug-in richiedono una distribuzione blu/verde. Per ulteriori informazioni, consulta the section called “Modifiche che di solito causano implementazioni blu/verde”.

I plugin opzionali includono analizzatori linguistici e risultati di ricerca personalizzati. Ad esempio, il plug-in Amazon Personalize Search Ranking utilizza l'apprendimento automatico per personalizzare i risultati di ricerca per i tuoi clienti. Per ulteriori informazioni su questo plugin, consulta Personalizzazione dei risultati di ricerca da. OpenSearch Per un elenco di tutti i plugin supportati, consulta. the section called “Plug-in per versione motore”

Plugin Sudachi

Per il plugin Sudachi, quando riassoci un file di dizionario, questo non si riflette immediatamente sul dominio. Il dizionario si aggiorna quando viene eseguita la successiva distribuzione blu/verde sul dominio come parte di una modifica della configurazione o di un altro aggiornamento. In alternativa, puoi creare un nuovo pacchetto con i dati aggiornati, creare un nuovo indice utilizzando questo nuovo pacchetto, reindicizzare l'indice esistente nel nuovo indice e quindi eliminare il vecchio indice. Se preferisci utilizzare l'approccio di reindicizzazione, utilizza un alias di indice in modo da evitare interruzioni del traffico.

Inoltre, il plugin Sudachi supporta solo dizionari binari Sudachi, che puoi caricare con l'operazione API. CreatePackage Per informazioni sul dizionario di sistema predefinito e sul processo di compilazione dei dizionari utente, consulta la documentazione Sudachi.

L'esempio seguente mostra come utilizzare i dizionari di sistema e utente con il tokenizer Sudachi. È necessario caricare questi dizionari come pacchetti personalizzati con tipo `TXT-DICTIONARY` e fornire i relativi ID dei pacchetti nelle impostazioni aggiuntive.

```
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"
          }
```

```
        }
      }
    }
  }
}
```

Aggiornamento dei pacchetti

Questa sezione spiega solo come aggiornare un pacchetto di dizionario personalizzato, poiché i pacchetti di plugin opzionali sono già aggiornati automaticamente. Il caricamento di una nuova versione di un dizionario su Amazon S3 non aggiorna automaticamente il pacchetto su Amazon OpenSearch Service. OpenSearch Il servizio archivia la propria copia del file, quindi se carichi una nuova versione su S3, devi aggiornarla manualmente.

Ciascuno dei domini associati archivia anche la propria copia del file. Per mantenere prevedibile il comportamento di ricerca, i domini continueranno a utilizzare la versione corrente del pacchetto fino a quando non vengono aggiornati esplicitamente. Per aggiornare un pacchetto personalizzato, modifica il file in Amazon S3 Control, aggiorna il pacchetto in OpenSearch Service, quindi applica l'aggiornamento.

Aggiorna un pacchetto con AWS Management Console

1. Nella console OpenSearch di servizio, scegli Pacchetti.
2. Scegli un pacchetto, quindi seleziona Aggiorna.
3. Fornire il percorso S3 del file e quindi scegliere Aggiorna pacchetto.
4. Tornare alla schermata Pacchetti .
5. Quando lo stato del pacchetto è Disponibile, selezionarlo. Scegliere uno o più domini associati, selezionare Applica aggiornamento e confermare. Attendere che lo stato dell'associazione cambi in Attivo.
6. I passaggi successivi variano a seconda di come sono stati configurati gli indici:

   - Se il tuo dominio è in esecuzione OpenSearch con Elasticsearch 7.8 o versione successiva e utilizza solo analizzatori di ricerca con il campo aggiornabile impostato su true, non devi intraprendere ulteriori azioni. OpenSearch Il servizio aggiorna automaticamente gli indici utilizzando l'API _plugins/_refresh_search_analyzers.
   - Se il tuo dominio esegue Elasticsearch 7.7 o versioni precedenti, utilizza analizzatori di indici o non utilizza il campo, vedi. `updateable` the section called “Aggiornamenti manuali degli indici per i dizionari”

Sebbene la console sia il metodo più semplice, puoi anche utilizzare gli SDK o l'API AWS CLI di configurazione per aggiornare i pacchetti di servizi. OpenSearch Per ulteriori informazioni, consulta AWS CLI Command Reference e Amazon OpenSearch Service API Reference.

Aggiorna un pacchetto con l' AWS SDK

Invece di aggiornare manualmente un pacchetto nella console, per automatizzare il processo di aggiornamento è possibile utilizzare gli SDK. Il seguente script Python di esempio carica un nuovo file di pacchetto su Amazon S3, aggiorna il pacchetto in OpenSearch Service e applica il nuovo pacchetto al dominio specificato. Dopo aver verificato l'avvenuto aggiornamento, esegue una chiamata di esempio per OpenSearch dimostrare che i nuovi sinonimi sono stati applicati.

È necessario fornire valori per `host`, `region`, `file_name`, `bucket_name`, `s3_key`, `package_id`, `domain_name` e `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**
>
> Se ricevi un errore «pacchetto non trovato» quando esegui lo script utilizzando il AWS CLI, probabilmente significa che Boto3 sta utilizzando la regione specificata in ~/.aws/config, che non è la regione in cui si trova il bucket S3. Esegui `aws configure` e specifica la regione corretta oppure aggiungi esplicitamente la regione al client:
>
> ```
> client = boto3.client('opensearch', region_name='us-east-1')
> ```

Aggiornamenti manuali degli indici per i dizionari

Gli aggiornamenti manuali degli indici si applicano solo ai dizionari personalizzati, non ai plugin opzionali. Per utilizzare un dizionario aggiornato, è necessario aggiornare manualmente gli indici se si soddisfa una delle seguenti condizioni:

- Il dominio esegue Elasticsearch 7.7 o versioni precedenti.
- I pacchetti personalizzati vengono utilizzati come analizzatori di indice.
- I pacchetti personalizzati vengono utilizzati come analizzatori di ricerca, ma non includono il campo aggiornabile.

Per aggiornare gli analizzatori con i file del nuovo pacchetto, sono disponibili due opzioni:

- Chiudi e apri gli indici da aggiornare:

```
POST my-index/_close
POST my-index/_open
```

- Reindicizzare gli indici. Innanzitutto, create un indice che utilizzi il file dei sinonimi aggiornato (o un file completamente nuovo). Nota che è supportato solo 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"
      }
    }
  }
}
```

Quindi reindicizzare il vecchio indice nel nuovo indice:

```
POST _reindex
{
  "source": {
    "index": "my-index"
  },
  "dest": {
```

```
    "index": "my-new-index"
  }
}
```

Se gli analizzatori di indice vengono aggiornati con una certa frequenza, utilizzare gli alias di indice per mantenere un percorso coerente per l'indice più recente:

```
POST _aliases
{
  "actions": [
    {
      "remove": {
        "index": "my-index",
        "alias": "latest-index"
      }
    },
    {
      "add": {
        "index": "my-new-index",
        "alias": "latest-index"
      }
    }
  ]
}
```

Se il vecchio indice non è necessario, eliminarlo.

```
DELETE my-index
```

Dissociazione e rimozione dei pacchetti

La dissociazione di un pacchetto, che si tratti di un dizionario personalizzato o di un plug-in opzionale, da un dominio significa che non è più possibile utilizzare quel pacchetto quando si creano nuovi indici. Dopo la dissociazione di un pacchetto, gli indici esistenti che lo utilizzavano non possono più utilizzarlo. È necessario rimuovere il pacchetto da qualsiasi indice prima di poterlo dissociare, altrimenti la dissociazione fallisce.

La console è il modo più semplice per dissociare un pacchetto da un dominio e rimuoverlo dal servizio. OpenSearch La rimozione di un pacchetto dal OpenSearch servizio non lo rimuove dalla sua posizione originale su Amazon S3.

Dissocia un pacchetto da un dominio con AWS Management Console

1. Andare all'indirizzo https://aws.amazon.com e quindi scegliere Sign In to the Console (Accedi alla console).
2. In Analytics, scegli Amazon OpenSearch Service.
3. Nel riquadro di navigazione scegliere il dominio e quindi la scheda Packages (Pacchetti).
4. Scegliere un pacchetto, selezionare Operazioni, quindi scegliere Dissocia. Conferma la tua scelta.
5. Attendi che il pacchetto scompaia dall'elenco. Potrebbe essere necessario aggiornare il browser.
6. Se desideri utilizzare il pacchetto con altri domini, interrompi questa operazione a questo punto. Per continuare a rimuovere il pacchetto (se si tratta di un dizionario personalizzato), scegli Pacchetti nel pannello di navigazione.
7. Seleziona il pacchetto e scegli Elimina.

In alternativa, usa gli SDK o l' AWS CLI API di configurazione per dissociare e rimuovere i pacchetti. Per ulteriori informazioni, consulta AWS CLI Command Reference e Amazon OpenSearch Service API Reference.

Interrogazione dei dati OpenSearch di Amazon Service con SQL

Puoi usare SQL per interrogare il tuo Amazon OpenSearch Service, anziché usare la OpenSearch query DSL basata su JSON. Le query con SQL sono utili se si ha già familiarità con SQL o si desidera integrare il dominio con un'applicazione che utilizza SQL. Il supporto SQL è disponibile sui domini che eseguono Elasticsearch 6.5 OpenSearch o versioni successive.

> **Note**
>
> Questa documentazione descrive la compatibilità delle versioni tra OpenSearch Service e varie versioni del plug-in SQL, nonché il driver JDBC e ODBC. Consulta la OpenSearchdocumentazione open source per informazioni sulla sintassi di query, funzioni, query di metadati e funzioni aggregate di base e complesse.

Usa la tabella seguente per trovare la versione del plugin SQL supportata da ciascuna versione e da Elasticsearch. OpenSearch

OpenSearch

OpenSearch versione	Versione del plug-in SQL	Caratteristiche da tenere in considerazione
2.13.0	2.13.0.0	
2.11.0	211,0,0	Aggiunge il supporto per il linguaggio e le query PPL
2.9.0	2.9.0.0	Aggiungi il connettore Spark e supporta le funzioni tabellari e PromQL
2.7.0	2.7.0.0	Aggiungi API `datasource`
2.5.0	2.5.0.0	
2.3.0	2,30,0	Aggiungi funzioni di datetime `maketime` e `makedate`
1.3.0	1,30.0	Supporta la dimensione limite predefinita della query e la clausola IN per eseguire la selezione all'interno di un elenco di valori
1.2.0	1,20.0	Aggiungi un nuovo protocollo per il formato della risposta di visualizzazione
1.1.0	1.1.0.0	Supporto per la funzione di corrispondenza come filtro in SQL e PPL
1.0.0	1.0.0.0	Supporto per l'interrogazione di un flusso dei dati

Open Distro per Elasticsearch

Versione di Elasticsearch	Versione del plug-in SQL	Caratteristiche da tenere in considerazione
7,10	1,13,0	NULL FIRST e LAST per le funzioni finestra, la funzione CAST(), i comandi SHOW e DESCRIBE

Versione di Elasticsearch	Versione del plug-in SQL	Caratteristiche da tenere in considerazione
7.9	1.11.0	Aggiunta di ulteriori funzioni di data/ora, parola chiave ORDER BY
7.8	1.9.0	
7.7	18.0	
7.3	1.3.0	Operatori multipli di stringhe e numeri
7.1	1.1.0	

Chiamata di esempio

Per eseguire query sui dati con SQL, inviare le richieste HTTP a `_sql` utilizzando il seguente formato:

```
POST domain-endpoint/_plugins/_sql
{
  "query": "SELECT * FROM my-index LIMIT 50"
}
```

> **Note**
>
> Se il tuo dominio utilizza Elasticsearch anziché Elasticsearch OpenSearch, il formato è. `_opendistro/_sql`

Note e differenze

Le chiamate a `_plugins/_sql` includono i nomi degli indici nel corpo della richiesta e quindi hanno le stesse considerazioni delle policy di accesso delle operazioni bulk, mget e msearch. Come sempre, seguire il principio del privilegio minimo quando si concedono autorizzazioni alle operazioni API.

Per le considerazioni sulla sicurezza relativa all'utilizzo di SQL con il controllo granulare degli accessi, consultare the section called “Controllo granulare degli accessi”.

Il plugin OpenSearch SQL include molte impostazioni regolabili. In OpenSearch Service, utilizzate il `_cluster/settings` percorso, non il percorso delle impostazioni del plugin path (`_plugins/_query/settings`):

```
PUT _cluster/settings
{
  "transient" : {
    "plugins.sql.enabled" : true
  }
}
```

Per i domini Elasticsearch legacy, sostituisci `plugins` con `opendistro`:

```
PUT _cluster/settings
{
  "transient" : {
    "opendistro.sql.enabled" : true
  }
}
```

SQL Workbench

SQL Workbench è un'interfaccia utente di OpenSearch Dashboards che consente di eseguire query SQL su richiesta, tradurre SQL nel suo equivalente REST e visualizzare e salvare i risultati come testo, JSON, JDBC o CSV. Per ulteriori informazioni, consultare Query Workbench.

SQL CLI

SQL CLI è un'applicazione Python autonoma che è possibile avviare con il comando `opensearchsql`. Per la procedura di installazione, configurazione e utilizzo, consulta SQL CLI.

Driver JDBC

Il driver Java Database Connectivity (JDBC) consente di integrare i domini di OpenSearch servizio con le applicazioni di business intelligence (BI) preferite. Per scaricare il driver, fai clic qui. Per ulteriori informazioni, consulta il repository. GitHub

La tabella seguente riepiloga la compatibilità delle versioni per il driver.

OpenSearch

OpenSearch versione	Versione driver JDBC
2.13	1.1.0.1
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	1.1.0.1

Open Distro per Elasticsearch

Versione di Elasticsearch	Versione driver JDBC
7,10	1,13,0
7.9	1.11.0
7.8	1.9.0
7.7	18.0
7.4	1.4.0
7.1	1.0.0
6.8	0.9.0

Versione di Elasticsearch	Versione driver JDBC
6.7	0.9.0
6,5	0.9.0

Driver ODBC

Il driver Open Database Connectivity (ODBC) è un driver ODBC di sola lettura per Windows e macOS che consente di collegare applicazioni di business intelligence e visualizzazione dei dati come Microsoft Excel al plug-in SQL.

È possibile scaricare un file di driver funzionante di esempio nella pagina degli artefatti. OpenSearch Per informazioni sull'installazione del driver, consulta il repository SQL su. GitHub

Ricerca K-Nearest Neighbor (k-NN) su Amazon Service OpenSearch

Acronimo dell'algoritmo k-Nearest Neighbors associato, k-NN for OpenSearch Amazon Service consente di cercare punti in uno spazio vettoriale e trovare i «vicini più vicini» per tali punti in base alla distanza euclidea o alla somiglianza del coseno. Nei casi d'uso sono inclusi suggerimenti (ad esempio, una funzionalità "altri brani che potrebbero piacerti" in un'applicazione musicale), il riconoscimento delle immagini e il rilevamento delle frodi.

> **Note**
>
> Questa documentazione descrive la compatibilità delle versioni tra OpenSearch Service e varie versioni del plug-in k-NN, nonché le limitazioni relative all'utilizzo del plug-in con il servizio gestito. OpenSearch Per una documentazione completa del plugin k-NN, inclusi esempi semplici e complessi, riferimenti ai parametri e il riferimento API completo per il plug-in, consulta la documentazione open source. OpenSearch La documentazione open source copre anche l'ottimizzazione delle prestazioni e le impostazioni dei cluster specifiche di K-NN.

Utilizza le seguenti tabelle per trovare la versione del plugin k-NN in esecuzione sul tuo dominio Amazon OpenSearch Service. Ogni versione del plugin k-NN corrisponde a una OpenSearchversione di Elasticsearch.

OpenSearch

OpenSearch versione	Versione plug-in k-NN	Funzionalità significative
2.13	2,130,0	
2.11	211,0,0	Aggiunto il supporto per `ignore_unmapped` le interroga zioni in k-NN
2.9	2,9,0,0	Implementati vettori di byte k-NN e filtraggio efficiente con il motore Faiss
2.7	2.7.0.0	
2.5	2,5,0,0	Esteso SystemIndexPlugin per l'indice del sistema modello K-NN, aggiunte estensioni di file specifiche per Lucene al core HybridFS
2.3	2.3.0.0	
1.3	1,30.0	
1.2	1,20.0	Aggiunto il supporto per la biblioteca Faiss
1.1	1.1.0.0	
1	1.0.0.0	Le REST API rinominate, pur supportando la compatibilità con le versioni precedenti, hanno rinominato lo spazio dei nomi da `opendistro` a `opensearch`

Elasticsearch

Versione di Elasticsearch	Versione plug-in k-NN	Caratteristiche da tenere in considerazione
7.1	1,30.0	Distanza Euclidea
7.4	1,40.0	

Versione di Elasticsearch	Versione plug-in k-NN	Caratteristiche da tenere in considerazione
7.7	1,80.0	Similitudine coseno
7.8	1,9,0,0	
7.9	1.11.0.0	API di riscaldamento, punteggio personalizzato
7,10	1,130,0	Distanza di marcia, distanza di norma L1, scripting painless

Nozioni di base su k-NN

Per utilizzare k-NN, è necessario creare un indice con l'impostazione `index.knn` e aggiungere uno o più campi del tipo di dati `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
      }
    }
  }
}
```

Il tipo di dati `knn_vector` supporta un singolo elenco di fino a 10.000 numeri in virgola mobile, con il numero di numeri in virgola mobile definito dal parametro `dimension` richiesto. Dopo aver creato l'indice, aggiungi alcuni dati.

```
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 }
```

Quindi puoi cercare i dati utilizzando il tipo di query `knn`.

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  }
}
```

In questo caso, `k` è il numero di neighbors che la query deve restituire, ma è necessario includere anche l'opzione `size`. In caso contrario, vengono ottenuti i risultati `k` per ogni partizione (e ogni segmento) anziché i risultati `k` per l'intera query. k-NN supporta un valore massimo di `k` pari a 10.000.

Se si combina la query `knn` con altre clausole, è possibile che vengano restituiti meno risultati `k`. In questo esempio, la clausola `post_filter` riduce il numero di risultati da 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
      }
    }
  }
}
```

Se devi gestire un grande volume di query mantenendo prestazioni ottimali, puoi utilizzare l'`_msearch`API per creare una ricerca di massa con JSON e inviare una singola richiesta per eseguire più ricerche:

```
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 }} } }
```

Il video seguente mostra come configurare ricerche vettoriali di massa per le query K-NN.

Differenze, regolazione e limitazioni di k-NN

OpenSearch consente di modificare tutte le impostazioni k-NN utilizzando l'API. `_cluster/settings` In OpenSearch Service, puoi modificare tutte le impostazioni tranne `knn.memory.circuit_breaker.enabled` e`knn.circuit_breaker.triggered`. Le statistiche k-NN sono incluse come metriche di Amazon CloudWatch .

In particolare, confronta la `KNNGraphMemoryUsage` metrica su ciascun nodo di dati con la `knn.memory.circuit_breaker.limit` statistica e la RAM disponibile per il tipo di istanza. OpenSearch Il servizio utilizza metà della RAM di un'istanza per l'heap Java (fino a una dimensione dell'heap di 32 GiB). Per impostazione predefinita, k-NN utilizza fino al 50% della metà rimanente, quindi un tipo di istanza con 32 GiB di RAM può ospitare 8 GiB di grafici (32 * 0,5 * 0,5). Le prestazioni possono risentirne se l'utilizzo della memoria grafica supera questo valore.

Non è possibile migrare un indice k-NN verso una conservazione a freddo se l'indice UltraWarmutilizza k-NN () approssimativo. `"index.knn": true` Se `index.knn` è impostato su `false` (k-NN preciso), è comunque possibile spostare l'indice su altri livelli di archiviazione.

Ricerca tra cluster in Amazon Service OpenSearch

La ricerca tra cluster in Amazon OpenSearch Service ti consente di eseguire query e aggregazioni su più domini connessi. Spesso ha più senso utilizzare più domini più piccoli invece di un singolo dominio di grandi dimensioni, soprattutto quando si eseguono diversi tipi di carichi di lavoro.

I domini specifici del carico di lavoro consentono di completare le seguenti attività:

- Ottimizzare ogni dominio scegliendo i tipi di istanza per carichi di lavoro specifici.
- Stabilire i limiti di isolamento del guasto tra i carichi di lavoro. Ciò significa che se uno dei carichi di lavoro genera errori, il guasto è contenuto all'interno di quel dominio specifico e non influisce sugli altri carichi di lavoro.
- Scalabilità più semplice tra domini.

La ricerca tra cluster supporta OpenSearch le dashboard, quindi puoi creare visualizzazioni e dashboard in tutti i tuoi domini. Paghi le tariffe standard per il trasferimento AWS dei dati per i risultati di ricerca trasferiti tra domini.

> **Note**
>
> L'open source dispone OpenSearch anche di documentazione per la ricerca tra cluster. La configurazione differisce notevolmente per i cluster open source rispetto ai domini Amazon OpenSearch Service gestiti. In particolare, in OpenSearch Service, si configurano le connessioni tra cluster utilizzando cURL AWS Management Console anziché tramite cURL. Inoltre, il servizio gestito utilizza AWS Identity and Access Management (IAM) per l'autenticazione tra cluster oltre al controllo granulare degli accessi. Pertanto, consigliamo di

utilizzare questa documentazione, anziché la documentazione open source, per configurare la OpenSearch ricerca tra cluster per i domini.

Argomenti

Limitazioni

La ricerca tra cluster presenta diverse limitazioni importanti:

- Non puoi connettere un dominio Elasticsearch a un dominio. OpenSearch
- Non puoi connetterti a cluster /Elasticsearch OpenSearch autogestiti.
- Per connettere domini tra regioni, entrambi i domini devono essere su Elasticsearch 7.10 o versione successiva oppure. OpenSearch
- Un dominio può avere un massimo di 20 connessioni in uscita. Analogamente, un dominio può avere un massimo di 20 connessioni in ingresso. In altre parole, un dominio può connettersi a un massimo di 20 altri domini.
- Il dominio di origine deve avere la stessa versione o una versione successiva del dominio di destinazione. Se configuri una connessione bidirezionale tra due domini e desideri aggiornarne uno o entrambi, devi prima eliminare una delle connessioni.
- Non è possibile utilizzare dizionari personalizzati o SQL con la ricerca tra cluster.
- Non puoi utilizzare AWS CloudFormation per connettere domini.
- Non è possibile utilizzare la ricerca tra cluster su istanze M3 o istanze espandibili (T2 e T3).

Prerequisiti di ricerca tra cluster

Prima di configurare la ricerca tra cluster, assicurarsi che i domini soddisfino i seguenti requisiti:

- Due OpenSearch domini o domini Elasticsearch nella versione 6.7 o successiva
- Controllo granulare degli accessi abilitato
- Nessuna crittografia abilitata ode-to-node

Prezzi della funzionalità di ricerca tra cluster

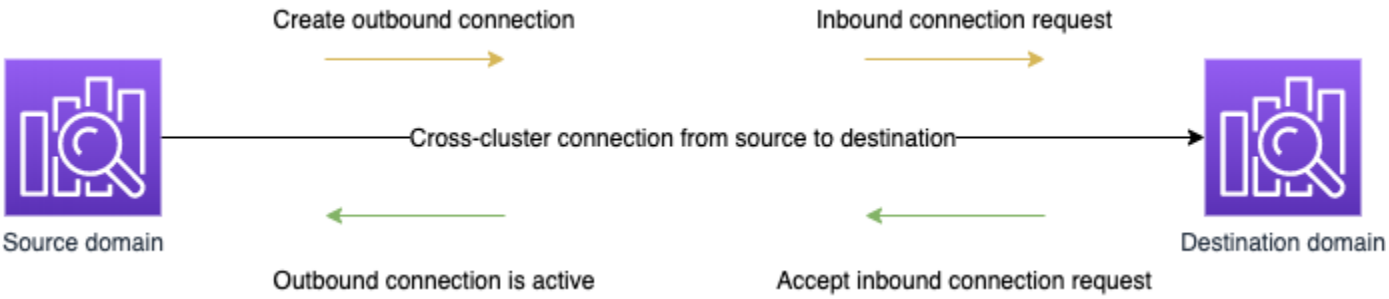
Non è previsto alcun costo aggiuntivo per la ricerca tra domini.

Configurazione di una connessione

Il dominio "di origine" si riferisce al dominio da cui proviene una richiesta di ricerca tra cluster. In altre parole, il dominio di origine è quello a cui si invia la richiesta iniziale di ricerca.

Il dominio "di destinazione" è il dominio sul quale il dominio di origine esegue le query.

Una connessione tra cluster è unidirezionale dall'origine al dominio di destinazione. Ciò significa che il dominio di destinazione non può eseguire query sul dominio di origine. Tuttavia, è possibile impostare un'altra connessione nella direzione opposta.



Il dominio di origine crea una connessione "in uscita" al dominio di destinazione. Il dominio di destinazione riceve una richiesta di connessione "in ingresso" dal dominio di origine.

Per impostare una connessione

1. Nel pannello di controllo del dominio scegliere un dominio e selezionare la scheda Connessioni.
2. Nella sezione Connessioni in uscita scegli Richiesta.
3. Per Alias di connessione, specifica un nome per la connessione.
4. Scegli se connetterti a un dominio nella tua Account AWS regione o in un altro account o regione.

- Per connetterti a un cluster nella tua regione Account AWS e nella tua regione, seleziona il dominio dal menu a discesa e scegli Richiedi.
- Per connetterti a un cluster in un'altra regione Account AWS o in un'altra regione, seleziona l'ARN del dominio remoto e scegli Richiesta. Per connettere domini tra regioni, entrambi i domini devono eseguire Elasticsearch versione 7.10 o successiva oppure. OpenSearch

5. Per ignorare i cluster non disponibili per le query sui cluster, seleziona Ignora non disponibile. Questa impostazione garantisce che le query tra cluster restituiscano risultati parziali nonostante gli errori su uno o più cluster remoti.
6. La ricerca tra cluster convalida innanzitutto la richiesta di connessione per assicurare che i prerequisiti siano soddisfatti. Se i domini risultano incompatibili, la richiesta di connessione entra nello stato `Validation failed`.
7. Dopo che la richiesta di connessione è stata convalidata correttamente, viene inviata al dominio di destinazione, dove deve essere approvata. Fino a quando non si avviene questa approvazione, la connessione rimane in uno stato `Pending acceptance`. Quando la richiesta di connessione viene accettata nel dominio di destinazione, lo stato cambia in `Active` e il dominio di destinazione diventa disponibile per le query.

   - La pagina del dominio mostra i dettagli generali dello stato del dominio e dello stato dell'istanza del dominio di destinazione. Solo i proprietari dei domini dispongono della flessibilità necessaria per creare, visualizzare, rimuovere e monitorare le connessioni da o verso i propri domini.

Dopo aver stabilito la connessione, tutto il traffico che passa tra i nodi dei domini connessi viene crittografato. Se si connette un dominio VPC a un dominio non VPC e il dominio non VPC è un endpoint pubblico in grado di ricevere traffico da Internet, il traffico tra cluster tra i domini è ancora crittografato e protetto.

Rimozione di una connessione

La rimozione di una connessione interrompe qualsiasi operazione tra cluster sui relativi indici.

1. Nel pannello di controllo del dominio, passa alla scheda Connessioni.
2. Selezionare le connessioni di dominio che si desidera rimuovere e scegliere Elimina, quindi confermare l'eliminazione.

È possibile eseguire queste operazioni sul dominio di origine o di destinazione per rimuovere la connessione. Dopo aver rimosso la connessione, questa sarà ancora visibile con lo stato `Deleted` per altri 15 giorni.

Non è possibile eliminare un dominio con connessioni tra cluster attive. Per eliminare un dominio, rimuovere innanzitutto tutte le connessioni in ingresso e in uscita da tale dominio. Questo per essere certi di considerare gli utenti del dominio tra cluster prima di eliminare il dominio.

Configurazione della sicurezza e spiegazione passo per passo di esempio

1. Si invia una richiesta di ricerca tra cluster al dominio di origine.
2. Il dominio di origine valuta tale richiesta in base alla policy di accesso al dominio. Poiché la ricerca tra cluster richiede un controllo di accesso granulare, è consigliabile una policy di accesso aperta nel dominio di origine.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

> **Note**
>
> Se includi indici remoti nel percorso, devi codificare in formato URL l'URI nell'ARN del dominio. Ad esempio, utilizzare `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst%3Aremote_index` anziché `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst:remote_index`.

Se si sceglie di utilizzare una policy di accesso restrittiva oltre al controllo di accesso granulare, la policy deve consentire l'accesso almeno a `es:ESHttpGet`.

```
{
  "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. Il controllo di accesso granulare nel dominio di origine valuta la richiesta:

   - La richiesta è firmata con credenziali di base IAM o HTTP valide?
   - In tal caso, l'utente dispone dell'autorizzazione per eseguire la ricerca e accedere ai dati?

   Se la richiesta ricerca solo i dati nel dominio di destinazione, ad esempio `dest-alias:dest-index/_search`, sono necessarie solo le autorizzazioni per il dominio di destinazione.

   Se la richiesta cerca dati su entrambi i domini, ad esempio `source-index,dest-alias:dest-index/_search`, sono necessarie le autorizzazioni per entrambi i domini.

   Nel controllo granulare degli accessi, gli utenti devono disporre dell'`indices:admin/shards/search_shards`autorizzazione oltre alle autorizzazioni standard `read` o `search` alle autorizzazioni per gli indici pertinenti.

4. Il dominio di origine invia la richiesta al dominio di destinazione. Il dominio di destinazione valuta la richiesta in base alla policy di accesso al dominio. È necessario includere l'autorizzazione `es:ESCrossClusterGet` per il dominio di destinazione:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

Assicurarsi che l'autorizzazione `es:ESCrossClusterGet` sia applicata per `/dst-domain` e non per `/dst-domain/*`.

Tuttavia, questo policy minima consente solo ricerche tra cluster. Per eseguire altre operazioni, ad esempio l'indicizzazione dei documenti e l'esecuzione di ricerche standard, sono necessarie ulteriori autorizzazioni. Si consiglia la seguente policy per il dominio di destinazione:

```
{
  "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**
>
> Per impostazione predefinita, tutte le richieste di ricerca intercluster tra domini vengono crittografate in transito come parte della crittografia. node-to-node

5. Il dominio di destinazione esegue la ricerca e restituisce i risultati al dominio di origine.
6. Il dominio di origine combina i propri risultati (se presenti) con i risultati del dominio di destinazione e li restituisce all'utente.
7. Consigliamo Postman per le richieste di test:

   - Nel dominio di destinazione, indicizzare un documento:

     ```
     POST https://dst-domain.us-east-1.es.amazonaws.com/books/_doc/1

     {
       "Dracula": "Bram Stoker"
     }
     ```

   - Per eseguire una query su questo indice dal dominio di origine, includere l'alias di connessione del dominio di destinazione all'interno della query.

     ```
     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"
           }
         }
       ]
     ```

```
}
```

È possibile trovare l'alias di connessione nella scheda Connessioni nel pannello di controllo del dominio.

- Se si imposta una connessione tra `domain-a -> domain-b` con l'alias di connessione `cluster_b` e `domain-a -> domain-c` con l'alias di connessione `cluster_c`, ricercare `domain-a`, `domain-b` e `domain-c` come segue:

```
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"
    }
  }
}
```

Risposta

```
{
  "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
        }
      }
    ]
  }
}
```

Se non hai scelto di ignorare i cluster non disponibili nella configurazione della connessione, tutti i cluster di destinazione che cerchi devono essere disponibili affinché la richiesta di ricerca venga eseguita correttamente. In caso contrario, l'intera richiesta avrà esito negativo: anche se uno dei domini non è disponibile non verrà restituito alcun risultato della ricerca.

OpenSearch Dashboard

È possibile visualizzare i dati di più domini connessi nello stesso modo di un singolo dominio, tranne per il fatto che è necessario accedere agli indici remoti utilizzando `connection-alias:index`. Quindi, il modello di indice deve corrispondere a `connection-alias:index`.

Imparare a classificarsi per Amazon OpenSearch Service

OpenSearch utilizza un framework di classificazione probabilistico chiamato BM-25 per calcolare i punteggi di pertinenza. Se una parola chiave distintiva appare più frequentemente in un documento, BM-25 assegna un punteggio di pertinenza più elevato a tale documento. Questo framework, tuttavia, non tiene conto del comportamento degli utenti come i dati click-through, che possono aumentare ulteriormente la rilevanza.

Learning to Rank è un plug-in OpenSearch open source che consente di utilizzare il machine learning e i dati comportamentali per ottimizzare la pertinenza dei documenti. Il plug-in utilizza modelli delle librerie XGBoost e Ranklib per assegnare un nuovo punteggio ai risultati della ricerca. Il plugin Elasticsearch LTR è stato inizialmente sviluppato da OpenSource Connections, con contributi significativi da Wikimedia Foundation, Snagajob Engineering, Bonsai e Yelp Engineering. La OpenSearch versione del plugin è derivata dal plugin Elasticsearch LTR.

Learning to Rank richiede Elasticsearch OpenSearch 7.7 o versione successiva. Per utilizzare il plug-in Learning to Rank, è necessario disporre delle autorizzazioni complete di amministratore. Per ulteriori informazioni, consultare the section called “Modifica dell'utente principale”.

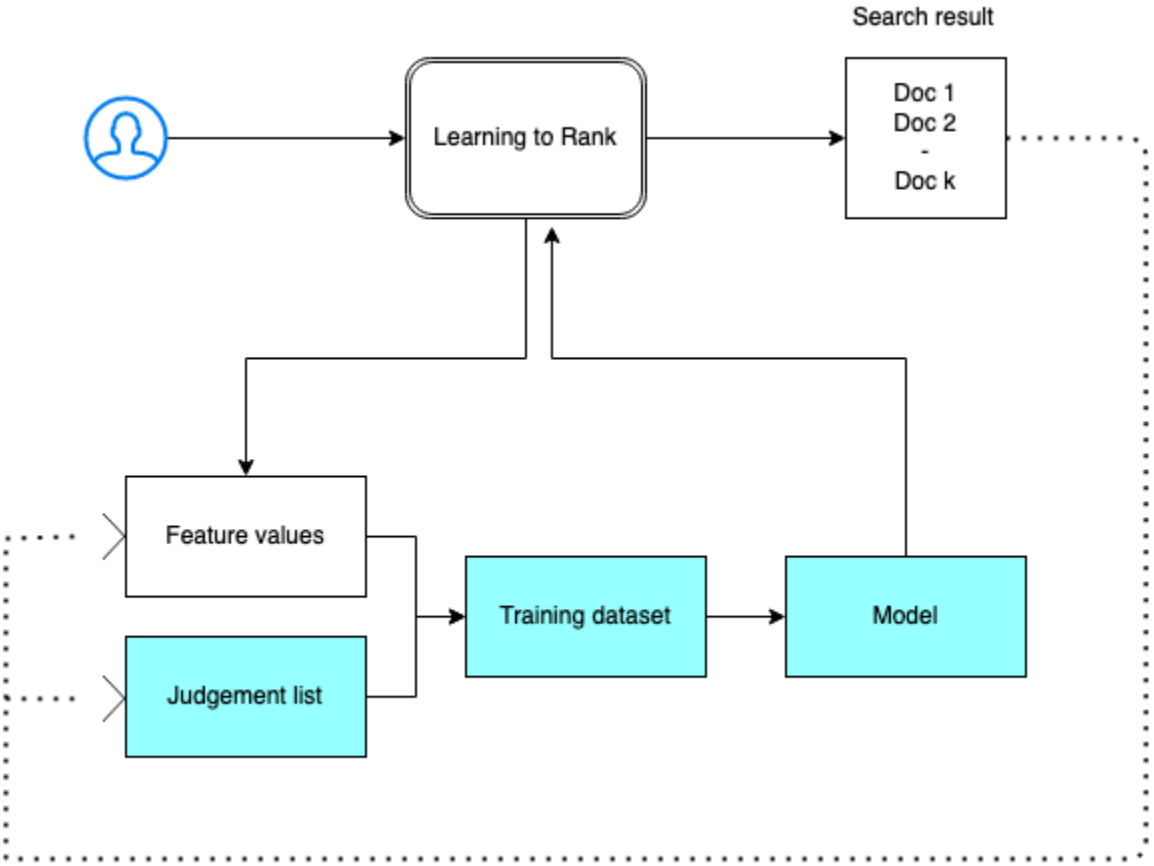
> **Note**
>
> Questa documentazione fornisce una panoramica generale del plugin Learning to Rank e ti aiuta a iniziare a usarlo. La documentazione completa, comprese le descrizioni delle fasi e dell'API, è disponibile nella documentazione di Learning to Rank.

Argomenti

- Nozioni di base su Learning to Rank
- API Learning to Rank

Nozioni di base su Learning to Rank

Devi fornire un elenco di giudizi, preparare un set di dati di addestramento e addestrare il modello al di fuori di Amazon OpenSearch Service. Le parti in blu si trovano al di fuori del OpenSearch servizio:



Fase 1: Inizializzazione del plug-in

Per inizializzare il plugin Learning to Rank, invia la seguente richiesta al tuo dominio OpenSearch di servizio:

```
PUT _ltr
```

```
{
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : ".ltrstore"
}
```

Questo comando crea un indice `.ltrstore` nascosto che memorizza informazioni sui metadati, ad esempio set di funzioni e modelli.

Fase 2: Creazione di un elenco dei giudizi

> **Note**
>
> È necessario eseguire questo passaggio al di fuori del OpenSearch Servizio.

Un elenco di giudizi è una raccolta di esempi da cui apprende un modello di machine learning. L'elenco dei giudizi deve includere parole chiave importanti e un insieme di documenti classificati per ogni parola chiave.

In questo esempio, abbiamo un elenco di giudizi per un set di dati di film. Un grado pari a 4 indica una corrispondenza perfetta. Un grado pari a 0 indica la corrispondenza peggiore.

Grado	Parola chiave	ID documento	Nome del film
4	rambo	7555	Rambo
3	rambo	1370	Rambo III
3	rambo	1369	Rambo 2 - La vendetta
3	rambo	1368	La vendetta

Preparare l'elenco dei giudizi nel formato seguente:

```
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"
```

Per un esempio più completo di un elenco dei giudizi, consultare Giudizi di film.

È possibile creare questo elenco di giudizi manualmente con l'aiuto di annotatori umani o dedurlo a livello di programmazione dai dati analitici.

Fase 3: Creazione di un set di funzionalità

Una funzionalità è un campo che corrisponde alla pertinenza di un documento, ad esempio `title`, `overview`, `popularity score`(numero di visualizzazioni) e così via.

Creare un set di funzionalità con un modello Mustache per ogni funzionalità. Per ulteriori informazioni sulle funzionalità, consultare Utilizzo delle funzionalità.

In questo esempio viene creato un set di funzionalità `movie_features` con i campi `title` e `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}}"
            }
          }
        }
      ]
    }
}
```

Se si esegue una query sull'indice `.ltrstore` originale, viene recuperato il set di funzionalità:

```
GET _ltr/_featureset
```

Fase 4: Registrazione dei valori delle funzionalità

I valori delle funzionalità sono i punteggi di pertinenza calcolati da BM-25 per ogni funzionalità.

Combinare il set di funzionalità e l'elenco dei giudizi per registrare i valori delle funzionalità. Per ulteriori informazioni sulle funzionalità di registrazione, consultare Punteggi della funzionalità di registrazione.

In questo esempio, `bool` recupera i documenti classificati con il filtro e quindi seleziona il set di funzionalità con la query `sltr`. La query `ltr_log` combina i documenti e le funzionalità in modo da registrare i valori delle funzionalità corrispondenti:

```
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"
      }
    }
  }
}
```

L'aspetto di una risposta di esempio è simile al seguente:

```
{
  "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"
        ]
      }
    ]
  }
}
```

Nell'esempio precedente, la prima funzionalità non ha un valore di funzionalità perché la parola chiave "rambo" non viene visualizzata nel campo del titolo del documento con un ID uguale a 1368. Questo è un valore di funzionalità mancante nei dati di addestramento.

Fase 5: Creazione di un set di dati di addestramento

> **Note**
>
> È necessario eseguire questa operazione al di fuori del OpenSearch Servizio.

Il passo successivo consiste nel combinare l'elenco dei giudizi e i valori delle funzionalità per creare un set di dati di addestramento. Se l'elenco dei giudizi originale ha la seguente struttura:

```
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
```

Convertirlo nel set di dati di addestramento finale, che assomiglia a questo:

```
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
```

È possibile eseguire questo passaggio manualmente o scrivere un programma per automatizzarlo.

Fase 6: Scelta di un algoritmo e costruzione del modello

> **Note**
>
> È necessario eseguire questo passaggio al di fuori del OpenSearch Servizio.

Con il set di dati di addestramento in atto, il passo successivo è quello di utilizzare le librerie XGBoost o Ranklib per costruire un modello. Le librerie XGBoost e Ranklib consentono di costruire modelli popolari come LambdaMART, Random Forests e così via.

Per i passaggi per utilizzare XGBoost e Ranklib per creare il modello, consulta rispettivamente XGBoost e la documentazione. RankLib Per utilizzare Amazon per SageMaker creare il modello XGBoost, consulta XGBoost Algorithm.

Fase 7: Implementazione del modello

Dopo aver creato il modello, implementarlo nel plug-in Learning to Rank. Per ulteriori informazioni sull'implementazione di un modello, consultare Caricamento di un modello addestrato.

In questo esempio viene creato un modello `my_ranklib_model` utilizzando la libreria 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>
"""
    }
  }
}
```

Per visualizzare il modello, inviare la seguente richiesta:

```
GET _ltr/_model/my_ranklib_model
```

Passaggio 8: Ricerca con Learning to Rank

Dopo aver implementato il modello, è possibile eseguire la ricerca.

Eseguire la query `sltr` con le funzionalità di cui si sta utilizzando e il nome del modello da eseguire:

```
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 Learning to Rank, "Rambo" viene visualizzato come primo risultato perché gli è stato assegnato il voto più alto nell'elenco dei giudizi:

```
{
  "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"
        }
      }
    ]
  }
}
```

Se esegui una ricerca senza utilizzare il plug-in Learning to Rank, OpenSearch restituisce risultati diversi:

```
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"
        }
      }
    ]
  }
}
```

In base a quanto si pensa che il modello stia funzionando, regolare l'elenco dei giudizi e le funzionalità. Ripetere quindi i passaggi da 2 a 8 per migliorare i risultati della classifica nel tempo.

API Learning to Rank

Utilizzare le operazioni di Learning to Rank per lavorare a livello di programmazione con set di funzionalità e modelli.

Creazione dell'archiviazione

Crea un indice `.ltrstore` nascosto che memorizza informazioni sui metadati, ad esempio set di funzionalità e modelli.

```
PUT _ltr
```

Eliminazione dell'archiviazione

Elimina l'indice `.ltrstore` nascosto e reimposta il plug-in.

```
DELETE _ltr
```

Creazione di un set di funzionalità

Crea un set di funzionalità.

```
POST _ltr/_featureset/<name_of_features>
```

Eliminazione di un set di funzionalità

Elimina un set di funzionalità.

```
DELETE _ltr/_featureset/<name_of_feature_set>
```

Ottenimento di un set di funzionalità

Recupera un set di funzionalità.

```
GET _ltr/_featureset/<name_of_feature_set>
```

Creazione del modello

Crea un modello.

```
POST _ltr/_featureset/<name_of_feature_set>/_createmodel
```

Eliminazione di un modello

Elimina un modello.

```
DELETE _ltr/_model/<name_of_model>
```

Ottenimento del modello

Recupera un modello.

```
GET _ltr/_model/<name_of_model>
```

Ottenimento delle statistiche

Fornisce informazioni sul comportamento del plug-in.

```
GET _ltr/_stats
```

Puoi anche utilizzare i filtri per recuperare una singola statistica:

```
GET _ltr/_stats/<stat>
```

Inoltre, puoi limitare le informazioni a un singolo nodo del cluster:

```
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
    }
  }
}
```

Le statistiche sono fornite a due livelli, nodo e cluster, come specificato nelle tabelle seguenti:

Statistiche a livello di nodo

Nome campo	Descrizione
request_total_count	Conteggio totale delle richieste di classific azione.
request_error_count	Conteggio totale delle richieste non riuscite.
cache	Statistiche su tutte le cache (funzionalità, set di funzionalità, modelli). Una occorrenza della cache si verifica quando un utente esegue una query sul plug-in e il modello è già caricato in memoria.

Nome campo	Descrizione
cache.eviction_count	Numero di rimozioni della cache.
cache.hit_count	Numero di occorrenze della cache.
cache.miss_count	Numero di mancati riscontri nella cache. Un mancato riscontro nella cache si verifica quando un utente esegue una query sul plug-in e il modello non è ancora caricato in memoria.
cache.entry_count	Numero di voci nella cache.
cache.memory_usage_in_bytes	Memoria totale utilizzata in byte.
cache.cache_capacity_reached	Indica se viene raggiunto il limite della cache.

Statistiche a livello di cluster

Nome campo	Descrizione
archiviazioni	Indica dove vengono archiviati i set di funzionalità e i metadati del modello. (Il valore di default è “.ltrstore”. Altrimenti, viene aggiunto il prefisso “.ltrstore_” a un nome fornito dall'utente).
stores.status	Stato dell'indice.
stores.feature_sets	Numero di set di funzionalità.
stores.features_count	Numero di funzionalità.
stores.model_count	Numero di modelli.
status	Lo stato del plug-in in base allo stato degli indici del feature store (rosso, giallo o verde) e allo stato dell'interruttore automatico (aperto o chiuso).

Nome campo	Descrizione
cache.cache_capacity_reached	Indica se viene raggiunto il limite della cache.

Ottenimento delle statistiche della cache

Restituisce le statistiche sull'utilizzo della cache e della memoria.

```
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": {
                ...
            }
        }
    }
```

```
}
```

Cancellazione della cache

Cancella la cache del plug-in. Utilizzare questa opzione per aggiornare il modello.

```
POST _ltr/_clearcache
```

Ricerca asincrona in Amazon Service OpenSearch

Con la ricerca asincrona per Amazon OpenSearch Service puoi inviare una query di ricerca che viene eseguita in background, monitorare l'avanzamento della richiesta e recuperare i risultati in una fase successiva. È possibile recuperare i risultati parziali man mano che diventano disponibili prima del completamento della ricerca. Al termine della ricerca, salvare i risultati per il recupero e l'analisi successivi.

La ricerca asincrona richiede OpenSearch 1.0 o versione successiva oppure Elasticsearch 7.10 o versione successiva.

Questa documentazione fornisce una breve panoramica della ricerca asincrona. Descrive inoltre i limiti dell'uso della ricerca asincrona con un dominio Amazon OpenSearch Service gestito anziché con un cluster open source. OpenSearch Per la documentazione completa sulla ricerca asincrona, comprese le impostazioni disponibili, le autorizzazioni e un riferimento completo all'API, consulta Ricerca asincrona nella documentazione. OpenSearch

Chiamata di ricerca di esempio

Per eseguire una ricerca asincrona, inviare le richieste HTTP a `_plugins/_asynchronous_search` utilizzando il seguente formato:

```
POST opensearch-domain/_plugins/_asynchronous_search
```

> **Note**
>
> Se utilizzi Elasticsearch 7.10 invece di una versione, sostituiscilo con in tutte le richieste di ricerca asincrone OpenSearch . `_plugins` `_opendistro`

È possibile specificare le seguenti opzioni di ricerca asincrona:

Opzioni	Descrizione	Valore predefinito	Richiesto
`wait_for_completion_timeout`	Specifica il tempo che si prevede di attendere per i risultati. È possibile visualizzare tutti i risultati ottenuti in questo tempo, proprio come in una normale ricerca. È possibile eseguire il polling dei risultati rimanenti in base a un ID. Il valore massimo è 300 secondi.	1 secondo	No
`keep_on_completion`	Specifica se si desidera salvare i risultati nel cluster al termine della ricerca. È possibile esaminare i risultati memorizzati in un secondo momento.	`false`	No
`keep_alive`	Specifica il tempo in cui il risultato viene salvato nel cluster. Ad esempio, 2d significa che i risultati vengono memorizzati nel cluster per 48 ore. I risultati della ricerca salvati vengono eliminati dopo questo periodo o se la ricerca viene annullata. Si noti che questo tempo include il runtime della query. Se la query impiega più di questo periodo di tempo, il processo la annulla automaticamente.	12 ore	No

Richiesta di esempio

```
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**
>
> Sono supportati tutti i parametri della richiesta che si applicano a una query `_search` standard. Se utilizzi Elasticsearch 7.10 anziché una versione, sostituiscilo con. OpenSearch `_plugins` `_opendistro`

Autorizzazioni di ricerca asincrona

La ricerca asincrona supporta il controllo granulare degli accessi. Per informazioni dettagliate sull'uso delle autorizzazioni per adattarle al proprio caso d'uso, consultare Sicurezza asincrona della ricerca.

Per i domini con il controllo granulare degli accessi abilitato, sono necessarie le seguenti autorizzazioni minime per un ruolo:

```
# 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'
```

Per i domini con il controllo granulare degli accessi disabilitato, utilizzare l'accesso IAM e la chiave segreta per firmare tutte le richieste. È possibile accedere ai risultati con l'ID di ricerca asincrona.

Impostazioni della ricerca asincrona

OpenSearch consente di modificare tutte le impostazioni di ricerca asincrona disponibili utilizzando l'API. `_cluster/settings` In OpenSearch Service, puoi modificare solo le seguenti impostazioni:

- `plugins.asynchronous_search.node_concurrent_running_searches`
- `plugins.asynchronous_search.persist_search_failures`

Funzionalità di ricerca tra cluster

È possibile eseguire una ricerca asincrona tra cluster con le seguenti limitazioni minori:

- È possibile eseguire una ricerca asincrona solo nel dominio di origine.
- Non è possibile ridurre a icona i round trip di rete come parte di una query di ricerca tra cluster.

Se si imposta una connessione tra `domain-a -> domain-b` con l'alias di connessione `cluster_b` e `domain-a -> domain-c` con l'alias di connessione `cluster_c`, ricercare in maniera asincrona `domain-a`, `domain-b` e `domain-c` come segue:

```
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": []
    }
  }
}
```

Risposta

```
{
  "id" :
 "Fm9pYzJyVG91U19xb0hIQUJnMHJfRFEAAAAAAAknghQ1OWVBczNZQjVEa2dMYTBXaTdEagAAAAAAAAAB",
  "state" : "RUNNING",
  "start_time_in_millis" : 1609329314796,
  "expiration_time_in_millis" : 1609761314796
}
```

Per ulteriori informazioni, consulta the section called “Funzionalità di ricerca tra cluster”.

UltraWarm

Le ricerche asincrone con UltraWarm indici continuano a funzionare. Per ulteriori informazioni, consulta the section called “UltraWarm archiviazione”.

> **Note**
>
> È possibile monitorare le statistiche di ricerca asincrone in. CloudWatch Per un elenco completo di parametri, consulta the section called “Parametri di ricerca asincrona”.

Ricerca puntuale in Amazon OpenSearch Service

Point in Time (PIT) è un tipo di ricerca che consente di eseguire diverse query su un set di dati fisso nel tempo. In genere, quando si esegue la stessa query sullo stesso indice in momenti diversi, si ottengono risultati diversi perché i documenti vengono costantemente indicizzati, aggiornati ed eliminati. Con PIT, è possibile eseguire query su uno stato costante del set di dati.

L'uso principale della ricerca PIT è abbinarla alla `search_after` funzionalità. Questo è il metodo di impaginazione preferito OpenSearch, specialmente per l'impaginazione profonda, perché opera su un set di dati congelato nel tempo, non è vincolato a una query e supporta un'impaginazione coerente in avanti e indietro. È possibile utilizzare PIT con un dominio che esegue la versione 2.5. OpenSearch

> **Note**
>
> Questo argomento fornisce una panoramica di PIT e alcuni aspetti da considerare quando lo si utilizza su un dominio Amazon OpenSearch Service gestito anziché su un OpenSearch cluster autogestito. Per la documentazione completa di PIT, incluso un riferimento completo sulle API, consulta Point in Time nella OpenSearch documentazione open source.

Considerazioni

Considerate quanto segue quando configurate le vostre ricerche PIT:

- Se state eseguendo l'aggiornamento da un dominio che esegue la OpenSearch versione 2.3 e avete bisogno di un controllo preciso degli accessi sulle azioni PIT, dovete aggiungere manualmente tali azioni e ruoli.

- Non c'è resilienza per PIT. Il riavvio del nodo, la chiusura del nodo, le implementazioni blu/verdi e il riavvio del OpenSearch processo causano la perdita di tutti i dati PIT.
- Se uno shard si riposiziona durante l'implementazione blu/verde, solo i segmenti di dati in tempo reale vengono trasferiti al nuovo nodo. I segmenti di shard detenuti da PIT (sia esclusivamente che quelli condivisi con i dati in tempo reale) rimangono sul vecchio nodo.
- Le ricerche PIT attualmente non funzionano con la ricerca asincrona.

Crea un PIT

Per eseguire una query PIT, inviate le richieste HTTP a `_search/point_in_time` utilizzando il seguente formato:

```
POST opensearch-domain/my-index/_search/point_in_time?keep_alive=time
```

È possibile specificare le seguenti opzioni PIT:

Opzioni	Descrizione	Valore predefinito	Richiesto
`keep_alive`	Il periodo di tempo necessario per conservare il PIT. Ogni volta che si accede a un PIT con una richiesta di ricerca, la durata del PIT viene prolungata del periodo di tempo pari al `keep_alive` parametro. Questo parametro di interrogazione è obbligatorio quando si crea un PIT, ma facoltativo in una richiesta di ricerca.		Sì
`preference`	Una stringa che specifica il nodo o lo shard utilizzato per eseguire la ricerca.	Casuale	No
`routing`	Una stringa che specifica di indirizzare le richieste di ricerca a uno shard specifico.	Il documento `_id`	No
`expand_wildcards`	Una stringa che specifica il tipo di indice che può corrispondere al modello dei caratteri jolly. Supporta valori separati da virgole. I valori validi sono i seguenti.	`open`	No

Opzioni	Descrizione	Valore predefinito	Richiesto
	• `all`: corrisponde a qualsiasi indice o flusso di dati, compresi quelli nascosti. • `open`: abbina indici aperti e non nascosti o flussi di dati non nascosti. • `closed`: abbina indici chiusi e non nascosti o flussi di dati non nascosti. • `hidden`: abbina indici o flussi di dati nascosti. Deve essere combinato con aperto, chiuso o sia aperto che chiuso. • `none`: Non sono accettati modelli jolly.		
`allow_partial_pit_creation`	Un valore booleano che specifica se creare un PIT con errori parziali.	`true`	No

Risposta di esempio

```
{
    "pit_id":
 "o463QQEPbXktaW5kZXgtMDAwMDAxFnNOWU43ckt3U3IyaFVpbGE1UWEtMncAFjFyeXBsRGJmVFM2RTB6eVg1aVVqQncAA
    "_shards": {
        "total": 1,
        "successful": 1,
        "skipped": 0,
        "failed": 0
    },
    "creation_time": 1658146050064
}
```

Quando si crea un PIT, si riceve un ID PIT nella risposta. Questo è l'ID che utilizzate per eseguire ricerche con il PIT.

Autorizzazioni temporanee

PIT supporta un controllo granulare degli accessi. Se stai eseguendo l'aggiornamento a un dominio OpenSearch versione 2.5 e hai bisogno di un controllo degli accessi dettagliato, devi creare manualmente ruoli con le seguenti autorizzazioni:

```
# 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"
```

Per i domini con OpenSearch versione 2.5 e successive, puoi utilizzare il ruolo integrato. `point_in_time_full_access` Per ulteriori informazioni, consulta il modello di sicurezza nella OpenSearch documentazione.

Impostazioni PIT

OpenSearch consente di modificare tutte le impostazioni PIT disponibili utilizzando l'`_cluster/settings`API. In OpenSearch Service, al momento non è possibile modificare le impostazioni.

Funzionalità di ricerca tra cluster

È possibile creare PIT, cercare con ID PIT, elencare PIT ed eliminare PIT tra cluster con le seguenti limitazioni minori:

- È possibile elencare tutti ed eliminare tutti i PIT solo nel dominio di origine.
- Non è possibile ridurre a icona i round trip di rete come parte di una query di ricerca tra cluster.

Per ulteriori informazioni, consulta the section called “Funzionalità di ricerca tra cluster”.

UltraWarm

Le ricerche PIT con UltraWarm indici continuano a funzionare. Per ulteriori informazioni, consulta the section called “UltraWarm archiviazione”.

> **Note**
>
> È possibile monitorare le statistiche di ricerca PIT in. CloudWatch Per un elenco completo di parametri, consulta the section called “Metriche puntuali”.

Ricerca semantica in Amazon Service OpenSearch

A partire dalla OpenSearch versione 2.9, è possibile utilizzare la ricerca semantica per comprendere le query di ricerca e migliorare la pertinenza della ricerca. Puoi utilizzare la ricerca semantica in due modi: con la ricerca neurale e con la ricerca K-Nearest Neighbor (k-NN).

Con OpenSearch Service, puoi configurare connettori AI e servizi esterni. Servizi AWS Utilizzando la console, puoi anche creare un modello ML con un AWS CloudFormation modello. Per ulteriori informazioni, consulta the section called “CloudFormation integrazioni di modelli”.

Per la documentazione completa sulla ricerca semantica, inclusa una step-by-step guida all'uso della ricerca semantica, consulta Ricerca semantica nella documentazione open source. OpenSearch

Ricerca simultanea di segmenti in Amazon Service OpenSearch

A partire dalla OpenSearch versione 2.13, puoi utilizzare la ricerca simultanea per segmenti per aiutarti a cercare segmenti in parallelo durante la fase di interrogazione. Per la documentazione completa sulla ricerca simultanea di segmenti, consulta Ricerca simultanea di segmenti nella documentazione open source. OpenSearch Per informazioni sui CloudWatch parametri di Amazon relativi alla ricerca simultanea di segmenti, consulta Metriche e metriche delle istanze. UltraWarm

Esistono alcune limitazioni aggiuntive che si applicano quando utilizzi la ricerca di segmenti corrente con Amazon OpenSearch Service:

- Non puoi abilitare la ricerca simultanea di segmenti a livello di indice in OpenSearch Service.
- Per impostazione predefinita, OpenSearch Service utilizza un conteggio di 2 sezioni con il meccanismo del numero massimo di sezioni.

Utilizzo delle OpenSearch dashboard con Amazon Service OpenSearch

OpenSearch Dashboards è uno strumento di visualizzazione open source progettato per funzionare con. OpenSearch Amazon OpenSearch Service fornisce un'installazione di OpenSearch dashboard con ogni dominio OpenSearch di servizio. OpenSearch Le dashboard vengono eseguite sugli hot data node del dominio.

Puoi trovare un link a OpenSearch Dashboards nella dashboard del tuo dominio nella console di OpenSearch servizio. Per i domini in esecuzione OpenSearch, l'URL è. *domain-endpoint*`/_dashboards/` Per i domini che eseguono la versione precedente di Elasticsearch, l'URL è. *domain-endpoint*`/_plugin/kibana`

Le query che utilizzano questa installazione predefinita di OpenSearch Dashboards hanno un timeout di 300 secondi.

> **Note**
>
> Questa documentazione descrive le OpenSearch dashboard nel contesto di Amazon OpenSearch Service, inclusi i diversi modi per connettersi ad esso. Per una documentazione completa, tra cui una guida introduttiva, istruzioni per creare una dashboard, la gestione delle dashboard e Dashboards Query Language (DQL), consulta OpenSearch Dashboards nella documentazione open source. OpenSearch

Le seguenti sezioni trattano alcuni casi d'uso comuni delle dashboard: OpenSearch

- the section called “Controllo dell'accesso ai dashboard OpenSearch ”
- the section called “Configurazione delle OpenSearch dashboard per l'utilizzo di un server di mappe WMS”
- the section called “Connessione di un server Dashboards locale al servizio OpenSearch ”

Controllo dell'accesso ai dashboard OpenSearch

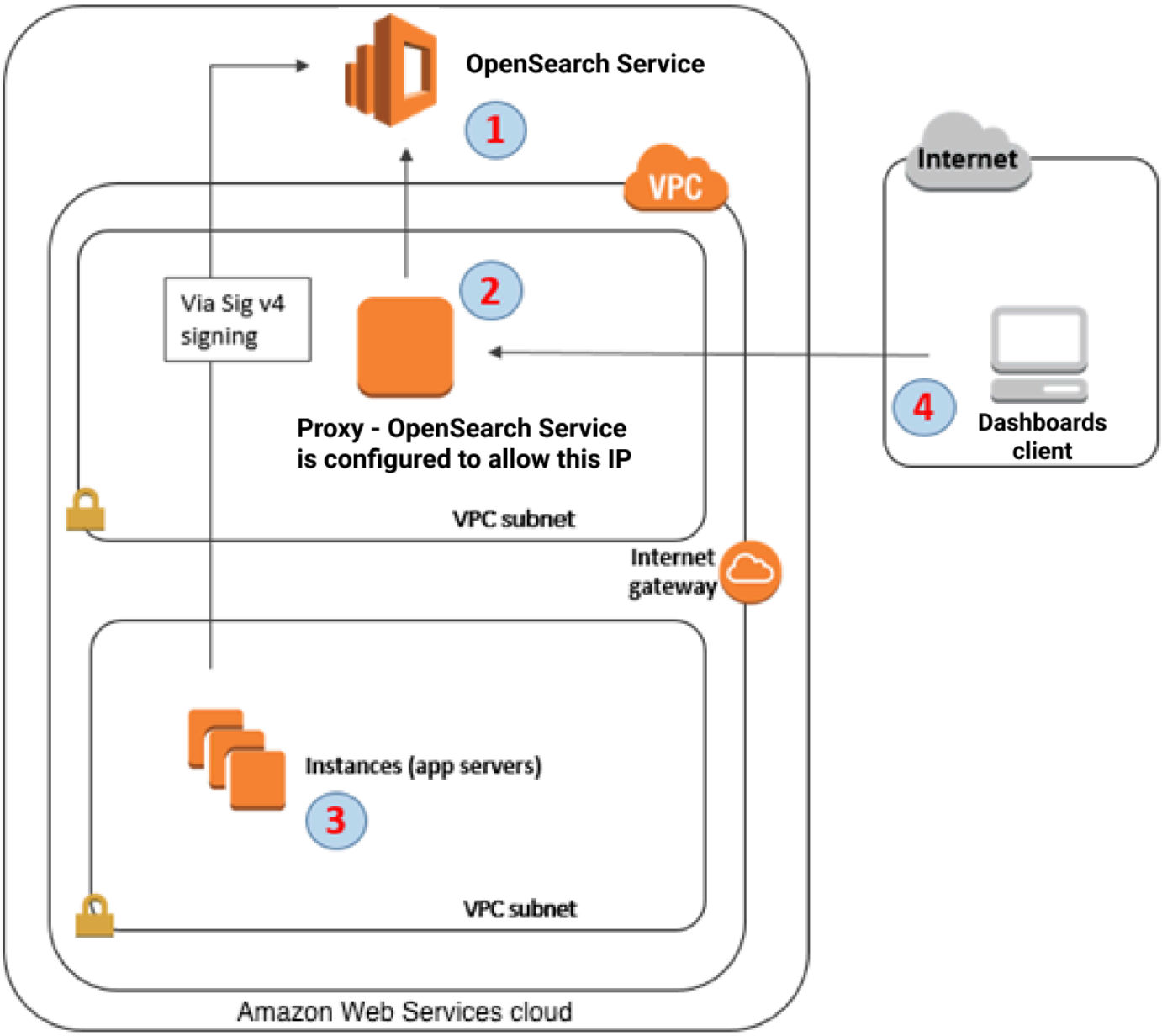
Dashboards non supporta nativamente utenti e ruoli IAM, ma OpenSearch Service offre diverse soluzioni per controllare l'accesso alle dashboard:

- Abilitare l'autenticazione SAML per Dashboards.
- Utilizzare il controllo granulare degli accessi con l'autenticazione di base HTTP.
- Configura l'autenticazione Cognito per Dashboards.
- Per i domini ad accesso pubblico, configurare una policy di accesso basata su IP, che utilizzi o meno un server proxy.
- Per i domini con accesso VPC, utilizzare una policy di accesso aperta, che utilizzi o meno un server proxy, e gruppi di sicurezza per controllare l'accesso. Per ulteriori informazioni, consulta the section called “Informazioni sulle policy d'accesso nei domini VPC”.

Utilizzo di un proxy per accedere al servizio da dashboard OpenSearch OpenSearch

> **Note**
>
> Questo processo è valido solo se il dominio usa l'accesso pubblico e non vuoi usare l'autenticazione Cognito. Per informazioni, consulta the section called “Controllo dell'accesso ai dashboard OpenSearch ”.

Poiché Dashboards è un' JavaScript applicazione, le richieste provengono dall'indirizzo IP dell'utente. Il controllo degli accessi basato su IP può essere poco pratico a causa del numero elevato di indirizzi IP che sarebbe necessario includere nella whitelist perché ogni utente possa accedere a Dashboards. Una soluzione alternativa consiste nel posizionare un server proxy tra OpenSearch Dashboards e Service. OpenSearch È quindi possibile aggiungere una policy d'accesso basata su IP che accetta le richieste provenienti da un solo indirizzo IP, quello del proxy. Il seguente diagramma mostra questa configurazione.



1. Questo è il tuo dominio di OpenSearch servizio. IAM offre accesso autorizzato al dominio. Un'ulteriore policy d'accesso basata su IP permette l'accesso al server proxy.
2. Questo è il server proxy, in esecuzione su un'istanza Amazon EC2.
3. Altre applicazioni possono utilizzare la procedura di firma Signature Version 4 per inviare richieste autenticate al OpenSearch Servizio.
4. OpenSearch I client Dashboards si connettono al dominio OpenSearch di servizio dell'utente tramite il proxy.

Per abilitare questo tipo di configurazione, è necessaria una policy basata su risorse che specifica i ruoli e gli indirizzi IP. Ecco una policy di esempio:

```
{
   "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":[
                  "203.0.113.0/24",
                  "2001:DB8:1234:5678::/64"
               ]
            }
         },
         "Resource":"arn:aws:es:us-west-2:111111111111:domain/my-domain/*"
      }
   ]
}
```

Ti consigliamo di configurare l'istanza EC2 che esegue il server proxy con un indirizzo IP elastico (EIP). In questo modo, puoi sostituire l'istanza quando necessario e collegarvi comunque lo stesso indirizzo IP pubblico. Per ulteriori informazioni, consulta Elastic IP Addresses nella Amazon EC2 User Guide.

Se si utilizza un server proxy e l'autenticazione Cognito, potrebbe essere necessario dover aggiungere impostazioni per Dashboards e Amazon Cognito in modo da evitare errori `redirect_mismatch`. Fai riferimento al file `nginx.conf` di esempio seguente:

```
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;
    }
}
```

Configurazione delle OpenSearch dashboard per l'utilizzo di un server di mappe WMS

L'installazione predefinita di OpenSearch Dashboards for OpenSearch Service include un servizio di mappe, ad eccezione dei domini nelle regioni India e Cina. Il servizio di mappe supporta fino a 10 livelli di zoom.

Indipendentemente dalla regione, è possibile configurare Dashboards per l'utilizzo di un server WMS (Web Map Service) diverso per le visualizzazioni delle mappe delle coordinate. Le visualizzazioni delle mappe regionali supportano solo il servizio mappe predefinito.

Per configurare Dashboards per l'uso di un server di mappe WMS:

1. Aprire Dashboards.
2. Scegliere Gestione stack.
3. Scegliere Advanced Settings (Impostazioni avanzate).
4. Individua visualization:tileMap:WMSdefaults.
5. Modifica `enabled` in `true` e `url` nell'URL di un server di mappe WMS valido:

   ```
   {
     "enabled": true,
     "url": "wms-server-url",
     "options": {
       "format": "image/png",
       "transparent": true
     }
   }
   ```
6. Seleziona Salvataggio delle modifiche.

Per applicare il nuovo valore di default alle visualizzazioni, potrebbe essere necessario ricaricare Dashboards. Se sono state salvate le visualizzazioni, scegli Opzioni dopo aver aperto la visualizzazione. Verifica che il server di mappe WMS sia abilitato e l'URL WMS contenga il server di mappe preferito, quindi scegli Applica modifiche.

> **Note**
>
> I servizi mappe spesso prevedono costi di licenza o limitazioni. Sei responsabile di tutti questi aspetti per qualsiasi server di mappe che specifichi. Potresti trovare utile provare i servizi mappe di U.S. Geological Survey.

Connessione di un server Dashboards locale al servizio OpenSearch

Se hai già investito molto tempo nella configurazione della tua istanza OpenSearch Dashboards, puoi utilizzarla al posto (o in aggiunta) all'istanza Dashboards predefinita fornita dal Servizio. OpenSearch La procedura seguente funziona per i domini che utilizzano il controllo granulare degli accessi con una policy di accesso aperto.

Per connettere un server OpenSearch Dashboards locale al servizio OpenSearch

1. Nel tuo dominio OpenSearch di servizio, crea un utente con le autorizzazioni appropriate:
   a. In Dashboards, passare a Sicurezza, Utenti interni, quindi scegliere Crea un utente interno.
   b. Fornire nome utente e password e scegliere Crea.
   c. Passare a Ruoli e selezionare un ruolo.
   d. Selezionare Utenti mappati e scegliere Gestisci mappatura.
   e. In Utenti, aggiungere il nome utente e scegliere Mappa.
2. Scarica e installa la versione appropriata del plug-in di OpenSearch sicurezza sull'installazione OSS di Dashboards autogestita.
3. Sul server Dashboards locale, apri il `config/opensearch_dashboards.yml` file e aggiungi l'endpoint di OpenSearch servizio con il nome utente e la password che hai creato in precedenza:

   ```
   opensearch.hosts: ['https://domain-endpoint']
   opensearch.username: 'username'
   opensearch.password: 'password'
   ```

   È possibile utilizzare il seguente file `opensearch_dashboards.yml` di esempio:

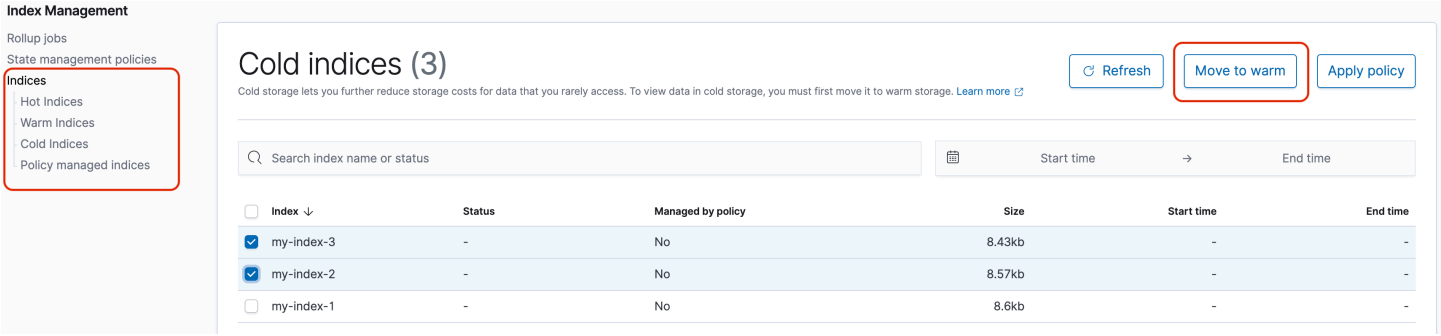
```
server.host: '0.0.0.0'

opensearch.hosts: ['https://domain-endpoint']

opensearchDashboards.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]
```

Per visualizzare gli indici OpenSearch del servizio, avvia il server Dashboards locale, vai su Dev Tools ed esegui il seguente comando:

```
GET _cat/indices
```

Gestione degli indici nelle dashboard OpenSearch

L'installazione di OpenSearch Dashboards sul dominio di OpenSearch servizio fornisce un'interfaccia utente utile per la gestione degli indici in diversi livelli di storage del dominio. Scegliete Gestione degli indici dal menu principale delle dashboard per visualizzare tutti gli indici in storage a caldo e a freddo UltraWarm, nonché gli indici gestiti dalle politiche di Index State Management (ISM). Utilizza la gestione degli indici per spostarli tra l'archiviazione a caldo e a freddo e per monitorare le migrazioni tra i tre livelli.



Tieni presente che non vedrai le opzioni degli indici caldi, caldi e freddi a meno che tu non abbia abilitato e/o abilitato la conservazione a freddo. UltraWarm

Funzionalità aggiuntive

L'installazione predefinita di OpenSearch Dashboards in ogni dominio OpenSearch di servizio presenta alcune funzionalità aggiuntive:

- Interfacce utente per i vari plugin OpenSearch
- Tenant
- Report

  Utilizzare il menu Creazione di report per generare report CSV on demand dalla pagina Individua e report PDF o PNG di pannelli di controllo o visualizzazioni. I report CSV hanno un limite di 10.000 righe.
- Grafici Gantt
- Notebook

Gestione degli indici in Amazon Service OpenSearch

Dopo aver aggiunto dati ad Amazon OpenSearch Service, spesso devi reindicizzarli, utilizzare gli alias dell'indice, spostare un indice su uno storage più conveniente o eliminarlo del tutto. Questo capitolo tratta UltraWarm lo storage, la conservazione a freddo e la gestione dello stato dell'indice. Per informazioni sulle API dell' OpenSearch indice, consulta la OpenSearch documentazione.

Argomenti

UltraWarm spazio di archiviazione per Amazon OpenSearch Service

UltraWarm offre un modo conveniente per archiviare grandi quantità di dati di sola lettura su Amazon Service. OpenSearch I nodi di dati standard utilizzano l'archiviazione "hot", che assume la forma di archivi di istanze o volumi Amazon EBS collegati a ciascun nodo. L'archiviazione a caldo offre le prestazioni più veloci possibili per l'indicizzazione e la ricerca di nuovi dati.

Invece dello storage collegato, UltraWarm i nodi utilizzano Amazon S3 e una sofisticata soluzione di caching per migliorare le prestazioni. Per gli indici su cui non scrivi attivamente, esegui query meno frequentemente e che non richiedono le stesse prestazioni, UltraWarm offre costi notevolmente inferiori per GiB di dati. Poiché gli indici caldi sono di sola lettura a meno che non vengano restituiti all'archiviazione a caldo, sono più adatti per dati immutabili, UltraWarm come i log.

In OpenSearch, gli indici caldi si comportano come qualsiasi altro indice. Puoi interrogarli utilizzando le stesse API o usarli per creare visualizzazioni nelle dashboard. OpenSearch

Argomenti

Prerequisiti

UltraWarm presenta alcuni importanti prerequisiti:

- UltraWarm richiede Elasticsearch 6.8 OpenSearch o versione successiva.
- Per utilizzare l'archiviazione warm, i domini devono disporre di nodi master dedicati.
- Quando si utilizza un dominio Multi-AZ con standby, il numero di nodi caldi deve essere un multiplo del numero di zone di disponibilità utilizzate.
- Se il dominio utilizza un tipo di istanza T2 o T3 per i nodi di dati, non è possibile utilizzare l'archiviazione a caldo.
- Se il tuo indice utilizza un k-NN approssimato (`"index.knn": true`), non puoi spostarlo in un'archiviazione ad accesso frequente.
- Se il dominio utilizza un controllo granulare degli accessi, gli utenti devono essere mappati al `ultrawarm_manager` ruolo nelle OpenSearch dashboard per effettuare chiamate API. UltraWarm

> **Note**
>
> Il `ultrawarm_manager` ruolo potrebbe non essere definito in alcuni domini di servizio preesistenti. OpenSearch Se il ruolo non è visualizzato in Dashboards, sarà necessario crearlo manualmente.

Configurazione delle autorizzazioni

Se si abilita UltraWarm su un dominio di OpenSearch servizio preesistente, il `ultrawarm_manager` ruolo potrebbe non essere definito nel dominio. Gli utenti senza privilegi di amministratore devono essere mappati a questo ruolo in modo da gestire gli indici a caldo sui domini che utilizzano il controllo granulare degli accessi. Per creare manualmente il ruolo `ultrawarm_manager`, procedere nel seguente modo:

1. In OpenSearch Dashboard, vai su Sicurezza e scegli Autorizzazioni.
2. Scegliere Crea gruppo di operazioni e configurare i seguenti gruppi:

Group name (Nome gruppo)	Autorizzazioni
`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. Scegliere Ruoli, quindi selezionare Crea ruolo.
4. Denominare il ruolo ultrawarm_manager.
5. Per Autorizzazioni cluster, selezionare `ultrawarm_cluster` e `cluster_monitor`.
6. Per Indice, digitare *.

7. Per Autorizzazioni indice, selezionare `ultrawarm_index_read`, `ultrawarm_index_write` e `indices_monitor`.
8. Scegli Crea.
9. Dopo aver creato il ruolo, associalo a qualsiasi utente o ruolo di backend che gestirà gli indici. UltraWarm

UltraWarm requisiti di archiviazione e considerazioni sulle prestazioni

Come illustrato in precedenzathe section called “Calcolo dei requisiti di archiviazione”, i dati nell'archiviazione a caldo comportano un sovraccarico significativo: repliche, spazio riservato Linux e OpenSearch spazio riservato ai servizi. Ad esempio, una partizione primaria da 20 GiB con una partizione di replica richiede circa 58 GiB di archiviazione ad accesso frequente.

Poiché utilizza Amazon S3, non UltraWarm comporta alcun sovraccarico. Nel calcolo dei requisiti UltraWarm di archiviazione, si considera solo la dimensione degli shard primari. La durata dei dati in S3 elimina la necessità di repliche e S3 elimina tutte le considerazioni relative al sistema operativo o al servizio. La stessa partizione da 20 GiB richiede 20 GiB di archiviazione a caldo. Se si esegue il provisioning di un'istanza `ultrawarm1.large.search`, è possibile utilizzare tutti i 20 TiB della relativa archiviazione massima per le partizioni primarie. Vedere the section called “UltraWarm quote di archiviazione” per un riepilogo dei tipi di istanza e la quantità massima di archiviazione che ciascuna può gestire.

Tuttavia UltraWarm, consigliamo comunque una dimensione massima dello shard di 50 GiB. Il numero di core della CPU e la quantità di RAM allocata a ciascun tipo di UltraWarm istanza danno un'idea del numero di shard che possono essere cercati contemporaneamente. Tieni presente che, sebbene solo gli shard primari contino ai fini UltraWarm dello storage in S3, in OpenSearch Dashboard le dimensioni UltraWarm dell'indice vengono `_cat/indices` comunque riportate come il totale di tutti gli shard primari e di replica.

Ad esempio, ogni istanza `ultrawarm1.medium.search` ha due core CPU e può indirizzare fino a 1,5 TiB di archiviazione su S3. Due di queste istanze hanno un'archiviazione combinata di 3 TiB, che corrisponde a circa 62 partizioni se ogni partizione è 50 GiB. Se una richiesta al cluster esegue la ricerca solo in quattro di queste partizioni, le prestazioni potrebbero essere eccellenti. Se la richiesta è ampia ed esegue la ricerca in tutte le 62 partizioni, i quattro core della CPU potrebbero faticare per eseguire l'operazione. Monitora le `WarmJVMMemoryPressure` UltraWarm metriche `WarmCPUUtilization` e per capire come le istanze gestiscono i carichi di lavoro.

Se le ricerche sono vaste o frequenti, valuta la possibilità di lasciare gli indici nell'archiviazione ad accesso frequente. Proprio come qualsiasi altro OpenSearch carico di lavoro, il passaggio più importante per determinare se UltraWarm soddisfa le proprie esigenze è eseguire test rappresentativi sui clienti utilizzando un set di dati realistico.

UltraWarm prezzi

Con l'archiviazione ad accesso frequente, si paga per ciò che si fornisce. Alcune istanze richiedono un volume Amazon EBS allegato, mentre altre includono un archivio di istanze. Se lo spazio di archiviazione è vuoto o pieno, si paga lo stesso prezzo.

Con UltraWarm lo storage, paghi solo quello che usi. Un'istanza `ultrawarm1.large.search` può indirizzare fino a 20 TiB di archiviazione su S3, ma se si memorizza solo 1 TiB di dati, viene addebitato solo 1 TiB di dati. Come tutti gli altri tipi di nodi, paghi anche una tariffa oraria per ogni UltraWarm nodo. Per ulteriori informazioni, consulta the section called “Prezzi”.

Abilitazione UltraWarm

La console è il modo più semplice per creare un dominio che utilizza l'archiviazione calda. Durante la creazione del dominio, scegli Abilita nodi UltraWarm dati e il numero di nodi caldi che desideri. Lo stesso processo di base funziona sui domini esistenti, a condizione che soddisfino i prerequisiti. Anche dopo la modifica dello stato del dominio da Processing a Active, UltraWarm potrebbe non essere disponibile all'uso per diverse ore.

Quando si utilizza un dominio Multi-AZ con standby, il numero di nodi caldi deve essere un multiplo del numero di zone di disponibilità utilizzate. Per ulteriori informazioni, consulta the section called “Multi-AZ con Standby”.

Puoi anche utilizzare l'API AWS CLIo di configurazione per abilitare UltraWarm, in particolare `WarmEnabled`, `WarmCount`, e `WarmType` le opzioni in. `ClusterConfig`

> **Note**
>
> I domini supportano un numero massimo di nodi a caldo. Per informazioni dettagliate, vedi the section called “Quote”.

Comando CLI di esempio

Il AWS CLI comando seguente crea un dominio con tre nodi di dati, tre nodi master dedicati, sei nodi caldi e un controllo granulare degli accessi abilitato:

```
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
```

Per ulteriori informazioni, consultare Riferimento ai comandi AWS CLI.

Richiesta all'API di configurazione di esempio

La seguente richiesta all'API di configurazione crea un dominio con tre nodi di dati, tre nodi master dedicati e sei nodi a caldo con il controllo granulare degli accessi abilitato e una policy di accesso restrittiva:

```
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/*\"}]}"
}
```

Per informazioni dettagliate, consulta l'Amazon OpenSearch Service API Reference.

Migrazione degli indici verso lo storage UltraWarm

Se hai finito di scrivere su un indice e non hai più bisogno delle prestazioni di ricerca più veloci possibili, esegui la migrazione da hot a: UltraWarm

```
POST _ultrawarm/migration/my-index/_warm
```

Quindi controlla lo stato della migrazione:

```
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
    }
  }
}
```

Per eseguire una migrazione, l'integrità dell'indice deve essere verde. Se si esegue la migrazione di diversi indici in rapida successione, è possibile ottenere un riepilogo di tutte le migrazioni in chiaro, simile all'API `_cat`:

```
GET _ultrawarm/migration/_status?v

index    migration_type state
my-index HOT_TO_WARM    RUNNING_SHARD_RELOCATION
```

OpenSearch Il servizio migra un indice alla volta su. UltraWarm In coda possono essere presenti fino a 200 migrazioni. Qualsiasi richiesta che supera il limite verrà rifiutata. Per controllare il numero corrente di migrazioni nella coda, monitorare il parametro`HotToWarmMigrationQueueSize`. Gli indici rimangono disponibili durante tutto il processo di migrazione, senza tempi di inattività.

Il processo di migrazione ha i seguenti stati:

```
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
```

Come indicato da questi stati, le migrazioni potrebbero non riuscire durante gli snapshot, le traslocazioni di sezioni o le fusioni forzate. Gli errori durante gli snapshot o il trasferimento di partizioni sono in genere dovuti a errori dei nodi o a problemi di connettività S3. La mancanza di spazio su disco è solitamente la causa sottostante degli errori di unioni forzate.

Al termine di una migrazione, la stessa richiesta `_status` restituisce un errore. Se controlli l'indice in quel momento, puoi visualizzare alcune impostazioni che sono univoche per gli indici a caldo:

```
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`, in questo caso, è il numero di repliche passive, che non consumano spazio su disco.
- `routing.allocation.require.box_type` specifica che l'indice deve utilizzare nodi caldi anziché nodi di dati standard.
- `merge.policy.max_merge_at_once_explicit` specifica il numero di segmenti da unire contemporaneamente durante la migrazione.

Gli indici nella memoria a caldo sono di sola lettura a meno che non vengano restituiti all'archiviazione a caldo, che li rende UltraWarm più adatti a dati immutabili, come i log. È possibile eseguire query sugli indici ed eliminarli, ma non è possibile aggiungere, aggiornare o eliminare singoli documenti. Se ci si prova, potrebbe essere restituito il seguente errore:

```
{
  "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
}
```

Automazione delle migrazioni

Si consiglia di utilizzare the section called “Index State Management” per automatizzare il processo di migrazione dopo che un indice raggiunge una certa età o soddisfa altre condizioni. Consultare la policy di esempio che illustra tale flusso di lavoro.

Regolazione della migrazione

Le migrazioni degli indici verso lo storage richiedono un'unione forzata. UltraWarm Ogni OpenSearch indice è composto da un certo numero di frammenti e ogni frammento è composto da un certo numero di segmenti di Lucene. L'operazione di unione forzata elimina i documenti contrassegnati per l'eliminazione e consente di risparmiare spazio su disco. Per impostazione predefinita, UltraWarm unisce gli indici in un unico segmento.

È possibile modificare questo valore fino a 1.000 segmenti utilizzando l'impostazione `index.ultrawarm.migration.force_merge.max_num_segments`. Valori più elevati velocizzano il processo di migrazione, ma aumentano la latenza delle query per l'indice a caldo al termine della migrazione. Per modificare l'impostazione, effettuare la seguente richiesta:

```
PUT my-index/_settings
{
  "index": {
    "ultrawarm": {
      "migration": {
        "force_merge": {
          "max_num_segments": 1
        }
      }
    }
  }
}
```

Per verificare quanto tempo richiede questa fase del processo di migrazione, monitorare il parametro `HotToWarmMigrationForceMergeLatency`.

Annullamento di migrazioni

UltraWarm gestisce le migrazioni in sequenza, in una coda. Se una migrazione è nella coda, ma non è ancora stata avviata, è possibile rimuoverla dalla coda utilizzando la seguente richiesta:

```
POST _ultrawarm/migration/_cancel/my-index
```

Se il dominio utilizza il controllo granulare degli accessi, per effettuare questa richiesta è necessaria l'autorizzazione `indices:admin/ultrawarm/migration/cancel`.

Elenco degli indici ad accesso frequente e degli indici a caldo

UltraWarm aggiunge due opzioni aggiuntive, simili a`_all`, per aiutare a gestire gli indici caldi e caldi. Per un elenco di tutti gli indici ad accesso frequente o a caldo, effettua le seguenti richieste:

```
GET _warm
GET _hot
```

Puoi utilizzare queste opzioni in altre richieste che specificano gli indici:

```
_cat/indices/_warm
_cluster/state/_all/_hot
```

Ritorno di indici a caldo all'archiviazione ad accesso frequente

Se è necessario scrivere nuovamente su un indice, eseguire la migrazione di nuovo all'archiviazione ad accesso frequente:

```
POST _ultrawarm/migration/my-index/_hot
```

È possibile avere fino a 10 migrazioni in coda dalla memorizzazione a caldo a quella a caldo alla volta. OpenSearch Il servizio elabora le richieste di migrazione una alla volta, nell'ordine in cui sono state messe in coda. Per controllare il numero corrente, monitorare il parametro `WarmToHotMigrationQueueSize`.

Al termine della migrazione, controllare le impostazioni dell'indice per assicurarti che soddisfino le tue esigenze. Gli indici tornano all'archiviazione ad accesso frequente con una replica.

Ripristino degli indici caldi dalle istantanee

Oltre al repository standard per le istantanee automatiche, UltraWarm aggiunge un secondo archivio per gli indici caldi,. `cs-ultrawarm` Ogni snapshot in questo repository contiene un solo indice. Se si elimina un indice a caldo, il relativo snapshot rimarrà nel repository `cs-ultrawarm` per altri 14 giorni, proprio come qualsiasi altro snapshot automatico.

Quando si ripristina uno snapshot da `cs-ultrawarm`, viene ripristinata l'archiviazione a caldo, non l'archiviazione ad accesso frequente. Gli snapshot nei repository `cs-automated` e `cs-automated-enc` ripristinano l'archiviazione ad accesso frequente.

Per ripristinare un'istantanea in una memoria calda UltraWarm

1. Identificare lo snapshot più recente che contiene l'indice che si desidera ripristinare:

```
GET _snapshot/cs-ultrawarm/_all?verbose=false

{
  "snapshots": [{
    "snapshot": "snapshot-name",
    "version": "1.0",
    "indices": [
      "my-index"
    ]
  }]
}
```

> **Note**
>
> Per impostazione predefinita, l'`GET _snapshot/<repo>`operazione visualizza informazioni dettagliate sui dati come ora di inizio, ora di fine e durata per ogni istantanea all'interno di un repository. L'`GET _snapshot/<repo>`operazione recupera le informazioni dai file di ogni istantanea contenuta in un repository. Se non sono necessarie l'ora di inizio, l'ora di fine e la durata e si richiedono solo il nome e le informazioni sull'indice di un'istantanea, si consiglia di utilizzare il `verbose=false` parametro quando si elencano le istantanee per ridurre al minimo i tempi di elaborazione ed evitare il timeout.

2. Se l'indice esiste già, eliminalo:

```
DELETE my-index
```

   Se non si desidera eliminare l'indice, riportarlo all'archiviazione ad accesso frequente e reindicizzarlo.

3. Ripristinare lo snapshot:

```
POST _snapshot/cs-ultrawarm/snapshot-name/_restore
```

UltraWarm ignora tutte le impostazioni dell'indice specificate in questa richiesta di ripristino, ma è possibile specificare opzioni come e. `rename_pattern` `rename_replacement` Per un riepilogo delle opzioni di ripristino delle OpenSearch istantanee, consulta la OpenSearch documentazione.

Snapshot manuali di indici a caldo

Puoi eseguire snapshot manuali di indici a caldo, ma non è consigliabile. Il repository `cs-ultrawarm` automatico contiene già uno snapshot per ogni indice a caldo, acquisito durante la migrazione, senza costi aggiuntivi.

Per impostazione predefinita, OpenSearch Service non include indici caldi nelle istantanee manuali. Ad esempio, la chiamata seguente include solo gli indici ad accesso frequente:

```
PUT _snapshot/my-repository/my-snapshot
```

Per eseguire snapshot manuali di indici a caldo, occorre fare delle considerazioni importanti.

- Non è possibile mescolare indici ad accesso frequente e indici a caldo. Ad esempio, la seguente richiesta ha esito negativo:

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1,hot-index-1",
    "include_global_state": false
  }
  ```

  Se mescoli indici ad accesso frequente e indici a caldo, le istruzioni con caratteri jolly (*) non riescono.
- Puoi includere un solo indice a caldo per ogni snapshot. Ad esempio, la seguente richiesta ha esito negativo:

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1,warm-index-2,other-warm-indices-*",
  ```

```
  "include_global_state": false
}
```

Questa richiesta ha esito positivo:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1",
  "include_global_state": false
}
```

- Gli snapshot manuali vengono sempre ripristinati nell'archiviazione ad accesso frequente, anche se originariamente includevano un indice a caldo.

Migrazione degli indici a caldo all'archiviazione a freddo

Se hai dati UltraWarm che richiedi raramente, valuta la possibilità di migrarli alla conservazione a freddo. L'archiviazione a freddo è pensata per i dati a cui si accede solo occasionalmente o che non sono più utilizzati. Non puoi leggere o scrivere su indici a freddo, ma puoi eseguirne di nuovo la migrazione allo storage a caldo senza alcun costo ogni volta che devi eseguire una query su tali indici. Per istruzioni, consulta the section called “Migrazione degli indici all'archiviazione a freddo”.

Disabilitazione UltraWarm

La console è il modo più semplice per UltraWarm disabilitare. Scegli il dominio, Operazioni quindi Modifica configurazione cluster. Deseleziona Abilita nodi UltraWarm dati e scegli Salva modifiche. È inoltre possibile utilizzare l'opzione `WarmEnabled` nell'API di configurazione e in AWS CLI .

Prima di disabilitarli UltraWarm, devi eliminare tutti gli indici caldi o migrarli nuovamente all'archiviazione a caldo. Una volta esaurita la memoria a caldo, attendi cinque minuti prima di provare a disattivarla. UltraWarm

Conservazione a freddo per Amazon OpenSearch Service

Lo storage a freddo ti consente di archiviare qualsiasi quantità di dati storici o ad accesso raro sul tuo dominio Amazon OpenSearch Service e di analizzarli su richiesta, a un costo inferiore rispetto ad altri livelli di storage. L'archiviazione a freddo è adatta se si ha bisogno di effettuare ricerche periodiche o analisi forensi sui dati più vecchi. Esempi pratici di dati adatti per l'archiviazione a freddo includono

i log a cui si accede raramente, i dati che devono essere conservati per soddisfare i requisiti di conformità o i log che hanno un valore storico.

Analogamente allo UltraWarmstorage, lo storage a freddo è supportato da Amazon S3. Quando è necessario interrogare dati non aggiornati, è possibile collegarli in modo selettivo ai nodi esistenti UltraWarm. È possibile gestire la migrazione e il ciclo di vita dei dati a freddo manualmente o con le policy di Index State Management.

Argomenti

Prerequisiti

L'archiviazione a freddo ha i seguenti prerequisiti:

- La conservazione a freddo richiede Elasticsearch versione 7.9 OpenSearch o successiva.
- Per abilitare la conservazione a freddo su un dominio OpenSearch di servizio, è necessario abilitarla anche UltraWarm sullo stesso dominio.
- Per utilizzare l'archiviazione a freddo, i domini devono disporre di nodi principali dedicati.

- Se il dominio utilizza un tipo di istanza T2 o T3 per i nodi di dati, non è possibile utilizzare l'archiviazione a freddo.
- Se il tuo indice utilizza un k-NN approssimato (`"index.knn": true`), non puoi spostarlo in un'archiviazione offline sicura.
- Se il dominio utilizza un controllo granulare degli accessi, gli utenti non amministratori devono essere mappati al `cold_manager` ruolo nelle OpenSearch dashboard per gestire gli indici freddi.

> **Note**
>
> Il `cold_manager` ruolo potrebbe non esistere in alcuni domini di servizio preesistenti. OpenSearch Se il ruolo non è visualizzato in Dashboards, sarà necessario crearlo manualmente.

Configurazione delle autorizzazioni

Se abiliti la conservazione a freddo su un dominio di OpenSearch servizio preesistente, il `cold_manager` ruolo potrebbe non essere definito nel dominio. Se il dominio utilizza un controllo granulare degli accessi, gli utenti non amministratori devono essere mappati a questo ruolo per gestire gli indici freddi. Per creare manualmente il ruolo `cold_manager`, procedere nel seguente modo:

1. In OpenSearch Dashboard, vai su Sicurezza e scegli Autorizzazioni.
2. Scegliere Crea gruppo di operazioni e configurare i seguenti gruppi:

Group name (Nome gruppo)	Autorizzazioni
`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`

Group name (Nome gruppo)	Autorizzazioni
	• `indices:admin/ultrawarm/migration/cancel`

3. Scegliere Ruoli, quindi selezionare Crea ruolo.
4. Denominare il ruolo cold_manager.
5. Per Autorizzazioni cluster, scegliere il gruppo `cold_cluster` creato.
6. Per Indice, immettere `*`.
7. Per Autorizzazioni indice, scegliere il gruppo `cold_index` creato.
8. Scegli Crea.
9. Dopo aver creato il ruolo, associalo a qualsiasi ruolo utente o di backend che gestisce gli indici freddi.

Requisiti di archiviazione a freddo e considerazioni sulle prestazioni

Poiché lo storage a freddo utilizza Amazon S3, non comporta alcun sovraccarico dello storage a caldo, ad esempio repliche, spazio riservato Linux e spazio riservato Service. OpenSearch L'archiviazione a freddo non ha tipi di istanza specifici perché non ha alcuna capacità di calcolo collegata. Con l'archiviazione a freddo è possibile archiviare qualsiasi quantità di dati. Monitora la `ColdStorageSpaceUtilization` metrica in Amazon CloudWatch per vedere quanto spazio di archiviazione a freddo stai utilizzando.

Prezzi dell'archiviazione a freddo

Analogamente all' UltraWarm archiviazione, con la conservazione a freddo paghi solo per l'archiviazione dei dati. Non è previsto alcun costo di calcolo per i dati a freddo e non verrà addebitato nulla se nello spazio di archiviazione a freddo non ci sono dati.

Non si applicano spese di trasferimento quando si spostano i dati tra l'archiviazione a freddo e quella a caldo. Mentre gli indici vengono migrati tra l'archiviazione a caldo e quella a freddo, si continua a pagare solo una copia dell'indice. Al termine della migrazione, l'indice viene fatturato in base al livello di archiviazione in cui è stata eseguita la migrazione. Per ulteriori informazioni sui prezzi delle celle frigorifere, consulta i prezzi OpenSearch di Amazon Service.

Abilitazione dell'archiviazione a freddo

La console è il modo più semplice per creare un dominio che utilizza l'archiviazione a freddo. Durante la creazione del dominio, scegliere Abilita archiviazione a freddo. Lo stesso processo di base funziona sui domini esistenti, a condizione che soddisfino i prerequisiti. Anche dopo che lo stato del dominio cambia da Elaborazione a Attivo, l'archiviazione a freddo potrebbe non essere disponibile per diverse ore.

Per abilitare l'archiviazione a freddo è possibile utilizzare anche la AWS CLI o l'API di configurazione.

Comando CLI di esempio

Il AWS CLI comando seguente crea un dominio con tre nodi di dati, tre nodi master dedicati, la conservazione a freddo abilitata e il controllo granulare degli accessi abilitato:

```
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
```

Per ulteriori informazioni, consultare Riferimento ai comandi AWS CLI.

Richiesta dell'API di configurazione di esempio

La seguente richiesta all'API di configurazione crea un dominio con tre nodi di dati, tre nodi principali dedicati, l'archiviazione a freddo abilitata e il controllo granulare degli accessi abilitato:

```
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"
}
```

Per informazioni dettagliate, consulta l'Amazon OpenSearch Service API Reference.

Gestione degli indici freddi nelle dashboard OpenSearch

Puoi gestire gli indici caldi, caldi e freddi con l'interfaccia Dashboards esistente nel tuo dominio di servizio. OpenSearch Dashboards consente di eseguire la migrazione degli indici tra l'archiviazione a caldo e quella a freddo e di monitorare lo stato della migrazione degli indici, senza utilizzare la CLI o l'API di configurazione. Per ulteriori informazioni, consulta Gestione degli indici nei dashboard. OpenSearch

Migrazione degli indici all'archiviazione a freddo

Quando si esegue la migrazione degli indici all'archiviazione a freddo, si fornisce un intervallo di tempo per i dati per semplificare l'individuazione. È possibile selezionare un campo timestamp in base ai dati dell'indice, fornire manualmente un timestamp di inizio e di fine oppure scegliere di non specificarne uno.

Parametro	Valore supportato	Descrizione
`timestamp_field`	Il campo data/ora dalla mappatura dell'indice.	I valori minimo e massimo del campo forniti vengono calcolati e archiviati come metadati `start_time` e `end_time` per l'indice a freddo.
`start_time` e `end_time`	Uno dei seguenti formati: • strict_date_optional_time. Ad esempio: `yyyy-MM-dd'T'HH:mm:ss.SSSZ` o `yyyy-MM-dd` • L'ora Epoch espressa in millisecondi	I valori forniti vengono calcolati e archiviati come metadati `start_time` e `end_time` per l'indice a freddo.

Se non si intendi specificare un timestamp, aggiungere `?ignore=timestamp` alla richiesta.

La richiesta seguente esegue la migrazione di un indice a caldo all'archiviazione a freddo e fornisce ora di inizio e fine per i dati in tale indice:

```
POST _ultrawarm/migration/my-index/_cold
  {
    "start_time": "2020-03-09",
    "end_time": "2020-03-09T23:00:00Z"
  }
```

Quindi controlla lo stato della migrazione:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_METADATA_RELOCATION",
    "migration_type": "WARM_TO_COLD"
  }
}
```

OpenSearch Il servizio migra un indice alla volta nella conservazione a freddo. È possibile disporre di un massimo di 100 migrazioni nella coda. Qualsiasi richiesta che supera il limite verrà rifiutata. Per controllare il numero corrente di migrazioni nella coda, monitorare il parametro`WarmToColdMigrationQueueSize`. Il processo di migrazione ha i seguenti stati:

```
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.
```

Automatizzazione delle migrazioni all'archiviazione a freddo

Si consiglia di utilizzare Index State Management per automatizzare il processo di migrazione dopo che un indice raggiunge una certa età o soddisfa altre condizioni. Guarda la policy di esempio, che dimostra come migrare automaticamente gli indici dalla conservazione a caldo a quella a freddo. UltraWarm

> **Note**
>
> Un `timestamp_field` esplicito è necessario per spostare gli indici nell'archiviazione a freddo utilizzando una policy di Index State Management.

Annullamento delle migrazioni all'archiviazione a freddo

Se una migrazione all'archiviazione a freddo è in coda o in uno stato di errore, è possibile annullare la migrazione utilizzando la seguente richiesta:

```
POST _ultrawarm/migration/_cancel/my-index

{
  "acknowledged" : true
}
```

Se il dominio utilizza il controllo granulare degli accessi, per effettuare questa richiesta è necessaria l'autorizzazione `indices:admin/ultrawarm/migration/cancel`.

Elencare gli indici freddi

Prima di eseguire l'interrogazione, puoi elencare gli indici in cold storage per decidere a quali migrare per ulteriori analisi. UltraWarm La richiesta seguente elenca tutti gli indici freddi, ordinati per nome dell'indice:

```
GET _cold/indices/_search
```

Risposta di esempio

```
{
  "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"
    }
  ]
}
```

Filtraggio

È possibile filtrare gli indici a freddo in base a un modello di indice basato su prefisso e a offset di intervallo di tempo.

La seguente richiesta elenca gli indici che corrispondono al modello di prefisso di `event-*`:

```
GET _cold/indices/_search
 {
   "filters":{
      "index_pattern": "event-*"
   }
 }
```

Risposta di esempio

```
{
  "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 seguente richiesta restituisce indici con campi di metadati `start_time` e `end_time` tra `2019-03-01` e `2020-03-01`:

```
GET _cold/indices/_search
{
  "filters": {
    "time_range": {
      "start_time": "2019-03-01",
      "end_time": "2020-03-01"
    }
  }
}
```

Risposta di esempio

```
{
  "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"
    }
  ]
}
```

Ordinamento

È possibile ordinare gli indici a freddo in base ai campi di metadati, ad esempio il nome dell'indice o la dimensione. La richiesta seguente elenca tutti gli indici ordinati per dimensione in ordine decrescente:

```
GET _cold/indices/_search
 {
 "sort_key": "size:desc"
 }
```

Risposta di esempio

```
{
  "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"
    }
  ]
}
```

Altre chiavi di ordinamento valide sono `start_time:asc/desc`, `end_time:asc/desc` e `index_name:asc/desc`.

Paginazione

È possibile impaginare un elenco di indici freddi. Configurare il numero di indici da restituire per pagina con il parametro `page_size` (il valore di default è 10). Ogni richiesta `_search` sugli indici a freddo restituisce un `pagination_id` che è possibile utilizzare per le chiamate successive.

La seguente richiesta impagina i risultati di una richiesta `_search` degli indici a freddo e visualizza i successivi 100 risultati:

```
GET _cold/indices/_search?page_size=100
{
"pagination_id": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
}
```

Migrazione degli indici a freddo all'archiviazione a caldo

Dopo aver ristretto l'elenco degli indici freddi con i criteri di filtro della sezione precedente, trasferiscili nuovamente UltraWarm dove puoi interrogare i dati e utilizzarli per creare visualizzazioni.

La richiesta seguente esegue la migrazione di due indici a freddo all'archiviazione a caldo:

```
POST _cold/migration/_warm
 {
 "indices": "my-index1,my-index2"
 }


{
  "acknowledged" : true
}
```

Per verificare lo stato della migrazione e recuperare l'ID di migrazione, inviare la seguente richiesta:

```
GET _cold/migration/_status
```

Risposta di esempio

```
{
  "cold_to_warm_migration_status" : [
    {
      "migration_id" : "tyLjXCA-S76zPQbPVHkOKA",
      "indices" : [
        "my-index1,my-index2"
      ],
      "state" : "RUNNING_INDEX_CREATION"
    }
  ]
}
```

Per ottenere informazioni sulla migrazione specifiche dell'indice, includere il nome dell'indice:

```
GET _cold/migration/my-index/_status
```

Anziché specificare un indice, è possibile elencare gli indici in base al relativo stato di migrazione corrente. I valori validi sono `_failed`, `_accepted` e `_all`.

Il comando seguente ottiene lo stato di tutti gli indici in una singola richiesta di migrazione:

```
GET _cold/migration/_status?migration_id=my-migration-id
```

Recuperare l'ID di migrazione utilizzando la richiesta di stato. Per informazioni dettagliate sulla migrazione, aggiungere `&verbose=true`.

È possibile migrare gli indici dall'archiviazione a freddo a quella a caldo in batch da 10 o meno, con un massimo di 100 indici simultanei. Qualsiasi richiesta che supera il limite verrà rifiutata. Per controllare il numero di migrazioni in atto, monitora il parametro `ColdToWarmMigrationQueueSize`. Il processo di migrazione ha i seguenti stati:

```
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.
```

Ripristino di indici a freddo da snapshot

Se devi ripristinare un indice freddo eliminato, puoi ripristinarlo al livello caldo seguendo le istruzioni riportate the section called “Ripristino degli indici caldi dalle istantanee” e poi migrando nuovamente l'indice al livello freddo. Non è possibile ripristinare un indice di freddo eliminato direttamente nel livello freddo. OpenSearch Il servizio conserva gli indici freddi per 14 giorni dopo la loro eliminazione.

Annullamento delle migrazioni dall'archiviazione a freddo a quella a caldo

Se una migrazione dell'indice dall'archiviazione a freddo a quella a caldo è in coda o in uno stato di errore, è possibile annullare la migrazione utilizzando la seguente richiesta:

```
POST _cold/migration/my-index/_cancel

{
  "acknowledged" : true
}
```

Per annullare la migrazione per un batch di indici (massimo 10 alla volta), specificare l'ID di migrazione:

```
POST _cold/migration/_cancel?migration_id=my-migration-id

{
  "acknowledged" : true
}
```

Recuperare l'ID di migrazione utilizzando la richiesta di stato.

Aggiornamento dei metadati dell'indice a freddo

È possibile aggiornare i campi `start_time` e `end_time` per un indice a freddo:

```
PATCH _cold/my-index
 {
 "start_time": "2020-01-01",
 "end_time": "2020-02-01"
 }
```

Non è possibile aggiornare il `timestamp_field` di un indice nell'archiviazione a freddo.

> **Note**
>
> OpenSearch Dashboards non supporta il metodo PATCH. Per aggiornare i metadati a freddo, utilizzare curl, Postman o qualche altro metodo.

Eliminazione di indici freddi

Se non si utilizza una policy ISM, è possibile eliminare manualmente gli indici a freddo. La seguente richiesta elimina un indice a freddo:

```
DELETE _cold/my-index

{
  "acknowledged" : true
}
```

Disabilitazione dell'archiviazione a freddo

La console OpenSearch di servizio è il modo più semplice per disabilitare la conservazione a freddo. Seleziona il dominio e scegli Operazioni, Modifica configurazione cluster, quindi deseleziona Abilita archiviazione a freddo.

Per utilizzare la AWS CLI o l'API di configurazione, sotto`ColdStorageOptions`, imposta. `"Enabled"="false"`

Prima di disabilitare l'archiviazione a freddo, è necessario eliminare tutti gli indici a freddo o migrarli nuovamente all'archiviazione a caldo, altrimenti l'operazione di disabilitazione non riuscirà.

Archiviazione OR1 per Amazon Service OpenSearch

OR1 è una famiglia di istanze per Amazon OpenSearch Service che offre un modo conveniente per archiviare grandi quantità di dati. Un dominio con istanze OR1 utilizza Amazon Elastic Block Store (Amazon gp3 EBS) `io1` o volumi per lo storage principale, con i dati copiati in modo sincrono su Amazon S3 non appena arrivano. Questa struttura di storage offre una maggiore velocità di indicizzazione con un'elevata durabilità. La famiglia di istanze OR1 supporta anche il ripristino automatico dei dati in caso di errore. Per informazioni sulle opzioni relative al tipo di istanza OR1, vedere. the section called “Tipi di istanza della generazione attuale”

Se esegui l'indicizzazione di carichi di lavoro pesanti di analisi operativa, come l'analisi dei log, l'osservabilità o l'analisi della sicurezza, puoi trarre vantaggio dalle migliori prestazioni ed efficienza di calcolo delle istanze OR1. Inoltre, il ripristino automatico dei dati offerto dalle istanze OR1 migliora l'affidabilità complessiva del dominio.

OpenSearch Il servizio invia ad Amazon i parametri OR1 relativi allo storage. CloudWatch Per un elenco di parametri disponibili, consulta ???.

Le istanze OR1 sono disponibili su richiesta o con prezzi per istanze riservate, con una tariffa oraria per le istanze e lo storage forniti in Amazon EBS e Amazon S3.

Argomenti

- Limitazioni
- In che modo OR1 si differenzia dallo storage UltraWarm
- Utilizzo delle istanze OR1

Limitazioni

Considera le seguenti limitazioni quando utilizzi le istanze OR1 per il tuo dominio.

- Il tuo dominio deve avere la OpenSearch versione 2.11 o successiva.
- Il dominio deve avere la crittografia a riposo abilitata. Per ulteriori informazioni, consulta ???.
- Il tuo dominio deve essere un nuovo dominio. Non è possibile modificare un dominio esistente per utilizzare istanze OR1.
- Se il tuo dominio utilizza nodi master dedicati, devono utilizzare istanze Graviton. Per ulteriori informazioni sui nodi master dedicati, consulta. ???
- Le dimensioni degli shard sulle istanze OR1 devono essere inferiori a 100 GiB. Gli shard di dimensioni superiori a 100 GiB possono rallentare i tempi di ripristino. Se crei shard di dimensioni superiori a 100 GiB su istanze OR1 OpenSearch , Service blocca le richieste di scrittura sul dominio. Se desideri comunque utilizzare shard più grandi di 100 GiB, AWS Supportcontatta per richiedere un aumento della quota.
- L'intervallo di aggiornamento per gli indici sulle istanze OR1 deve essere pari o superiore a 10 secondi. L'intervallo di aggiornamento predefinito per le istanze OR1 è di 10 secondi.

In che modo OR1 si differenzia dallo storage UltraWarm

OpenSearch Il servizio fornisce UltraWarm istanze ottimizzate per ridurre i costi di archiviazione di dati non aggiornati. Sia OR1 che le UltraWarm istanze archiviano i dati localmente in Amazon EBS e in remoto in Amazon S3. Tuttavia, OR1 e le UltraWarm istanze differiscono in diversi modi importanti:

- Le istanze OR1 conservano una copia dei dati nell'archiviazione locale e remota. UltraWarm le istanze, per ridurre i costi di archiviazione, conservano i dati principalmente nello storage remoto. A seconda dei modelli di utilizzo, potrebbero spostarli nella memoria locale.
- Le istanze OR1 sono attive e possono accettare operazioni di lettura e scrittura, mentre i dati sulle UltraWarm istanze sono di sola lettura finché non vengono spostati manualmente nella memoria a caldo.
- UltraWarm si affida alle istantanee degli indici per la durabilità dei dati. Le istanze OR1, invece, eseguono la replica e il ripristino in background. In caso di indice rosso, le istanze OR1 ripristinano automaticamente gli shard mancanti dallo storage remoto in Amazon S3. Il tempo di ripristino varia a seconda del volume di dati da recuperare.

Per ulteriori informazioni sullo UltraWarm storage, vedere???.

Utilizzo delle istanze OR1

Puoi selezionare istanze OR1 per i tuoi nodi di dati quando crei un nuovo dominio con AWS Management Console, the AWS Command Line Interface (AWS CLI) o SDK. AWS Puoi quindi indicizzare e interrogare i dati utilizzando gli strumenti esistenti.

Console

1. Accedi alla console di Amazon OpenSearch Service all'indirizzohttps://console.aws.amazon.com/aos/.
2. Nel riquadro di navigazione a sinistra, scegli Domains (Domini).
3. Scegli Crea dominio.
4. Inserisci un nome per il tuo dominio insieme alle altre opzioni preferite. In Famiglia di istanze, scegli OR1. Scegli Crea per avviare il processo di creazione del dominio.

AWS CLI

1. Accedi al tuo AWS CLI terminale. Se devi installare il AWS CLI, vedi Installare o aggiornare la versione più recente di AWS CLI.
2. Per utilizzare lo storage OR1, è necessario fornire il valore della dimensione del tipo di istanza OR1 specifico nel `InstanceType` campo quando si crea un dominio. È inoltre necessario abilitare la crittografia a riposo.

   L'esempio seguente crea un dominio con istanze OR1 di dimensioni. `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/*"}]}'
```

Gestione dello stato dell'indice in Amazon OpenSearch Service

Index State Management (ISM) in Amazon OpenSearch Service ti consente di definire politiche di gestione personalizzate che automatizzano le attività di routine e le applicano a indici e modelli di indice. Non è più necessario configurare e gestire processi esterni per eseguire le operazioni di indice.

Una policy contiene uno stato predefinito e un elenco di stati fra cui l'indice può transitare. All'interno di ciascuno stato, puoi definire un elenco di operazioni da eseguire e di condizioni che attivano queste transizioni. Un tipico caso d'uso è quello di eliminare periodicamente i vecchi indici dopo

un certo periodo di tempo. Ad esempio, puoi definire una policy che sposta l'indice nello stato `read_only` dopo 30 giorni e successivamente lo elimina dopo 90 giorni.

Dopo aver collegato una policy a un indice, ISM crea un processo che viene eseguito ogni 5-8 minuti (o 30-48 minuti per i cluster precedenti alla versione 1.3) per eseguire le operazioni di policy, controllare le condizioni e passare l'indice in stati diversi. Il tempo di base per l'esecuzione di questo processo è ogni 5 minuti, più viene aggiunto un jitter casuale tra lo 0 e il 60% per evitare che le attività arrivino da tutti gli indici contemporaneamente. ISM non esegue processi se lo stato del cluster è rosso.

ISM richiede Elasticsearch OpenSearch 6.8 o versione successiva.

> **Note**
>
> Questa documentazione fornisce una breve panoramica di ISM e diverse politiche di esempio. Spiega inoltre in che modo ISM per i domini Amazon OpenSearch Service differisce da ISM sui cluster OpenSearch autogestiti. Per la documentazione completa di ISM, incluso un riferimento completo ai parametri, le descrizioni di ogni impostazione e un riferimento all'API, consulta Index State Management nella documentazione. OpenSearch

> **Important**
>
> Non puoi più utilizzare modelli di indice per applicare policy ISM agli indici appena creati. È possibile continuare a gestire automaticamente gli indici appena creati con il campo del modello ISM. Questo aggiornamento introduce una modifica sostanziale che influisce sui CloudFormation modelli esistenti che utilizzano questa impostazione.

Creazione di una policy ISM

Per iniziare a utilizzare la gestione degli stati degli indici

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Seleziona il dominio per cui creare una policy ISM.
3. Dalla dashboard del dominio, vai all'URL delle OpenSearch dashboard e accedi con il nome utente e la password principali. L'URL segue il seguente formato:

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

4. Apri il pannello di navigazione a sinistra all'interno di OpenSearch Dashboards e scegli Gestione degli indici, quindi Crea politica.
5. Utilizza il plug-in editor visivo o editor JSON per creare policy. Consigliamo di utilizzare l'editor visivo in quanto offre un modo più strutturato per definire le policy. Per assistenza nella creazione di policy, consulta le policy di esempio qui sotto.
6. Dopo aver creato una policy, puoi collegarla a uno o più indici:

```
POST _plugins/_ism/add/my-index
{
  "policy_id": "my-policy-id"
}
```

> **Note**
>
> Se il tuo dominio sta eseguendo una versione legacy di Elasticsearch, usa `_opendistro`invece di `_plugins`.

In alternativa, seleziona l'indice nelle OpenSearch dashboard e scegli Applica politica.

Policy di esempio

Le policy di esempio riportate di seguito illustrano come automatizzare i casi d'uso comuni di ISM.

Archiviazione ad accesso frequente, a caldo, a freddo

Questa policy di esempio sposta un indice dalla memorizzazione a caldo a UltraWarm, e infine, a conservazione a freddo. Quindi, elimina l'indice.

L'indice si trova inizialmente nello stato `hot`. Dopo dieci giorni, ISM lo sposta allo stato `warm`. 80 giorni dopo, quando l'indice ha 90 giorni, lo sposta nello stato `cold`. Dopo un anno, il servizio invia una notifica ad una stanza Amazon Chime indicante che l'indice sta per essere eliminato, quindi lo elimina definitivamente.

Tenere presente che gli indici a freddo richiedono l'operazione `cold_delete` piuttosto che la normale operazione `delete`. Inoltre, per gestire gli indici a freddo con ISM nei dati è necessario un `timestamp_field` esplicito.

```
{
  "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": {}
        }]
      }
    ]
  }
}
```

Riduzione del numero di repliche

Questa seconda policy di esempio riduce il numero di repliche a zero dopo sette giorni per risparmiare spazio su disco e quindi elimina l'indice dopo 21 giorni. Questa policy presuppone che l'indice non sia critico e che non riceva più richieste di scrittura; la presenza di repliche zero comporta un rischio di perdita di dati.

```
{
  "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": []
      }
    ]
  }
}
```

Acquisizione di uno snapshot dell'indice

Questa policy di esempio utilizza l'operazione `snapshot` per acquisire uno snapshot di un indice non appena contiene almeno un documento. `repository` è il nome del repository di snapshot manuali registrato in Amazon S3. `snapshot` è il nome dello snapshot. Per i prerequisiti di snapshot e i passaggi per registrare un repository, consultare the section called “Creazione di snapshot di indici”.

```
{
  "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": []
      }
    ]
  }
}
```

Modelli ISM

È possibile configurare un campo `ism_template` in una policy in modo che quando si crea un indice corrispondente allo schema del modello, la policy viene automaticamente associata a tale indice. In questo esempio, qualsiasi indice creato con un nome che inizia con "log" viene automaticamente abbinata alla policy 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
    }
```

```
  }
}
```

Per un esempio più dettagliato, consultare Policy di esempio con modello ISM per il rollover automatico.

Differenze

Rispetto a OpenSearch Elasticsearch, ISM per Amazon OpenSearch Service presenta diverse differenze.

Operazioni ISM

- OpenSearch Il servizio supporta tre operazioni ISM uniche, `warm_migration`cold_migration, e: `cold_delete`
  - Se il dominio è UltraWarmabilitato, l'`warm_migration`azione trasferisce l'indice alla memorizzazione a caldo.
  - Se il tuo dominio ha l'archiviazione a freddo abilitata, l'operazione `cold_migration` transita l'indice all'archiviazione a freddo e l'operazione `cold_delete` elimina l'indice dall'archiviazione a freddo.

  Anche se una di queste operazioni non viene completata all'interno del periodo di timeout impostato, la migrazione o la cancellazione degli indici continua. L'impostazione di error_notification per una delle operazioni precedenti ti informerà che l'operazione non è riuscita se non è stata completata entro il periodo di timeout, ma la notifica è solo per tuo riferimento. L'effettiva operazione non ha alcun timeout intrinseco e continua a essere eseguita fino a quando riesce o non riesce.
- Se il tuo dominio esegue OpenSearch Elasticsearch 7.4 o versione successiva, OpenSearch Service supporta ISM e operazioni. `open` `close`

- Se il tuo dominio esegue Elasticsearch 7.7 OpenSearch o versione successiva, OpenSearch Service supporta l'operazione ISM. `snapshot`

Operazioni ISM di archiviazione a freddo

Per gli indici a freddo, devi specificare un parametro `?type=_cold` quando utilizzi le seguenti API ISM:

- Aggiungi policy
- Rimuovi policy
- Aggiorna policy
- Riprova indice non riuscito
- Spiega indice

Queste API per gli indici a freddo presentano le seguenti differenze aggiuntive:

- Gli operatori con caratteri jolly non sono supportati tranne quando li si utilizza alla fine. Ad esempio, `_plugins/_ism/<add, remove, change_policy, retry, explain>/logstash-*` è supportato ma `_plugins/_ism/<add, remove, change_policy, retry, explain>/iad-*-prod` non lo è.
- Non sono supportati più schemi e nomi di indici. Ad esempio, `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs` è supportato ma `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs,sample-data` non lo è.

Impostazioni ISM

OpenSearch ed Elasticsearch ti consentono di modificare tutte le impostazioni ISM disponibili utilizzando l'API. `_cluster/settings` Su Amazon OpenSearch Service, puoi modificare solo le seguenti impostazioni ISM:

- Impostazioni a livello di cluster:
  - `plugins.index_state_management.enabled`
  - `plugins.index_state_management.history.enabled`
- Impostazioni a livello di indice:
  - `plugins.index_state_management.rollover_alias`

Tutorial: Automazione dei processi di Index State Management

Questo tutorial dimostra come implementare una policy PPL che automatizza le attività di routine di gestione degli indici e applicarle agli indici e ai modelli di indice.

Index State Management (ISM) in Amazon OpenSearch Service ti consente di automatizzare le attività ricorrenti di gestione degli indici, in modo da evitare l'uso di strumenti aggiuntivi per gestire i cicli di vita degli indici. Puoi creare una policy che automatizzi queste operazioni in base all'età, alle dimensioni dell'indice e ad altre condizioni, il tutto dall'interno del tuo dominio Amazon OpenSearch Service.

OpenSearch Il servizio supporta tre livelli di archiviazione: lo stato «caldo» predefinito per la scrittura attiva e l'analisi a bassa latenza, UltraWarm per dati di sola lettura fino a tre petabyte e la conservazione a freddo per l'archiviazione illimitata a lungo termine.

Questo tutorial presenta un esempio di caso d'uso della gestione dei dati di serie temporali negli indici giornalieri. In questo tutorial, imposti un criterio che acquisisce un'istantanea automatica di ogni indice allegato dopo 24 ore. Quindi migra l'indice dallo stato caldo predefinito allo UltraWarm storage dopo due giorni, allo storage a freddo dopo 30 giorni e infine elimina l'indice dopo 60 giorni.

Prerequisiti

- Il dominio OpenSearch di servizio deve eseguire Elasticsearch versione 6.8 o successiva.
- Il dominio deve avere una conservazione a freddo UltraWarmabilitata.
- Devi registrare un repository di snapshot manuali per il tuo dominio.
- Il tuo ruolo utente richiede autorizzazioni sufficienti per accedere alla console OpenSearch di servizio. Se necessario, convalida e configura l'accesso ai domini.

Fase 1: Configura la policy PPL

Innanzitutto, configura una politica ISM nei OpenSearch dashboard.

1. Dalla dashboard del dominio nella console di OpenSearch servizio, accedi all'URL delle OpenSearch dashboard e accedi con il nome utente e la password principali. L'URL segue il seguente formato: *domain-endpoint*`/_dashboards/`.
2. In OpenSearch Dashboard, scegli Aggiungi dati di esempio e aggiungi uno o più indici di esempio al tuo dominio.
3. Aprire il pannello di navigazione sinistro e scegliere Gestione indici, quindi scegliere Crea policy.
4. Assegnare un nome alla policy `ism-policy-example`.
5. Sostituisci la policy predefinita con la seguente policy:

```
{
```

```
"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**
>
> Il campo `ism_template` automaticamente il criterio a qualsiasi indice appena creato che corrisponde a uno dei `index_patterns` specificati. In questo caso, tutti gli indici che iniziano per `index-`. È possibile modificare questo campo in modo che corrisponda a un formato di indice nel proprio ambiente. Per ulteriori informazioni sui modelli, consulta i modelli ISM.

6. Nella sezione `snapshot` della policy, sostituire *`snapshot-repo`* con il nome del repository degli snapshot che hai registrato per il tuo dominio. Facoltativamente, è anche possibile sostituire *`ism-snapshot`*, che sarà il nome dello snapshot al momento della creazione.
7. Scegli Crea. La policy dell'indice è ora visibile nella pagina Policy di gestione dello stato.

Fase 2: collega la policy a uno o più indici.

Dopo aver creato la policy, puoi collegarla a uno o più indici nel cluster.

1. Passa alla scheda Indici ad accesso frequente e cerca `opensearch_dashboards_sample`, che elenca tutti gli indici di esempio aggiunti nella fase 1.

2. Seleziona tutti gli indici e scegli Applica politica, quindi scegli la ism-policy-examplepolitica che hai appena creato.
3. Scegli Applica.

È possibile monitorare gli indici mentre si spostano attraverso i vari stati della pagina degli Indici gestiti dalle policy.

Riepilogo degli indici in Amazon OpenSearch Service con indici cumulativi

Gli indici cumulativi in Amazon OpenSearch Service consentono di ridurre i costi di storage raggruppando periodicamente i vecchi dati in indici riepilogati.

È possibile selezionare i campi di interesse e utilizzare un rollup di indice per creare un nuovo indice con solo i campi aggregati in periodi fissi più grossolani. È possibile archiviare mesi o anni di dati cronologici a una frazione del costo con le stesse prestazioni di query.

L'indicizzazione cumulativa richiede Elasticsearch 7.9 OpenSearch o versione successiva.

> **Note**
>
> Questa documentazione ti aiuta a iniziare a creare un job di indicizzazione cumulativa in Amazon OpenSearch Service. Per una documentazione completa, incluso un elenco di tutte le impostazioni disponibili e un riferimento completo all'API, consulta Index rollups nella OpenSearch documentazione.

Creazione di un processo di rollup dell'indice

Per iniziare, scegli Index Management in OpenSearch Dashboards. Selezionare Processi di rollup e scegliere Creazione di un processo di rollup.

Passaggio 1: configura gli indici

Impostare gli indici di origine e di destinazione. L'indice di origine è quello per cui si desidera eseguire il rollup. L'indice di destinazione è dove vengono salvati i risultati di rollup dell'indice.

Dopo aver creato un processo di rollup dell'indice, non sarà possibile modificarne le selezioni.

Fase 2: Definizione di aggregazioni e parametri

Selezionare gli attributi con le aggregazioni (termini e istogrammi) e i parametri (avg, sum, max, min e conteggio valore) per cui si desidera eseguire il rollup. Assicurarsi di non aggiungere troppi attributi altamente granulari perché si consumerà spazio.

Fase 3: Specifica delle pianificazioni

Specificare una pianificazione per eseguire il rollup degli indici mentre vengono importati. Il processo di rollup dell'indice è abilitato per impostazione predefinita.

Fase 4: Revisione e creazione

Rivedere la configurazione e selezionare Crea.

Fase 5: Ricerca nell'indice di destinazione

È possibile utilizzare l'API `_search` standard per cercare l'indice di destinazione. Non è possibile accedere alla struttura interna dei dati nell'indice di destinazione perché il plug-in riscrive automaticamente la query in background per adattarla all'indice di destinazione. Questo per assicurarsi di poter utilizzare la stessa query per l'indice di origine e di destinazione.

Per eseguire una query sull'indice di destinazione, impostare `size` su 0:

```
GET target_index/_search
{
  "size": 0,
  "query": {
    "match_all": {}
  },
  "aggs": {
    "avg_cpu": {
      "avg": {
        "field": "cpu_usage"
      }
    }
  }
}
```

> **Note**
>
> OpenSearch le versioni 2.2 e successive supportano la ricerca di più indici di rollup in un'unica richiesta. OpenSearch le versioni precedenti alla 2.2 e le versioni precedenti di Elasticsearch OSS supportano solo un indice di rollup per ricerca.

Trasformazione degli indici in Amazon Service OpenSearch

Mentre i processi di aggregazione degli indici consentono di ridurre la granularità dei dati raggruppando i vecchi dati in indici condensati, i processi di trasformazione consentono di creare una visualizzazione riepilogativa diversa dei dati incentrata su determinati campi, in modo da poterli visualizzare o analizzare in diversi modi.

Le trasformazioni degli indici dispongono di un'interfaccia utente Dashboards e di un'API REST. OpenSearch La funzionalità richiede la OpenSearch versione 1.0 o successiva.

> **Note**
>
> Questa documentazione fornisce una breve panoramica delle trasformazioni degli indici per aiutarti a iniziare a utilizzarli su un dominio Amazon OpenSearch Service. Per una documentazione completa e un riferimento all'API REST, consulta Index transforms nella documentazione open source OpenSearch .

Creazione di un processo di trasformazione dell'indice

Se non disponi di dati nel cluster, utilizza i dati di volo di esempio all'interno di OpenSearch Dashboards per provare Transform Jobs. Dopo aver aggiunto i dati, avvia OpenSearch Dashboards. Quindi scegliere Gestione degli indici, Processo di trasformazione e Crea processo di trasformazione.

Passaggio 1: scegli gli indici

Nella sezione Indici, selezionare l'indice di origine e di destinazione. È possibile selezionare un indice di destinazione esistente o crearne uno nuovo specificando un nome.

Se desideri trasformare solo un sottoinsieme dell'indice di origine, scegli Aggiungi filtro dati e usa la OpenSearch query DSL per specificare un sottoinsieme dell'indice di origine.

Fase 2: Scelta dei campi

Dopo aver scelto gli indici, scegli i campi che desideri utilizzare nel processo di trasformazione e se utilizzare raggruppamenti o aggregazioni.

- È possibile utilizzare i raggruppamenti per inserire i dati in bucket separati nell'indice trasformato. Ad esempio, se si desidera raggruppare tutte le destinazioni aeroportuali all'interno dei dati di volo di esempio, raggruppare il campo `DestAirportID` in un campo di destinazione del campo `DestAirportID_terms` e sarà possibile trovare gli ID dell'aeroporto raggruppati nell'indice trasformato al termine del processo di trasformazione.
- D'altra parte, le aggregazioni consentono di eseguire calcoli semplici. Ad esempio, è possibile includere un'aggregazione nel processo di trasformazione per definire un nuovo campo di `sum_of_total_ticket_price` che calcola la somma di tutti i biglietti aerei. Quindi è possibile analizzare i nuovi dati nell'indice trasformato.

Fase 3: Specifica di una pianificazione

I processi di trasformazione sono abilitati per impostazione predefinita e sono eseguiti in base a pianificazioni. Per trasforma intervallo di esecuzione, specificare un intervallo in minuti, ore o giorni.

Fase 4: Revisione e monitoraggio

Rivedere la configurazione e selezionare Crea. Quindi monitorare la colonna Stato del processo di trasformazione.

Fase 5: Ricerca nell'indice di destinazione

Una volta terminato il processo, è possibile utilizzare l'API `_search` standard per cercare l'indice di destinazione.

Ad esempio, dopo aver eseguito un processo di trasformazione che trasforma i dati di volo in base al campo `DestAirportID`, è possibile eseguire la seguente richiesta per restituire tutti i campi che hanno un valore `SFO`:

```
GET target_index/_search
{
  "query": {
    "match": {
      "DestAirportID_terms" : "SFO"
    }
```

```
  }
}
```

Replica tra cluster per Amazon Service OpenSearch

Con la replica tra cluster in Amazon OpenSearch Service, puoi replicare indici utente, mappature e metadati da un dominio di servizio a un altro. OpenSearch L'utilizzo della replica tra cluster aiuta a garantire il ripristino di emergenza in caso di interruzione e consente di replicare i dati su data center geograficamente distanti per ridurre la latenza. Paghi le tariffe standard di trasferimento AWS dei dati per i dati trasferiti tra domini.

La replica tra cluster segue un modello di replica attiva-passiva in cui l'indice locale o dei follower estrae i dati dall'indice remoto o leader. L'indice leader si riferisce all'origine dei dati o all'indice da cui si desidera replicare i dati. L'indice dei follower si riferisce alla destinazione dei dati o all'indice in cui si desidera replicare i dati.

La replica tra cluster è disponibile nei domini che eseguono Elasticsearch 7.10 o 1.1 o versioni successive. OpenSearch

> **Note**
>
> Questa documentazione descrive come configurare la replica tra cluster dal punto di vista di Amazon OpenSearch Service. Ciò include l'utilizzo AWS Management Console di per configurare connessioni tra cluster, cosa non possibile in un cluster autogestito. OpenSearch Per la documentazione completa, incluso un riferimento alle impostazioni e un riferimento completo all'API, consulta Replica tra cluster nella documentazione. OpenSearch

Argomenti

- Arresto della replica
- Auto-follow
- Aggiornamento dei domini connessi

Limitazioni

La replica tra cluster ha le seguenti limitazioni:

- Non puoi replicare i dati tra domini Amazon OpenSearch Service e cluster autogestiti OpenSearch o Elasticsearch.
- Non puoi replicare un indice da un dominio follower a un altro dominio di follower. Se desideri replicare un indice su più domini di follower, puoi replicarlo solo dal singolo dominio leader.
- Un dominio può essere connesso, tramite una combinazione di connessioni in entrata e in uscita, a un massimo di altri 20 domini.
- Quando si configura inizialmente una connessione tra cluster, il dominio leader deve trovarsi nella stessa versione o in una versione successiva rispetto al dominio follower.
- Non è possibile utilizzarlo AWS CloudFormation per connettere domini.
- Non è possibile utilizzare la replica tra cluster su istanze M3 o istanze espandibili (T2 e T3).
- Non è possibile replicare dati tra indici UltraWarm o indici freddi. Entrambi gli indici devono essere nell'archiviazione ad accesso frequente.
- Quando elimini un indice dal dominio leader, l'indice corrispondente nel dominio del follower non viene eliminato automaticamente.

Prerequisiti

Prima di configurare la replica tra cluster, assicurati che i domini soddisfino i seguenti requisiti:

- Elasticsearch 7.10 o 1.1 o versione successiva OpenSearch
- Controllo granulare degli accessi abilitato
- Nessuna crittografia abilitata ode-to-node

Requisiti per le autorizzazioni

Per avviare la replica, è necessario includere l'autorizzazione `es:ESCrossClusterGet` sul dominio remoto (principale). Consigliamo la seguente politica IAM sul dominio remoto. Questa policy consente anche di eseguire altre operazioni, come l'indicizzazione dei documenti e l'esecuzione di ricerche standard:

```
{
  "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"
    }
  ]
}
```

Assicurarsi che l'autorizzazione `es:ESCrossClusterGet` sia applicata per `/leader-domain` e non per `/leader-domain/*`.

Affinché gli utenti non amministratori possano eseguire attività di replica, devono essere mappati alle autorizzazioni appropriate. La maggior parte delle autorizzazioni corrisponde a operazioni REST API specifiche. Ad esempio, l'autorizzazione `indices:admin/plugins/replication/index/_resume` consente di riprendere la replica di un indice. Per un elenco completo delle autorizzazioni, consulta Autorizzazioni di replica nella documentazione. OpenSearch

> **Note**
>
> I comandi per avviare la replica e creare una regola di replica sono casi speciali. Poiché richiamano processi in background sui domini leader e follower, è necessario inserire un `leader_cluster_role` e nella richiesta. `follower_cluster_role` OpenSearch Il servizio utilizza questi ruoli in tutte le attività di replica del backend. Per informazioni sulla mappatura e l'utilizzo di questi ruoli, consulta Mappare i ruoli del cluster leader e follower nella documentazione. OpenSearch

Configurazione di una connessione tra cluster

Per replicare gli indici da un dominio all'altro, è necessario configurare una connessione tra cluster tra i domini. Il modo più semplice per connettere i domini è dalla scheda Connessioni del pannello di controllo del dominio. È inoltre possibile utilizzare l'API di configurazione o AWS CLI. Poiché la replica tra cluster segue un modello "pull" (ovvero di estrazione), le connessioni vengono avviate dal dominio follower.

> **Note**
>
> Se in precedenza sono stati collegati due domini per eseguire ricerche tra cluster, non sarà possibile utilizzare la stessa connessione per la replica. La connessione è contrassegnata come `SEARCH_ONLY` nella console. Per eseguire la replica tra due domini precedentemente connessi, è necessario eliminare la connessione e ricrearla. Una volta fatto questo, la connessione è disponibile sia per la ricerca tra cluster che per la replica tra cluster.

Per impostare una connessione

1. Nella console di Amazon OpenSearch Service, seleziona il dominio del follower, vai alla scheda Connessioni e scegli Richiesta.
2. Per Alias di connessione, specifica un nome per la connessione.
3. Scegli se connetterti a un dominio nella tua regione Account AWS e in un altro account o regione.

   - Per connetterti a un dominio nella tua regione Account AWS e nella tua regione, seleziona il dominio e scegli Richiedi.

- Per connetterti a un dominio in un'altra regione Account AWS o in un'altra regione, specifica l'ARN del dominio remoto e scegli Richiesta.

OpenSearch Il servizio convalida la richiesta di connessione. Se i domini non sono compatibili, la connessione ha esito negativo. Se la convalida ha esito positivo, viene inviata al dominio di destinazione per l'approvazione. Una volta che dominio di destinazione ha approvato la richiesta, sarà possibile iniziare la replica.

La replica tra cluster supporta la replica bidirezionale. Ciò significa che è possibile creare una connessione in uscita dal dominio A al dominio B e un'altra connessione in uscita dal dominio B al dominio A. È quindi possibile impostare la replica in modo che il dominio A segua un indice nel dominio B e il dominio B segua un indice nel dominio A.

Avvio della replica

Dopo aver stabilito una connessione tra cluster, potrai iniziare a replicare i dati. Innanzitutto, crea un indice da replicare nel dominio principale:

```
PUT leader-01
```

Per replicare tale indice, invia questo comando al dominio follower:

```
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"
   }
}
```

È possibile trovare l'alias di connessione nella scheda Connessioni nel pannello di controllo del dominio.

In questo esempio si presuppone che un amministratore stia emettendo la richiesta e utilizzi `all_access` per il `leader_cluster_role` e `follower_cluster_role` per semplicità. Negli ambienti di produzione, tuttavia, si consiglia di creare utenti di replica sugli indici leader e follower

e di mapparli di conseguenza. I nomi utente devono essere identici. Per informazioni su questi ruoli e su come mapparli, consulta Mappare i ruoli del cluster leader e follower nella OpenSearch documentazione.

Conferma della replica

Per confermare che la replica è in corso, ottieni lo stato di replica:

```
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
  }
}
```

I valori dei checkpoint principale e follower iniziano come numeri interi negativi e riflettono il numero di partizioni presenti (-1 per una partizione, -5 per cinque partizioni e così via). I valori aumentano e diventano numeri interi positivi con ogni modifica apportata. Se i valori sono uguali, significa che gli indici sono completamente sincronizzati. È possibile utilizzare questi valori di checkpoint per misurare la latenza di replica nei domini.

Per convalidare ulteriormente la replica, aggiungi un documento all'indice principale:

```
PUT leader-01/_doc/1
{
   "Doctor Sleep":"Stephen King"
}
```

Quindi conferma che viene visualizzato sull'indice follower:

```
GET follower-01/_search

{
```

```
    ...
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "follower-01",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 1.0,
        "_source" : {
          "Doctor Sleep" : "Stephen King"
        }
      }
    ]
  }
}
```

Sospensione e ripristino della replica

È possibile sospendere temporaneamente la replica se è necessario risolvere problemi o ridurre il carico sul dominio principale. Invia questa richiesta al dominio follower. Assicurati di includere un corpo della richiesta vuoto:

```
POST _plugins/_replication/follower-01/_pause
{}
```

Quindi ottieni lo stato per assicurarti che la replica sia sospesa:

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "PAUSED",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01"
}
```

Una volta completate le modifiche, riprendi la replica. Invia questa richiesta al dominio follower. Assicurati di includere un corpo della richiesta vuoto:

```
POST _plugins/_replication/follower-01/_resume
```

```
{}
```

Non è possibile riprendere la replica dopo che è stata sospesa per più di 12 ore. È necessario interrompere la replica, eliminare l'indice di follower e riavviare la replica del leader.

Arresto della replica

Quando si interrompe completamente la replica, l'indice follower smette di seguire l'indice principale e diventa un indice standard. Non è possibile riavviare una replica dopo averla arrestata.

Interrompi la replica dal dominio follower. Assicurati di includere un corpo della richiesta vuoto:

```
POST _plugins/_replication/follower-01/_stop
{}
```

Auto-follow

È possibile definire un set di regole di replica in base a un singolo dominio principale che replicano automaticamente gli indici che corrispondono a uno schema specificato. Quando un indice nel dominio leader corrisponde a uno dei modelli (ad esempio,`books*`), viene creato un indice di follower corrispondente nel dominio del follower. OpenSearch Il servizio replica tutti gli indici esistenti che corrispondono al modello, nonché i nuovi indici creati dall'utente. Non replica gli indici già presenti nel dominio follower.

Per replicare tutti gli indici (ad eccezione degli indici creati dal sistema e di quelli già esistenti nel dominio follower), utilizzare un modello con carattere jolly (`*`).

Creazione di una regola di replica

Crea una regola di replica nel dominio follower e specifica il nome della connessione tra cluster:

```
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"
   }
```

```
}
```

È possibile trovare l'alias di connessione nella scheda Connessioni nel pannello di controllo del dominio.

In questo esempio si presuppone che un amministratore stia emettendo la richiesta e usa `all_access` come ruoli per i domini principale e follower per semplicità. Negli ambienti di produzione, tuttavia, si consiglia di creare utenti di replica sugli indici leader e follower e di mapparli di conseguenza. I nomi utente devono essere identici. Per informazioni su questi ruoli e su come mapparli, consulta Mappare i ruoli del cluster leader e follower nella OpenSearch documentazione.

Per recuperare un elenco di regole di replica esistenti in un dominio, utilizza l'operazione API auto-follow.

Per testare la regola, crea un indice che corrisponda al pattern sul dominio principale:

```
PUT books-are-fun
```

Quindi controlla che la replica venga visualizzata sul dominio follower:

```
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
```

Eliminazione di una regola di replica

Quando si elimina una regola di replica, OpenSearch Service interrompe la replica di nuovi indici che corrispondono al modello, ma continua l'attività di replica esistente finché non si interrompe la replica di tali indici.

Elimina le regole di replica dal dominio follower:

```
DELETE _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name"
}
```

Aggiornamento dei domini connessi

Per aggiornare la versione del motore di due domini con una connessione tra cluster, aggiorna prima il dominio follower e poi il dominio leader. Non eliminate la connessione tra di essi, altrimenti la replica si interrompe e non sarà possibile riprenderla.

Migrazione degli indici di Amazon OpenSearch Service utilizzando la reindicizzazione remota

La reindicizzazione remota consente di copiare gli indici da un dominio Amazon OpenSearch Service a un altro. Puoi migrare gli indici da qualsiasi dominio di OpenSearch servizio o da cluster autogestiti ed Elasticsearch. OpenSearch

Un dominio e un indice remoti si riferiscono alla fonte dei dati o al dominio e all'indice da cui si desidera copiare i dati. Un dominio e un indice locali si riferiscono alla destinazione dei dati o al dominio e all'indice in cui si desidera copiare i dati.

La reindicizzazione remota richiede OpenSearch 1.0 o versione successiva oppure Elasticsearch 6.7 o versione successiva, sul dominio locale. Il dominio remoto deve essere precedente o avere la stessa versione principale del dominio locale. Le versioni di Elasticsearch sono considerate precedenti alle OpenSearch versioni, il che significa che puoi reindicizzare i dati dai domini Elasticsearch ai domini. OpenSearch All'interno della stessa versione principale, il dominio remoto può essere una qualsiasi versione secondaria. Ad esempio, è supportata la reindicizzazione remota da Elasticsearch 7.10.x a 7.9, ma non OpenSearch da 1.0 a Elasticsearch 7.10.x.

> **Note**
>
> Questa documentazione descrive come reindicizzare i dati tra domini Amazon OpenSearch Service. Per la documentazione completa sull'`reindex`operazione, inclusi i passaggi dettagliati e le opzioni supportate, consulta il documento Reindex nella documentazione. OpenSearch

Argomenti

- Prerequisiti
- Reindicizza i dati tra i domini Internet del Servizio OpenSearch
- Reindicizza i dati tra i domini OpenSearch di servizio quando il telecomando si trova in un VPC

- Reindicizza i dati tra domini non OpenSearch di servizio
- Reindicizzazione di set di dati di grandi dimensioni
- Impostazioni di reindicizzazione remota

Prerequisiti

La reindicizzazione remota ha i seguenti requisiti:

- Il dominio remoto deve essere accessibile dal dominio locale. Per un dominio remoto che risiede all'interno di un VPC, il dominio locale deve avere accesso al VPC. Questo processo varia in base alla configurazione di rete, ma probabilmente implica la connessione a una rete VPN o gestita o l'utilizzo della connessione endpoint VPC nativa. Per ulteriori informazioni, consulta the section called “Supporto per VPC”.
- La richiesta deve essere autorizzata dal dominio remoto come qualsiasi altra richiesta REST. Se il dominio remoto ha attivato il controllo granulare degli accessi, è necessario disporre dell'autorizzazione per eseguire la reindicizzazione sul dominio remoto e leggere l'indice sul dominio locale. Per ulteriori considerazioni sulla sicurezza, consultare the section called “Controllo granulare degli accessi”.
- Ti consigliamo di creare un indice con l'impostazione desiderata sul tuo dominio locale prima di iniziare il processo di reindicizzazione.
- Se il dominio utilizza un tipo di istanza T2 o T3 per i nodi di dati, non è possibile utilizzare la reindicizzazione remota.

Reindicizza i dati tra i domini Internet del Servizio OpenSearch

Lo scenario più semplice è che l'indice remoto si trovi nello stesso Regione AWS dominio locale con un endpoint accessibile pubblicamente e che tu abbia firmato le credenziali IAM.

Dal dominio remoto, specifica l'indice remoto da cui reindicizzare e l'indice locale da reindicizzare su:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index"
```

```
  },
  "dest": {
    "index": "local_index"
  }
}
```

È necessario aggiungere 443 alla fine dell'endpoint del dominio remoto per un controllo di convalida.

Per verificare che l'indice venga copiato nel dominio locale, invia questa richiesta al dominio locale:

```
GET local_index/_search
```

Se l'indice remoto si trova in una regione diversa dal dominio locale, inserisci il nome della regione, ad esempio in questa richiesta di esempio:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "region": "eu-west-1"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Nel caso di regioni isolate come quelle cinesi AWS GovCloud (US) o regionali, l'endpoint potrebbe non essere accessibile perché l'utente IAM non è riconosciuto in tali regioni.

Se il dominio remoto è protetto con l'autenticazione di base, specifica il nome utente e la password:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password"
```

```
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Reindicizza i dati tra i domini OpenSearch di servizio quando il telecomando si trova in un VPC

Ogni dominio di OpenSearch servizio è costituito dalla propria infrastruttura interna di cloud privato virtuale (VPC). Quando crei un nuovo dominio in un OpenSearch Service VPC esistente, viene creata un'interfaccia di rete elastica per ogni nodo di dati nel VPC.

Poiché l'operazione di reindicizzazione remota viene eseguita dal dominio del OpenSearch servizio remoto e quindi all'interno del relativo VPC privato, è necessario un modo per accedere al VPC del dominio locale. È possibile farlo utilizzando la funzionalità di connessione endpoint VPC integrata per stabilire una connessione o configurando un proxy. AWS PrivateLink

Se il tuo dominio locale utilizza OpenSearch la versione 1.0 o successiva, puoi utilizzare la console o la AWS CLI per creare una connessione. AWS PrivateLink Una AWS PrivateLink connessione consente alle risorse del VPC locale di connettersi privatamente alle risorse nel VPC remoto all'interno dello stesso. Regione AWS

Reindicizza i dati con AWS Management Console

Puoi utilizzare la reindicizzazione remota con la console per copiare gli indici tra due domini che condividono una connessione endpoint VPC.

1. Accedi alla console di Amazon OpenSearch Service all'indirizzohttps://console.aws.amazon.com/aos/.
2. Nel riquadro di navigazione a sinistra, scegli Domains (Domini).
3. Seleziona il dominio locale o il dominio in cui desideri copiare i dati. Si apre la pagina dei dettagli del dominio. Scegli la scheda Connessioni sotto le informazioni generali e scegli Richiedi.
4. Nella pagina Richiedi connessione, seleziona VPC Endpoint Connection per la tua modalità di connessione e inserisci altri dettagli pertinenti. Questi dettagli includono il dominio remoto, che è il dominio da cui vuoi copiare i dati. Quindi, scegli Request (Richiesta).

5. Vai alla pagina dei dettagli del dominio remoto, scegli la scheda Connessioni e trova la tabella Connessioni in entrata. Seleziona la casella di controllo accanto al nome del dominio da cui hai appena creato la connessione (il dominio locale). Scegli Approve (Approva).
6. Torna al dominio locale, scegli la scheda Connections (Connessioni) e individua la tabella Outbound connections (Connessioni in uscita). Dopo che la connessione tra i due domini è attiva, un endpoint diventa disponibile nella colonna Endpoint della tabella. Copia l'endpoint.
7. Apri il pannello di controllo per il dominio locale e scegli Dev Tools (Strumenti di sviluppo) nella barra di navigazione a sinistra. Per confermare che l'indice del dominio remoto non esiste ancora nel tuo dominio locale, esegui la seguente richiesta GET. Sostituiscilo *remote-domain-index-name*con il tuo nome di indice.

   ```
   GET remote-domain-index-name/_search
   {
      "query":{
         "match_all":{}
      }
   }
   ```

   Nell'output, dovresti vedere un errore che indica che l'indice non è stato trovato.
8. Sotto la tua richiesta GET, crea una richiesta POST e usa il tuo endpoint come host remoto, come riportato di seguito.

   ```
   POST _reindex
   {
      "source":{
         "remote":{
            "host":"connection-endpoint",
            "username":"username",
            "password":"password"
         },
         "index":"remote-domain-index-name"
      },
      "dest":{
         "index":"local-domain-index-name"
      }
   }
   ```

   Esegui questa richiesta.

9. Esegui nuovamente la richiesta GET. L'output dovrebbe ora indicare che l'indice locale esiste. Puoi interrogare questo indice per verificare che siano OpenSearch stati copiati tutti i dati dall'indice remoto.

Reindicizza i dati con le operazioni dell'API OpenSearch di servizio

Puoi utilizzare la reindicizzazione remota con l'API per copiare gli indici tra due domini che condividono una connessione endpoint VPC.

1. Utilizza l'operazione CreateOutboundConnectionAPI per richiedere una nuova connessione dal dominio locale al 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"
      }
   }
}
```

   Riceverai un `ConnectionId` messaggio nella risposta. Salva questo ID per utilizzarlo nel passaggio successivo.

2. Utilizza l'operazione AcceptInboundConnectionAPI con il tuo ID di connessione per approvare la richiesta dal dominio locale.

```
PUT https://es.region.amazonaws.com/2021-01-01/opensearch/cc/
inboundConnection/ConnectionId/accept
```

3. Usa l'operazione DescribeOutboundConnectionsAPI per recuperare l'endpoint per il tuo dominio remoto.

```
{
    "Connections": [
        {
            "ConnectionAlias": "remote-reindex-example",
            "ConnectionId": "connection-id",
            "ConnectionMode": "VPC_ENDPOINT",
            "ConnectionProperties": {
                "Endpoint": "connection-endpoint"
            },
            ...
        }
    ]
}
```

   Salva l'*endpoint di connessione da utilizzare* nel passaggio 5.

4. Per confermare che l'indice del dominio remoto non esiste ancora nel tuo dominio locale, esegui la seguente richiesta GET. Sostituiscilo *remote-domain-index-name*con il tuo nome di indice.

```
GET local-domain-endpoint/remote-domain-index-name/_search
{
   "query":{
      "match_all":{}
   }
}
```

   Nell'output, dovresti vedere un errore che indica che l'indice non è stato trovato.

5. Crea una richiesta POST e usa il tuo endpoint come host remoto, come segue.

```
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"
   }
}
```

Esegui questa richiesta.

6. Esegui nuovamente la richiesta GET. L'output dovrebbe ora indicare che l'indice locale esiste. È possibile interrogare questo indice per verificare che siano OpenSearch stati copiati tutti i dati dall'indice remoto.

Se il dominio remoto è ospitato all'interno di un VPC e non desideri utilizzare la funzionalità di connessione agli endpoint VPC, devi configurare un proxy con un endpoint accessibile pubblicamente. In questo caso, OpenSearch Service richiede un endpoint pubblico perché non è in grado di inviare traffico al tuo VPC.

Quando esegui un dominio in modalità VPC, uno o più endpoint vengono inseriti nel tuo VPC. Tuttavia, questi endpoint servono solo per il traffico che entra nel dominio all'interno del VPC e non consentono il traffico verso il VPC stesso.

Il comando remote reindex viene eseguito dal dominio locale, quindi il traffico di origine non è in grado di utilizzare tali endpoint per accedere al dominio remoto. Ecco perché in questo caso d'uso è necessario un proxy. Il dominio proxy deve avere un certificato firmato di una certification authority (CA) pubblica. I certificati autofirmati o privati firmati dalla CA non sono supportati.

Reindicizza i dati tra domini non OpenSearch di servizio

Se l'indice remoto è ospitato all'esterno del OpenSearch servizio, ad esempio in un'istanza EC2 autogestita, imposta il parametro su: `external true`

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password",
      "external": true
```

```
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

In questo caso, è supportata solo l'autenticazione di base con nome utente e password. Il dominio remoto deve avere un endpoint accessibile pubblicamente (anche se si trova nello stesso VPC del dominio di servizio OpenSearch locale) e un certificato firmato da una CA pubblica. I certificati autofirmati o privati firmati dalla CA non sono supportati.

Reindicizzazione di set di dati di grandi dimensioni

La reindicizzazione remota invia una richiesta di scorrimento al dominio remoto con i seguenti valori predefiniti:

- Contesto di ricerca di 5 minuti
- Timeout socket di 30 secondi
- Dimensione del batch di 1.000

Consigliamo di regolare questi parametri per adattarli ai dati. Per documenti di grandi dimensioni, considerare una dimensione batch più piccola e/o un timeout più lungo. Per ulteriori informazioni, consultare Scorri ricerca.

```
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"
  }
}
```

Si consiglia inoltre di aggiungere le seguenti impostazioni all'indice locale per prestazioni migliori:

```
PUT local_index
{
  "settings": {
    "refresh_interval": -1,
    "number_of_replicas": 0
  }
}
```

Al termine del processo di reindicizzazione, è possibile impostare il numero di repliche desiderato e rimuovere l'impostazione dell'intervallo di aggiornamento.

Per reindicizzare solo un sottoinsieme di documenti selezionati tramite una query, invia questa richiesta al dominio locale:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index",
    "query": {
      "match": {
        "field_name": "text"
      }
    }
  },
  "dest": {
    "index": "local_index"
  }
}
```

La reindicizzazione remota non supporta il partizionamento, quindi non è possibile eseguire più operazioni di scorrimento per la stessa richiesta in parallelo.

Impostazioni di reindicizzazione remota

Oltre alle opzioni di reindicizzazione standard, OpenSearch Service supporta le seguenti opzioni:

Opzioni	Valori validi	Descrizione	Richiesto
external	Booleano	Se il dominio remoto non è un dominio OpenSearch di servizio o se stai reindicizzando tra due domini VPC, specifica come. `true`	No
Regione	Stringa	Se il dominio remoto si trova in una regione diversa, specifica il nome della regione.	No

Gestione dei dati di serie temporali in Amazon OpenSearch Service con flussi di dati

Un flusso di lavoro tipico per la gestione dei dati delle serie temporali comporta più passaggi, ad esempio la creazione di un alias di indice di rollover, la definizione di un indice di scrittura e la definizione di mappatura e impostazioni comuni per gli indici di supporto.

I flussi di dati in Amazon OpenSearch Service aiutano a semplificare questo processo di configurazione iniziale. I flussi di dati funzionano immediatamente per i dati basati sul tempo, ad esempio i log delle applicazioni che in genere sono di natura aggiuntiva.

I flussi di dati richiedono la OpenSearch versione 1.0 o successiva.

> **Note**
>
> Questa documentazione fornisce i passaggi di base per aiutarti a iniziare a utilizzare i flussi di dati su un dominio Amazon OpenSearch Service. Per una documentazione completa, consulta Data Streams nella OpenSearch documentazione.

Nozioni di base sui flussi di dati

Un flusso di dati è composto internamente da più indici di supporto. Le richieste di ricerca vengono instradate a tutti gli indici di supporto, mentre le richieste di indicizzazione vengono instradate all'indice di scrittura più recente.

Fase 1: Creazione di un modello di indice

Per creare un flusso dei dati, è necessario innanzitutto creare un modello di indice che configura un set di indici come flusso dei dati. L'oggetto `data_stream` indica che si tratta di un flusso di dati e non di un modello di indice normale. Il modello di indice corrisponde al nome del flusso di dati:

```
PUT _index_template/logs-template
{
  "index_patterns": [
    "my-data-stream",
    "logs-*"
  ],
  "data_stream": {},
  "priority": 100
}
```

In questo caso, ogni documento inserito deve avere un campo `@timestamp`. Puoi inoltre definire il tuo campo timestamp personalizzato come proprietà nell'oggetto `data_stream`:

```
PUT _index_template/logs-template
{
  "index_patterns": "my-data-stream",
  "data_stream": {
    "timestamp_field": {
      "name": "request_time"
    }
  }
}
```

Fase 2: Creazione di un flusso di dati

Dopo aver creato un modello di indice, è possibile avviare direttamente l'importazione di dati senza dover creare un flusso di dati.

Poiché abbiamo un modello di indice corrispondente a un `data_stream` oggetto, crea OpenSearch automaticamente il flusso di dati:

```
POST logs-staging/_doc
{
  "message": "login attempt failed",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Fase 3: Importazione di dati nel flusso di dati

Per importare i dati in un flusso di dati, è possibile utilizzare le API di indicizzazione regolari. Assicurarsi che ogni documento indicizzato abbia un campo di timestamp. Se si prova a inserire un documento che non dispone di un campo timestamp, viene visualizzato un errore.

```
POST logs-redis/_doc
{
  "message": "login attempt",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Fase 4: Ricerca in un flusso di dati

È possibile eseguire una ricerca in un flusso di dati proprio come in un indice normale o in un alias di indice. L'operazione di ricerca si applica a tutti gli indici di supporto (tutti i dati presenti nel flusso).

```
GET logs-redis/_search
{
  "query": {
    "match": {
      "message": "login"
    }
  }
}
```

Fase 5: Rollover di un flusso di dati

È possibile configurare una policy Index State Management (ISM) per automatizzare il processo di rollover per il flusso di dati. La policy ISM viene applicata agli indici di supporto al momento della loro creazione. Quando si associa una policy a un flusso dei dati, questa influisce solo sugli

indici di supporto futuri di tale flusso dei dati. Inoltre, non è necessario fornire l'impostazione `rollover_alias`, perché la policy ISM deduce queste informazioni dall'indice di supporto.

> **Note**
>
> Se migri un indice di supporto alla conservazione a freddo, OpenSearch rimuove questo indice dal flusso di dati. Anche se si riporta l'indice su UltraWarm, l'indice rimane indipendente e non fa parte del flusso di dati originale. Dopo che un indice è stato rimosso dal flusso di dati, la ricerca all'interno del flusso non restituirà alcun dato dall'indice.

> **Warning**
>
> L'indice di scrittura per un flusso di dati non può essere migrato alla conservazione a freddo. Se desideri migrare i dati dal tuo flusso di dati alla cold storage, devi eseguire il rollover del flusso di dati prima della migrazione.

Fase 6: Gestisci i flussi di dati nelle dashboard OpenSearch

Per gestire i flussi di dati dai OpenSearch dashboard, apri OpenSearch Dashboard, scegli Gestione degli indici, seleziona Indici o Indici gestiti da policy.

Fase 7: Eliminazione di un flusso di dati

L'operazione di eliminazione elimina prima gli indici di supporto di un flusso dei dati e quindi elimina il flusso dei dati stesso.

Per eliminare un flusso di dati e tutti i relativi indici di supporto nascosti:

```
DELETE _data_stream/name_of_data_stream
```

Monitoraggio dei dati in Amazon OpenSearch Service

Monitorare in modo proattivo i dati in Amazon OpenSearch Service con avvisi e rilevamento di anomalie. Impostare gli avvisi per ricevere notifiche quando i dati superano determinate soglie. Il rilevamento delle anomalie utilizza il machine learning per rilevare automaticamente eventuali outlier nello streaming dei dati. È possibile associare il rilevamento delle anomalie con l'avviso per essere certi di ricevere una notifica non appena viene rilevata un'anomalia.

Argomenti

Configurazione degli avvisi in Amazon Service OpenSearch

Configura gli avvisi in Amazon OpenSearch Service per ricevere notifiche quando i dati di uno o più indici soddisfano determinate condizioni. Ad esempio, è possibile decidere di ricevere un'e-mail se l'applicazione registra più di cinque errori HTTP 503 in un'ora oppure di contattare uno sviluppatore se negli ultimi venti minuti non sono stati indicizzati nuovi documenti.

L'invio di avvisi richiede Elasticsearch OpenSearch 6.2 o versione successiva.

> **Note**
>
> Questa documentazione fornisce una breve panoramica degli avvisi ed evidenzia in che modo gli avvisi su un dominio Amazon OpenSearch Service differiscono dagli avvisi su un cluster open source. OpenSearch Per la documentazione completa sugli avvisi, tra cui un riferimento completo alle API, un elenco di campi di richiesta disponibili per i monitor compositi e le descrizioni delle variabili di attivazione e azione disponibili, consulta la sezione Avvisi nella documentazione. OpenSearch

Argomenti

Autorizzazioni per gli avvisi

Gli avvisi supportano il controllo granulare degli accessi. Per i dettagli sulla combinazione e l'abbinamento delle autorizzazioni in base al caso d'uso, consulta Alerting security nella documentazione. OpenSearch

Per accedere alla pagina Avvisi all'interno delle OpenSearch dashboard, devi almeno essere mappato al ruolo `alerting_read_access` predefinito o disporre di autorizzazioni equivalenti. Questo ruolo concede le autorizzazioni per visualizzare avvisi, destinazioni e monitor, ma non per confermare gli avvisi o modificare destinazioni o monitor.

Nozioni di base sugli avvisi

Per creare un avviso, si configura un monitor, che è un processo che viene eseguito in base a una pianificazione definita e interroga gli indici. OpenSearch Inoltre, è necessario configurare uno o più trigger che definiscono le condizioni in base alle quali vengono generati gli eventi. Infine, si configurano le azioni, ossia ciò che accade dopo l'attivazione di un avviso.

Nozioni di base sugli avvisi

1. Scegli Avvisi dal menu principale delle OpenSearch dashboard e scegli Crea monitor.
2. Crea un monitor per query, per bucket, per cluster o per documento. Per istruzioni, consulta la sezione Create a monitor (Creazione di un monitor).
3. Per Trigger, crea uno o più trigger. Per istruzioni, consulta la sezione Creazione di trigger.
4. Per Actions (Azioni), imposta un notification channel (canale di notifica) per l'avviso. Scegliere tra Slack, Amazon Chime, un webhook personalizzato o Amazon SNS. Come si può immaginare, le notifiche richiedono connettività al canale. Ad esempio, il dominio del OpenSearch servizio deve essere in grado di connettersi a Internet per inviare notifiche a un canale Slack o inviare un webhook personalizzato a un server di terze parti. Il webhook personalizzato deve avere un indirizzo IP pubblico per consentire a un dominio di OpenSearch servizio di inviargli avvisi.

> **Tip**
>
> Dopo che un'operazione ha inviato correttamente un messaggio, è responsabilità dell'utente proteggere l'accesso a tale messaggio (ad esempio, l'accesso a un canale Slack). Se il dominio contiene dati sensibili, considerare l'utilizzo di trigger senza operazioni e verificare periodicamente la presenza di avvisi in Dashboards.

Notifiche

Alerting si integra con Notifications, un sistema unificato per le notifiche. OpenSearch Notifications consente di configurare il servizio di comunicazione che si desidera utilizzare e di visualizzare le statistiche pertinenti oltre alle informazioni sulla risoluzione dei problemi. Per una documentazione completa, consulta Notifiche nella documentazione. OpenSearch

Per utilizzare le notifiche, sul tuo dominio deve essere installata la OpenSearch versione 2.3 o successiva.

> **Note**
>
> OpenSearch le notifiche sono distinte dalle notifiche di OpenSearch servizio, che forniscono dettagli sugli aggiornamenti del software di servizio, sui miglioramenti di Auto-Tune e altre importanti informazioni a livello di dominio. OpenSearch le notifiche sono specifiche del plug-in.

I canali di notifica hanno sostituito le destinazioni di avviso a partire OpenSearch dalla versione 2.0. Le destinazioni sono ufficialmente divenute obsolete e in futuro tutte le notifiche di avviso verranno gestite attraverso i canali.

Quando aggiorni i tuoi domini alla versione 2.3 o successiva (poiché il supporto del OpenSearch servizio per la versione 2.x inizia con la versione 2.3), le destinazioni esistenti vengono migrate automaticamente ai canali di notifica. Se una destinazione non riesce a migrare, il monitor continuerà a utilizzarla fino alla migrazione del monitor su un canale di notifica. Per ulteriori informazioni, consulta Domande sulle destinazioni nella documentazione. OpenSearch

Per iniziare a usare le notifiche, accedi alle OpenSearch dashboard e scegli Notifiche, Canali e Crea canale.

Amazon Simple Notification Service (Amazon SNS) è un tipo di canale supportato per le notifiche. Per autenticare gli utenti, è necessario fornire all'utente l'accesso completo ad Amazon SNS oppure lasciare che assuma un ruolo IAM munito delle autorizzazioni per accedere ad Amazon SNS. Per istruzioni, consulta la sezione Amazon SNS come tipo di canale.

Differenze

Rispetto alla versione open source di OpenSearch, gli avvisi in Amazon OpenSearch Service presentano alcune differenze notevoli.

Impostazioni degli avvisi

OpenSearch Il servizio consente di modificare le seguenti impostazioni di avviso:

- `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`

Tutte le altre impostazioni utilizzano i valori di default che non è possibile modificare.

Per disattivare gli avvisi, inviare la seguente richiesta:

```
PUT _cluster/settings
{
  "persistent" : {
    "plugins.scheduled_jobs.enabled" : false
  }
}
```

La richiesta seguente configura gli avvisi per eliminare automaticamente gli indici della cronologia dopo sette giorni, anziché i 30 giorni predefiniti:

```
PUT _cluster/settings
{
  "persistent": {
    "plugins.alerting.alert_history_retention_period": "7d"
  }
}
```

Se hai creato dei monitor in precedenza e desideri interrompere la creazione di indici di avviso giornalieri, elimina tutti gli indici della cronologia degli avvisi:

```
DELETE .plugins-alerting-alert-history-*
```

Per ridurre il numero di frammenti per gli indici cronologici, crea un modello di indice. La richiesta seguente imposta gli indici della cronologia per gli avvisi a una sola partizione e una sola replica:

```
PUT _index_template/template-name
{
  "index_patterns": [".opendistro-alerting-alert-history-*"],
  "template": {
    "settings": {
      "number_of_shards": 1,
      "number_of_replicas": 1
    }
  }
}
```

A seconda della tolleranza per la perdita di dati, si potrebbe anche prendere in considerazione l'utilizzo di repliche zero. Per ulteriori informazioni sulla creazione e la gestione dei modelli di indice, consulta Modelli di indice nella documentazione. OpenSearch

Rilevamento di anomalie in Amazon Service OpenSearch

Il rilevamento delle anomalie in Amazon OpenSearch Service rileva automaticamente le anomalie nei OpenSearch dati quasi in tempo reale utilizzando l'algoritmo Random Cut Forest (RCF). L'RCF è un algoritmo di machine learning non supervisionato che modella un disegno del flusso di dati in ingresso. L'algoritmo calcola un `anomaly grade` e un valore `confidence score` per ogni punto di dati in ingresso. Il rilevamento delle anomalie utilizza questi valori per differenziare un'anomalia dalle normali variazioni dei dati.

Puoi associare il plug-in di rilevamento delle anomalie al plug-in Alerting per avvisarti non appena viene rilevata un'anomalia.

Il rilevamento delle anomalie è disponibile nei domini che eseguono qualsiasi OpenSearch versione di Elasticsearch 7.4 o versione successiva. Tutti i tipi di istanza, tranne `t2.micro` e `t2.small`, supportano il rilevamento delle anomalie.

> **Note**
>
> Questa documentazione fornisce una breve panoramica del rilevamento delle anomalie nel contesto di Amazon OpenSearch Service. Per una documentazione completa, che include passaggi dettagliati, un riferimento all'API, un riferimento a tutte le impostazioni disponibili e i

passaggi per creare visualizzazioni e dashboard, consulta il rilevamento delle anomalie nella documentazione open source. OpenSearch

Prerequisiti

Il rilevamento delle anomalie ha i seguenti requisiti preliminari:

- Il rilevamento delle anomalie richiede Elasticsearch 7.4 OpenSearch o versione successiva.
- Il rilevamento delle anomalie supporta il controllo granulare degli accessi solo sulle versioni 7.9 e successive di Elasticsearch e su tutte le versioni di. OpenSearch Prima di Elasticsearch 7.9, solo gli utenti amministratori potevano creare, visualizzare e gestire i rilevatori.
- Se il tuo dominio utilizza un controllo granulare degli accessi, gli utenti non amministratori devono essere mappati al `anomaly_read_access` ruolo nelle OpenSearch dashboard per visualizzare i rilevatori o per creare e gestire i rilevatori. `anomaly_full_access`

Nozioni di base sul rilevamento di anomalie

Per iniziare, scegli Anomaly Detection in Dashboards. OpenSearch

Fase 1: Creazione di un rilevatore

Un rivelatore è un'attività individuale di rilevamento delle anomalie. È possibile creare più rilevatori, e tutti possono essere eseguiti simultaneamente. Ogni rilevatore analizza i dati provenienti da origini diverse.

Fase 2: Aggiunta di caratteristiche al rilevatore

Una caratteristica è il campo nell'indice che viene controllato per la presenza di anomalie. Un rilevatore può rilevare anomalie in una o più caratteristiche. È necessario scegliere una delle seguenti aggregazioni per ogni funzionalità: `average()`, `sum()`, `count()`, `min()` o `max()`.

> **Note**
>
> Il metodo di `count()` aggregazione è disponibile solo in Elasticsearch OpenSearch 7.7 o versioni successive. Per Elasticsearch 7.4, utilizzare un'espressione personalizzata come la seguente:

```
{
  "aggregation_name": {
     "value_count": {
        "field": "field_name"
     }
  }
}
```

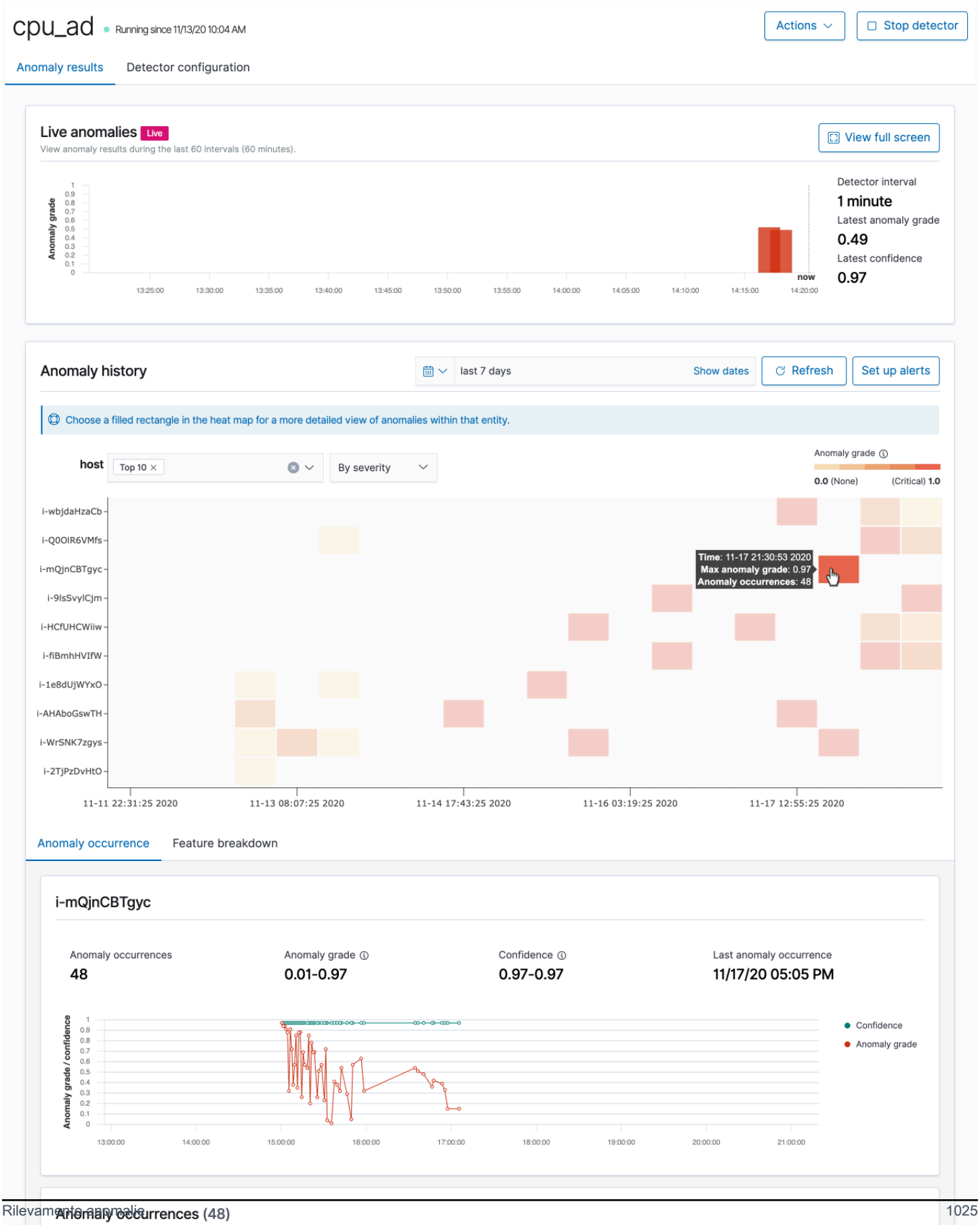
Il metodo di aggregazione determina ciò che costituisce un'anomalia. Ad esempio, se si sceglie `min()`, il rilevatore si concentra sulla ricerca di anomalie in base ai valori minimi della caratteristica. Se si sceglie `average()`, il rilevatore rileva anomalie in base ai valori medi della caratteristica. È possibile aggiungere un massimo di cinque caratteristiche per ogni rilevatore.

È possibile configurare le seguenti impostazioni facoltative (disponibili in Elasticsearch 7.7 e versioni successive):

- Campo Categoria: categorizzare o suddividere i dati con una dimensione come indirizzo IP, ID prodotto, codice paese e così via.
- Dimensione finestra: impostare il numero di intervalli di aggregazione dal flusso dei dati da considerare in una finestra di rilevamento.

Dopo aver configurato le funzioni, visualizzare in anteprima le anomalie dei campioni e, se necessario, regolare le impostazioni delle funzioni.

Fase 3: Osservazione dei risultati



- Anomalie in tempo reale visualizza i risultati delle anomalie in tempo reale per gli ultimi 60 intervalli. Ad esempio, se l'intervallo è impostato su 10, vengono visualizzati i risultati degli ultimi 600 minuti. Questo grafico viene aggiornato ogni 30 secondi.
- Cronologia delle anomalie traccia il grado di anomalia con il corrispondente livello di attendibilità.
- Il grafico Suddivisione delle caratteristiche traccia le caratteristiche in base al metodo di aggregazione. È possibile variare l'intervallo di data-ora del rilevatore.
- Occorrenze delle anomalie mostra `Start time`, `End time`, `Data confidence` e `Anomaly grade` per ogni anomalia rilevata.

  Se si imposta il campo della categoria, viene visualizzato una ulteriore mappa di calore che correla i risultati per le entità anomale. Scegliere un rettangolo pieno per visualizzare una vista più dettagliata dell'anomalia.

Fase 4: Configurazione degli avvisi

Per creare un monitoraggio per inviare notifiche quando vengono rilevate anomalie, scegliere Configura avvisi. Il plug-in reindirizza alla pagina Aggiungi monitor dove è possibile configurare un avviso.

Tutorial: Rileva un elevato utilizzo della CPU con il rilevamento delle anomalie

Questo tutorial dimostra come creare un rilevatore di anomalie in Amazon OpenSearch Service per rilevare un elevato utilizzo della CPU. Utilizzerai OpenSearch le dashboard per configurare un rilevatore per monitorare l'utilizzo della CPU e generare un avviso quando l'utilizzo della CPU supera una soglia specificata.

> **Note**
>
> Questi passaggi si applicano alla versione più recente di OpenSearch e potrebbero differire leggermente per le versioni precedenti.

Prerequisiti

- È necessario disporre di un dominio OpenSearch di servizio che esegue Elasticsearch 7.4 o versione successiva o qualsiasi versione. OpenSearch

- È necessario importare file di registro dell'applicazione nel cluster che contengono dati sull'utilizzo della CPU.

Fase 1: Creazione di un rilevatore

Innanzitutto, crea un rilevatore che identifichi le anomalie nei dati di utilizzo della CPU.

1. Apri il menu del pannello di sinistra in OpenSearch Dashboards e scegli Anomaly Detection, quindi scegli Crea rilevatore.
2. Assegna un nome al rilevatore **`high-cpu-usage`**.
3. Per l'origine dei dati, scegli il tuo indice che contiene i file di registro dell'utilizzo della CPU in cui desideri identificare le anomalie.
4. Seleziona Campo timestamp dai tuoi dati. Facoltativamente, puoi aggiungere un filtro dati. Questo filtro dati analizza solo un sottoinsieme dell'origine dati e riduce il rumore derivante da dati non rilevanti.
5. Impostazione della proprietà Intervallo del rilevatore a 2 minuti. Questo intervallo definisce il tempo (per intervallo di minuti) entro il quale il rilevatore raccoglie i dati.
6. Nello stato Ritardo di finestra, aggiungi un ritardo di 1 minuto. Questo ritardo aggiunge ulteriore tempo di elaborazione per garantire che tutti i dati all'interno della finestra siano presenti.
7. Seleziona Successivo. Nella dashboard di rilevamento delle anomalie, sotto il nome del rilevatore, selezionare Configura modello.
8. Per Nome caratteristica, digita **`max_cpu_usage`**. Per Stato della caratteristica, seleziona Attiva funzionalità.
9. Per Individuazione delle anomalie in base a , scegli Valore campo.
10. Per Metodo di aggregazione, scegli **`max()`**.
11. Per Campo, seleziona il campo nei dati per verificare la presenza di anomalie. Ad esempio, potrebbe essere chiamato `cpu_usage_percentage`.
12. Mantenere tutte le altre impostazioni come valori predefiniti e scegliere Successivo.
13. Ignorare la configurazione dei lavori del rilevatore e scegliere Successivo.
14. Nella finestra popup, scegliere quando avviare il rilevatore (automaticamente o manualmente), quindi scegliere Confermare.

Ora che il rilevatore è configurato, dopo l'inizializzazione, sarà possibile visualizzare i risultati in tempo reale dell'utilizzo della CPU nella sezione Risultati in tempo reale del rilevatore. La sezione

Anomalie dal vivo mostra tutte le anomalie che si verificano quando i dati vengono inseriti in tempo reale.

Fase 2: configura un avviso

Ora che hai creato un rilevatore, crea un monitor che richiami un avviso per inviare un messaggio a Slack quando rileva un utilizzo della CPU che soddisfa le condizioni specificate nelle impostazioni del rilevatore. Riceverai notifiche di Slack quando i dati di uno o più indici soddisfano le condizioni che richiamano l'avviso.

1. Apri il menu del pannello di sinistra in OpenSearch Dashboards e scegli Avvisi, quindi scegli Crea monitor.
2. Fornire un nome per il nome del monitor.
3. Per Tipo di monitoraggio, scegli Monitoraggio per query. Un monitor per query esegue una query specificata e definisce i trigger.
4. Per Metodo di definizione del monitor, scegli Rilevatore di anomalie, quindi selezionare il rilevatore creato nella sezione precedente dal menu a discesa Rilevatore.
5. Per Pianificazione, scegliere la frequenza con cui il monitor raccoglie i dati e la frequenza con cui si ricevono gli avvisi. Ai fini del presente tutorial, imposta la pianificazione per l'esecuzione di 7minuti.
6. Nella sezione Trigger, scegli Aggiungi trigger. Per Nome trigger, digita **`High CPU usage`**. Per questo tutorial, per Livello di gravità, scegli 1, che è il livello di gravità più alto.
7. Per Soglia di anomalie, scegli È SOPRA. Nel menu sottostante, scegli la soglia da applicare. Per questo tutorial, imposta il Grado di anomalie a 0.7.
8. Per Soglia di confidenza anomalie, scegli È SOPRA. Nel menu sottostante, inserisci lo stesso numero del tuo grado di anomalia. Per questo tutorial, imposta Soglia di confidenza anomalie a 0.7.
9. Nella sezione Operazioni, scegli Destinazione. Nel campo Nome, scegliere il nome della destinazione. Sul menu Tipo, scegli Margine di flessibilità. Nel campo Webhook URL, immettere un URL del webhook a cui ricevere gli avvisi. Per ulteriori informazioni, consulta Invio di messaggi tramite webhook in entrata.
10. Scegli Crea.

Risorse correlate

- the section called “Avviso”

- the section called “Rilevamento anomalie”
- API di rilevamento delle anomalie

Apprendimento automatico per Amazon OpenSearch Service

ML Commons è un OpenSearch plug-in che fornisce una serie di algoritmi di machine learning (ML) comuni tramite il trasporto e le chiamate API REST. Queste chiamate scelgono i nodi e le risorse giusti per ogni richiesta ML e monitorano le attività ML per garantire l'operatività. Ciò consente di sfruttare gli algoritmi ML open source esistenti e di ridurre lo sforzo richiesto per sviluppare nuove funzionalità di machine learning. Per ulteriori informazioni sul plug-in, consulta Machine learning nella documentazione. OpenSearch Questo capitolo spiega come utilizzare il plug-in con Amazon OpenSearch Service.

Argomenti

Connettori Amazon OpenSearch Service ML per Servizi AWS

Quando utilizzi connettori di apprendimento automatico (ML) di Amazon OpenSearch Service con un altro Servizio AWS, devi configurare un ruolo IAM per connettere in modo sicuro OpenSearch Service a quel servizio. Servizi AWS che puoi configurare un connettore per includere Amazon SageMaker e Amazon Bedrock. In questo tutorial, spieghiamo come creare un connettore da OpenSearch Service a SageMaker Runtime. Per ulteriori informazioni sui connettori, consulta Connettori supportati.

Argomenti

Prerequisiti

Per creare un connettore, devi disporre di un endpoint Amazon SageMaker Domain e di un ruolo IAM che conceda l'accesso OpenSearch al servizio.

Configura un SageMaker dominio Amazon

Consulta Deploy a Model in Amazon SageMaker nell'Amazon SageMaker Developer Guide per distribuire il tuo modello di machine learning. Prendi nota dell'URL dell'endpoint per il tuo modello, di cui hai bisogno per creare un connettore AI.

Creazione di un ruolo IAM

Imposta un ruolo IAM per delegare le autorizzazioni SageMaker di Runtime a Service. OpenSearch Per creare un nuovo ruolo, consulta Creating an IAM role (console) nella IAM User Guide. Facoltativamente, puoi utilizzare un ruolo esistente purché abbia lo stesso set di privilegi. Se crei un nuovo ruolo invece di usare un ruolo AWS gestito, sostituiscilo `opensearch-sagemaker-role` in questo tutorial con il nome del tuo ruolo.

1. Allega la seguente policy IAM gestita al tuo nuovo ruolo per consentire a OpenSearch Service di accedere al tuo SageMaker endpoint. Per allegare una policy a un ruolo, consulta Aggiungere i permessi di identità IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:InvokeEndpointAsync",
                "sagemaker:InvokeEndpoint"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. Segui le istruzioni riportate in Modifica della politica di fiducia di un ruolo per modificare la relazione di trust del ruolo. È necessario specificare OpenSearch Service nella `Principal` dichiarazione:

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

```
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "opensearchservice.amazonaws.com"
                ]
            }
        }
    ]
}
```

Ti consigliamo di utilizzare i tasti `aws:SourceAccount` e `aws:SourceArn` condition per limitare l'accesso a un dominio specifico. `SourceAccount`è l' Account AWS ID che appartiene al proprietario del dominio e il `SourceArn` è l'ARN del dominio. Ad esempio, puoi aggiungere il seguente blocco di condizioni alla politica di fiducia:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Configurazione delle autorizzazioni

Per creare il connettore, è necessaria l'autorizzazione per passare il ruolo IAM a OpenSearch Service. Devi inoltre disporre dell'accesso all'operazione `es:ESHttpPost`. Per concedere entrambe queste autorizzazioni, collega la policy seguente al ruolo IAM le cui credenziali vengono utilizzate per firmare la richiesta:

```
{
  "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/*"
    }
  ]
}
```

Se il tuo utente o ruolo non dispone `iam:PassRole` delle autorizzazioni per trasferire il ruolo, potresti riscontrare un errore di autorizzazione quando tenti di registrare un repository nel passaggio successivo.

Mappa il ruolo ML nelle OpenSearch dashboard (se utilizzi un controllo di accesso granulare)

Il controllo granulare degli accessi introduce un passaggio aggiuntivo per la configurazione di un connettore. Anche se si utilizza l'autenticazione di base HTTP per tutti gli altri scopi, è necessario mappare il ruolo `ml_full_access` al ruolo IAM che dispone delle autorizzazioni `iam:PassRole` per inviare `opensearch-sagemaker-role`.

1. Vai al plug-in OpenSearch Dashboards per il tuo dominio di servizio. OpenSearch Puoi trovare l'endpoint Dashboards nella dashboard del tuo dominio nella OpenSearch console di servizio.
2. Dal menu principale scegli Sicurezza, Ruoli e seleziona il ruolo ml_full_access.
3. Scegliere Utenti mappati, Gestisci mappatura.
4. In Ruoli di backend, aggiungi l'ARN del ruolo che ha le autorizzazioni da passare. `opensearch-sagemaker-role`

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Selezionare Mappa e confermare che l'utente o il ruolo venga visualizzato in Utenti mappati.

Crea un connettore di servizio OpenSearch

Per creare un connettore, invia una `POST` richiesta all'endpoint del dominio di OpenSearch servizio. Puoi usare curl, il client Python di esempio, Postman o un altro metodo per inviare una richiesta firmata. Nota che non puoi usare una `POST` richiesta nella console Kibana. La richiesta ha il seguente 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}\" } }"
      }
   ]
}
```

Se il dominio risiede all'interno di un cloud privato virtuale (VPC), il computer deve essere connesso al VPC affinché la richiesta crei correttamente il connettore AI. L'accesso a un VPC varia in base alla configurazione di rete, ma di solito comporta la connessione a una VPN o a una rete aziendale. Per verificare di poter accedere al dominio del OpenSearch servizio, accedi a `https://your-vpc-domain.region.es.amazonaws.com` In un browser Web e verifica di ricevere la risposta JSON predefinita.

Client Python di esempio

Il client Python è più semplice da automatizzare rispetto a una richiesta HTTP e ha una migliore riusabilità. Per creare il connettore AI con il client Python, salva il seguente codice di esempio in un file Python. Il client richiede i pacchetti AWS SDK for Python (Boto3)`requests`, e `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)
```

Connettori Amazon OpenSearch Service ML per piattaforme di terze parti

In questo tutorial, spieghiamo come creare un connettore da OpenSearch Service a Cohere. Per ulteriori informazioni sui connettori, consulta Connettori supportati.

Quando utilizzi un connettore di apprendimento automatico (ML) di Amazon OpenSearch Service con un modello remoto esterno, devi memorizzare le tue credenziali di autorizzazione specifiche in AWS Secrets Manager. Potrebbe trattarsi di una chiave API o di una combinazione di nome utente e password. Ciò significa che devi anche creare un ruolo IAM che consenta l'accesso al OpenSearch servizio per la lettura da Secrets Manager.

Argomenti

Prerequisiti

Per creare un connettore per Cohere o per qualsiasi provider esterno con OpenSearch Service, devi disporre di un ruolo IAM che conceda l'accesso al OpenSearch Servizio AWS Secrets Manager, a cui archiviare le tue credenziali. È inoltre necessario memorizzare le credenziali in Secrets Manager.

Creazione di un ruolo IAM

Imposta un ruolo IAM per delegare le autorizzazioni di Secrets Manager a OpenSearch Service. Puoi anche utilizzare il ruolo esistente`SecretManagerReadWrite`. Per creare un nuovo ruolo, consulta Creating an IAM role (console) nella IAM User Guide. Se crei un nuovo ruolo invece di utilizzare un ruolo AWS gestito, `opensearch-secretmanager-role` sostituiscilo in questo tutorial con il nome del tuo ruolo.

1. Allega la seguente policy IAM gestita al tuo nuovo ruolo per consentire a OpenSearch Service di accedere ai tuoi valori di Secrets Manager. Per allegare una policy a un ruolo, consulta Aggiungere autorizzazioni di identità IAM.

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

2. Segui le istruzioni riportate in Modifica della politica di fiducia di un ruolo per modificare la relazione di trust del ruolo. È necessario specificare OpenSearch Service nella `Principal` dichiarazione:

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

Ti consigliamo di utilizzare i tasti `aws:SourceAccount` e `aws:SourceArn` condition per limitare l'accesso a un dominio specifico. `SourceAccount`è l' Account AWS ID che appartiene al proprietario del dominio e il `SourceArn` è l'ARN del dominio. Ad esempio, puoi aggiungere il seguente blocco di condizioni alla politica di fiducia:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
```

```
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Configurazione delle autorizzazioni

Per creare il connettore, è necessaria l'autorizzazione per passare il ruolo IAM a OpenSearch Service. Devi inoltre disporre dell'accesso all'operazione `es:ESHttpPost`. Per concedere entrambe queste autorizzazioni, collega la policy seguente al ruolo IAM le cui credenziali vengono utilizzate per firmare la richiesta:

```
{
  "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/*"
    }
  ]
}
```

Se il tuo utente o ruolo non dispone `iam:PassRole` delle autorizzazioni per trasferire il ruolo, potresti riscontrare un errore di autorizzazione quando tenti di registrare un repository nel passaggio successivo.

Configurare AWS Secrets Manager

Per memorizzare le credenziali di autorizzazione in Secrets Manager, consulta Creare un AWS Secrets Manager segreto nella Guida per l'AWS Secrets Manager utente.

Dopo che Secrets Manager ha accettato la coppia chiave-valore come segreta, riceverai un ARN con il formato:. `arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-`

`a1b2c3` Tieni traccia di questo ARN, così come lo usi, e della tua chiave quando crei un connettore nel passaggio successivo.

Mappa il ruolo ML nelle OpenSearch dashboard (se utilizzi un controllo degli accessi granulare)

Il controllo granulare degli accessi introduce un passaggio aggiuntivo per la configurazione di un connettore. Anche se si utilizza l'autenticazione di base HTTP per tutti gli altri scopi, è necessario mappare il ruolo `ml_full_access` al ruolo IAM che dispone delle autorizzazioni `iam:PassRole` per inviare `opensearch-sagemaker-role`.

1. Vai al plug-in OpenSearch Dashboards per il tuo dominio di servizio. OpenSearch Puoi trovare l'endpoint Dashboards nella dashboard del tuo dominio nella OpenSearch console di servizio.
2. Dal menu principale scegli Sicurezza, Ruoli e seleziona il ruolo ml_full_access.
3. Scegliere Utenti mappati, Gestisci mappatura.
4. In Ruoli di backend, aggiungi l'ARN del ruolo che ha le autorizzazioni da passare. `opensearch-sagemaker-role`

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Selezionare Mappa e confermare che l'utente o il ruolo venga visualizzato in Utenti mappati.

Crea un connettore di servizio OpenSearch

Per creare un connettore, invia una `POST` richiesta all'endpoint del dominio di OpenSearch servizio. Puoi usare curl, il client Python di esempio, Postman o un altro metodo per inviare una richiesta firmata. Nota che non puoi usare una `POST` richiesta nella console Kibana. La richiesta ha il seguente 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\" }"
        }
    ]
}
```

Il corpo della richiesta per questa richiesta è diverso da quello di una richiesta di connettore open source in due modi. All'interno del `credential` campo, si passa l'ARN per il ruolo IAM che consente a OpenSearch Service di leggere da Secrets Manager, insieme all'ARN per il segreto what. Nel `headers` campo, si fa riferimento al segreto utilizzando la chiave segreta e al fatto che proviene da un ARN.

Se il tuo dominio risiede all'interno di un cloud privato virtuale (VPC), il tuo computer deve essere connesso al VPC affinché la richiesta crei correttamente il connettore AI. L'accesso a un VPC varia in base alla configurazione di rete, ma di solito comporta la connessione a una VPN o a una rete aziendale. Per verificare di poter accedere al dominio del OpenSearch servizio, accedi a `https://your-vpc-domain.region.es.amazonaws.com` In un browser Web e verifica di ricevere la risposta JSON predefinita.

Client Python di esempio

Il client Python è più semplice da automatizzare rispetto a una richiesta HTTP e ha una migliore riusabilità. Per creare il connettore AI con il client Python, salva il seguente codice di esempio in un file Python. Il client richiede i pacchetti AWS SDK for Python (Boto3)`requests`, e `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)
```

Utilizzo AWS CloudFormation per configurare l'inferenza remota per la ricerca semantica

A partire dalla OpenSearch versione 2.9, puoi utilizzare l'inferenza remota con la ricerca semantica per ospitare i tuoi modelli di machine learning (ML). L'inferenza remota utilizza il plug-in ML

Commons per consentirti di ospitare le inferenze del modello in remoto su servizi ML, come e Amazon SageMaker Amazon BedRock, e collegarli ad Amazon OpenSearch Service con connettori ML.

Per facilitare la configurazione dell'inferenza remota, Amazon OpenSearch Service fornisce un AWS CloudFormationmodello nella console. CloudFormation è un software Servizio AWS che consente di modellare, fornire AWS e gestire risorse di terze parti trattando l'infrastruttura come codice.

Il OpenSearch CloudFormation modello automatizza il processo di provisioning del modello per te, in modo che tu possa creare facilmente un modello nel tuo dominio di OpenSearch servizio e quindi utilizzare l'ID del modello per importare dati ed eseguire query di ricerca neurali.

Quando utilizzi codificatori neurali sparsi con la versione 2.12 e successive del OpenSearch servizio, ti consigliamo di utilizzare il modello tokenizer localmente anziché distribuirlo in remoto. Per ulteriori informazioni, consulta i modelli di codifica Sparse nella documentazione. OpenSearch

Argomenti

Prerequisiti

Per utilizzare un CloudFormation modello con OpenSearch Service, completa i seguenti prerequisiti.

Configura un dominio di OpenSearch servizio

Prima di poter utilizzare un CloudFormation modello, devi configurare un dominio Amazon OpenSearch Service con la versione 2.9 o successiva e il controllo granulare degli accessi abilitato. Crea un ruolo OpenSearch di backend del servizio per autorizzare il plug-in ML Commons a creare il connettore per te.

Il CloudFormation modello crea per te un ruolo Lambda IAM con il nome predefinito`LambdaInvokeOpenSearchMLCommonsRole`, che puoi sostituire se desideri scegliere un nome diverso. Dopo che il modello ha creato questo ruolo IAM, devi autorizzare la funzione Lambda a chiamare il tuo dominio di OpenSearch servizio. Per farlo, associa il ruolo denominato `ml_full_access` al tuo ruolo di backend OpenSearch Service con i seguenti passaggi:

1. Vai al plug-in OpenSearch Dashboards per il tuo dominio di OpenSearch servizio. Puoi trovare l'endpoint Dashboards nella dashboard del tuo dominio nella OpenSearch console di servizio.
2. Dal menu principale scegli Sicurezza, Ruoli e seleziona il ruolo ml_full_access.
3. Scegliere Utenti mappati, Gestisci mappatura.
4. In Ruoli di backend, aggiungi l'ARN del ruolo Lambda che richiede l'autorizzazione per chiamare il tuo dominio.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Selezionare Mappa e confermare che l'utente o il ruolo venga visualizzato in Utenti mappati.

Dopo aver mappato il ruolo, vai alla configurazione di sicurezza del tuo dominio e aggiungi il ruolo Lambda IAM alla OpenSearch tua policy di accesso al servizio.

Abilita le autorizzazioni sul tuo Account AWS

Account AWS Devi disporre dell'autorizzazione all'accesso CloudFormation e alla tecnologia Lambda, oltre a quello che Servizio AWS scegli per il modello, che sia Runtime SageMaker o Amazon. BedRock

Se utilizzi Amazon Bedrock, devi anche registrare il tuo modello. Consulta Model access nella Amazon Bedrock User Guide per registrare il tuo modello.

Se utilizzi il tuo bucket Amazon S3 per fornire artefatti del modello, devi aggiungere il ruolo CloudFormation IAM alla tua policy di accesso S3. Per ulteriori informazioni, consulta Aggiunta e rimozione di autorizzazioni per identità IAM nella Guida per l'utente di IAM .

Amazon SageMaker modelli

I SageMaker CloudFormation modelli Amazon definiscono più AWS risorse per configurare il plug-in neurale e la ricerca semantica per te.

Innanzitutto, utilizza il modello Integrazione con modelli di incorporamento del testo tramite Amazon per distribuire un SageMaker modello di incorporamento di testo in SageMaker Runtime come server. Se non fornisci un endpoint modello, CloudFormation crea un ruolo IAM che consente a SageMaker Runtime di scaricare gli artefatti del modello da Amazon S3 e distribuirli sul server. Se fornisci un endpoint, CloudFormation crea un ruolo IAM che consente alla funzione Lambda di accedere al dominio OpenSearch del servizio o, se il ruolo esiste già, aggiorna e riutilizza il ruolo. L'endpoint serve il modello remoto utilizzato per il connettore ML con il plug-in ML Commons.

Successivamente, utilizza il modello Integration with Sparse Encoders through Amazon Sagemaker per creare una funzione Lambda che consenta al dominio di configurare connettori di inferenza remoti. Dopo aver creato il connettore in OpenSearch Service, l'inferenza remota può eseguire una ricerca semantica utilizzando il modello remoto in Runtime. SageMaker Il modello ti restituisce l'ID del modello nel tuo dominio in modo che tu possa iniziare la ricerca.

Per utilizzare i SageMaker CloudFormation modelli Amazon

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nella barra di navigazione a sinistra, scegli Integrazioni.
3. In ciascuno dei SageMaker modelli Amazon, scegli Configura dominio, Configura dominio pubblico.
4. Segui le istruzioni nella CloudFormation console per effettuare il provisioning dello stack e configurare un modello.

> **Note**
>
> OpenSearch Il servizio fornisce anche un modello separato per configurare il dominio VPC. Se utilizzi questo modello, devi fornire l'ID VPC per la funzione Lambda.

Modelli Amazon Bedrock

Analogamente ai SageMaker CloudFormation modelli Amazon, il CloudFormation modello Amazon Bedrock fornisce le AWS risorse necessarie per creare connettori tra OpenSearch Service e Amazon Bedrock.

Innanzitutto, il modello crea un ruolo IAM che consente alla futura funzione Lambda di accedere al dominio del OpenSearch servizio. Il modello crea quindi la funzione Lambda, che consente al dominio di creare un connettore utilizzando il plug-in ML Commons. Dopo che OpenSearch Service ha creato il connettore, la configurazione dell'inferenza remota è terminata e puoi eseguire ricerche semantiche utilizzando le operazioni dell'API Amazon Bedrock.

Tieni presente che, poiché Amazon Bedrock ospita i propri modelli di machine learning, non è necessario distribuire un modello in Runtime. SageMaker Il modello utilizza invece un endpoint predeterminato per Amazon Bedrock e salta le fasi di fornitura degli endpoint.

Per utilizzare il modello Amazon Bedrock CloudFormation

1. Apri la console Amazon OpenSearch Service all'indirizzo https://console.aws.amazon.com/aos/home.
2. Nella barra di navigazione a sinistra, scegli Integrazioni.
3. Nella sezione Integrazione con il modello Amazon Titan Text Embeddings tramite Amazon Bedrock, scegli Configura dominio, Configura dominio pubblico.
4. Segui le istruzioni per configurare il tuo modello.

> **Note**
>
> OpenSearch Il servizio fornisce anche un modello separato per configurare il dominio VPC. Se utilizzi questo modello, devi fornire l'ID VPC per la funzione Lambda.

Inoltre, OpenSearch Service fornisce i seguenti modelli Amazon Bedrock per connettersi al modello Cohere e al modello di incorporamenti multimodali Amazon Titan:

- `Integration with Cohere Embed through Amazon Bedrock`
- `Integrate with Amazon Bedrock Titan Multi-modal`

Impostazioni ML Commons non supportate

Amazon OpenSearch Service non supporta l'uso delle seguenti impostazioni ML Commons:

- `plugins.ml_commons.allow_registering_model_via_url`
- `plugins.ml_commons.allow_registering_model_via_local_file`

Per ulteriori informazioni sulle impostazioni del cluster ML Commons, consulta le impostazioni del cluster ML Commons.

OpenSearch Modelli di framework di flussi di servizio

I modelli di framework di flusso di Amazon OpenSearch Service consentono di automatizzare attività complesse di configurazione e preelaborazione del OpenSearch servizio fornendo modelli per

casi d'uso comuni. Ad esempio, puoi utilizzare i modelli di Flow Framework per automatizzare le attività di configurazione dell'apprendimento automatico. I modelli di framework di flusso di Amazon OpenSearch Service forniscono una descrizione compatta del processo di configurazione in un documento JSON o YAML. Questi modelli descrivono configurazioni automatizzate di flussi di lavoro per chat conversazionali o generazione di query, connettori AI, strumenti, agenti e altri componenti che preparano OpenSearch Service per l'uso in backend per modelli generativi.

I modelli di framework di flusso di Amazon OpenSearch Service possono essere personalizzati per soddisfare esigenze specifiche. Per vedere un esempio di modello di framework di flusso personalizzato, consulta flow-framework. Per i modelli forniti dal OpenSearch servizio, consulta workflow-templates. Per una documentazione completa, che include passaggi dettagliati, un riferimento all'API e un riferimento a tutte le impostazioni disponibili, vedi Automating Configuration nella documentazione open source. OpenSearch

Creazione di connettori ML in Service OpenSearch

I modelli di framework di flusso di Amazon OpenSearch Service consentono di configurare e installare connettori ML utilizzando l'API create connector offerta in ml-commons. Puoi utilizzare i connettori ML per connettere OpenSearch Service ad altri AWS servizi o piattaforme di terze parti. Per ulteriori informazioni su questo argomento, consulta Creazione di connettori per piattaforme ML di terze parti. L'API del framework di flusso di Amazon OpenSearch Service consente di automatizzare le attività di configurazione e preelaborazione del OpenSearch servizio e può essere utilizzata per creare connettori ML.

Prima di poter creare un connettore in OpenSearch Service, devi fare quanto segue:

- Crea un SageMaker dominio Amazon.
- Crea un ruolo IAM.
- Configura l'autorizzazione al pass role.
- Mappa i ruoli flow-framework e ml-commons nelle dashboard. OpenSearch

Per ulteriori informazioni su come configurare i connettori ML per AWS i servizi, consulta i connettori ML OpenSearch di Amazon Service per AWS i servizi. Per ulteriori informazioni sull'utilizzo dei connettori OpenSearch Service ML con piattaforme di terze parti, consulta Connettori Amazon OpenSearch Service ML per piattaforme di terze parti.

Creazione di un connettore tramite un servizio flow-framework

Per creare un modello di flow-framework con connettore, è necessario inviare una POST richiesta all'endpoint del dominio di servizio. OpenSearch Puoi usare cURL, un client Python di esempio, Postman o un altro metodo per inviare una richiesta firmata. La POST richiesta ha il seguente formato:

```
POST /_plugins/_flow_framework/workflow
{
  "name": "Deploy Claude Model",
  "description": "Deploy a model using a connector to Claude",
  "use_case": "PROVISION",
  "version": {
    "template": "1.0.0",
    "compatibility": [
      "2.12.0",
      "3.0.0"
    ]
  },
  "workflows": {
    "provision": {
      "nodes": [
        {
          "id": "create_claude_connector",
          "type": "create_connector",
          "user_inputs": {
            "name": "Claude Instant Runtime Connector",
            "version": "1",
            "protocol": "aws_sigv4",
            "description": "The connector to BedRock service for Claude model",
            "actions": [
              {
                "headers": {
                  "x-amz-content-sha256": "required",
                  "content-type": "application/json"
                },
                "method": "POST",
                "request_body": "{ \"prompt\":\"${parameters.prompt}\",
 \"max_tokens_to_sample\":${parameters.max_tokens_to_sample},
 \"temperature\":${parameters.temperature},  \"anthropic_version\":
\"${parameters.anthropic_version}\" }",
                "action_type": "predict",
```

```
                "url": "https://bedrock-runtime.us-west-2.amazonaws.com/model/
anthropic.claude-instant-v1/invoke"
              }
            ],
            "credential": {
                "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-
role"
             },
            "parameters": {
              "endpoint": "bedrock-runtime.us-west-2.amazonaws.com",
              "content_type": "application/json",
              "auth": "Sig_V4",
              "max_tokens_to_sample": "8000",
              "service_name": "bedrock",
              "temperature": "0.0001",
              "response_filter": "$.completion",
              "region": "us-west-2",
              "anthropic_version": "bedrock-2023-05-31"
            }
          }
        }
      ]
    }
  }
}
```

Se il tuo dominio risiede in un cloud privato virtuale (Amazon VPC), devi essere connesso ad Amazon VPC affinché la richiesta crei correttamente il connettore AI. L'accesso a un Amazon VPC varia in base alla configurazione di rete, ma di solito comporta la connessione a una VPN o a una rete aziendale. Per verificare di poter accedere al dominio del OpenSearch servizio, accedi a `https://your-vpc-domain.region.es.amazonaws.com` In un browser Web e verifica di ricevere la risposta JSON predefinita.

Client Python di esempio

Il client Python è più semplice da automatizzare rispetto a una HTTP richiesta e ha una migliore riusabilità. Per creare il connettore AI con il client Python, salva il seguente codice di esempio in un file Python. Il client richiede i pacchetti AWS SDK for Python (Boto3), requests:HTTP forHumans e requests-aws4auth 1.2.3.

```
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/_flow_framework/workflow'
url = host + path

payload = {
  "name": "Deploy Claude Model",
  "description": "Deploy a model using a connector to Claude",
  "use_case": "PROVISION",
  "version": {
    "template": "1.0.0",
    "compatibility": [
      "2.12.0",
      "3.0.0"
    ]
  },
  "workflows": {
    "provision": {
      "nodes": [
        {
          "id": "create_claude_connector",
          "type": "create_connector",
          "user_inputs": {
            "name": "Claude Instant Runtime Connector",
            "version": "1",
            "protocol": "aws_sigv4",
            "description": "The connector to BedRock service for Claude model",
            "actions": [
              {
                "headers": {
                  "x-amz-content-sha256": "required",
                  "content-type": "application/json"
                },
                "method": "POST",
                "request_body": "{ \"prompt\":\"${parameters.prompt}\",
 \"max_tokens_to_sample\":${parameters.max_tokens_to_sample},
```

```
 \"temperature\":${parameters.temperature},  \"anthropic_version\":
\"${parameters.anthropic_version}\" }",
                "action_type": "predict",
                "url": "https://bedrock-runtime.us-west-2.amazonaws.com/model/
anthropic.claude-instant-v1/invoke"
              }
            ],
            "credential": {
                "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-
role"
             },
            "parameters": {
              "endpoint": "bedrock-runtime.us-west-2.amazonaws.com",
              "content_type": "application/json",
              "auth": "Sig_V4",
              "max_tokens_to_sample": "8000",
              "service_name": "bedrock",
              "temperature": "0.0001",
              "response_filter": "$.completion",
              "region": "us-west-2",
              "anthropic_version": "bedrock-2023-05-31"
            }
          }
        }
      ]
    }
  }
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Modelli di workflow predefiniti

Amazon OpenSearch Service fornisce diversi modelli di flusso di lavoro per alcuni casi d'uso comuni di machine learning (ML). L'utilizzo di un modello semplifica le configurazioni complesse e fornisce molti valori predefiniti per casi d'uso come la ricerca semantica o conversazionale. È possibile specificare un modello di workflow quando si chiama l'API Create Workflow.

- Per utilizzare un modello di workflow fornito dal OpenSearch servizio, specifica il caso d'uso del modello come parametro di `use_case` interrogazione.
- Per utilizzare un modello di workflow personalizzato, inserisci il modello completo nel corpo della richiesta. Per un esempio di modello personalizzato, vedi un esempio di modello JSON o un modello YAML di esempio.

Casi d'uso del modello

Questa tabella fornisce una panoramica dei diversi modelli disponibili, una descrizione dei modelli e i parametri richiesti.

Caso d'uso del modello	Descrizione	Parametri obbligatori
`bedrock_titan_embedding_model_deploy`	Crea e distribuisce un modello di incorporamento Amazon Bedrock (per impostazione predefinita, `titan-embed-text-v1`	`create_connector.credential.roleArn`
`bedrock_titan_embedding_model_deploy`	Crea e distribuisce un modello di incorporamento multimodale Amazon Bedrock (per impostazione predefinita, `titan-embed-text-v1`	`create_connector.credential.roleArn`
`cohere_embedding_model_deploy`	Crea e distribuisce un modello di incorporamento Cohere (per impostazione predefinita, 3.0). embed-english-v	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`cohere_chat_model_deploy`	Crea e distribuisce un modello di chat Cohere (per impostazione predefinita, Cohere Command).	`create_connector.credential.roleArn` , `create_connector.credential.secretArn`
`open_ai_embedding_`	Crea e distribuisce un modello di incorporamento OpenAI (per impostazione predefinita text-embedding-ada, -002).	`create_connector.credential.roleArn` ,

Caso d'uso del modello	Descrizione	Parametri obbligatori
`model_deploy`		`create_connector.credential.secretArn`
`openai_chat_model_deploy`	Crea e distribuisce un modello di chat OpenAI (per impostazione predefinita, gpt-3.5-turbo).	`create_connector.credential.roleArn`, `create_connector.credential.secretArn`
`semantic_search_with_cohere_embedding`	Configura la ricerca semantica e implementa un modello di incorporamento Cohere. È necessario fornire la chiave API per il modello Cohere.	`create_connector.credential.roleArn`, `create_connector.credential.secretArn`
`semantic_search_with_cohere_embedding_query_enricher`	Configura la ricerca semantica e implementa un modello di incorporamento Cohere. Aggiunge un processore di ricerca query_enricher che imposta un ID modello predefinito per le query neurali. È necessario fornire la chiave API per il modello Cohere.	`create_connector.credential.roleArn`, `create_connector.credential.secretArn`
`multimodal_search_with_bedrock_titan`	Implementa un modello multimodale Amazon Bedrock e configura una pipeline di ingestione con un processore text_image_embedding e un indice k-NN per la ricerca multimodale. Devi AWS fornire le tue credenziali.	`create_connector.credential.roleArn`

> **Note**
>
> Per tutti i modelli che richiedono un ARN segreto, l'impostazione predefinita prevede di memorizzare il segreto con il nome chiave «chiave» nel gestore AWS segreti.

Modelli predefiniti con modelli preaddestrati

Amazon OpenSearch Service offre due modelli di flusso di lavoro predefiniti aggiuntivi non disponibili nel servizio opensource OpenSearch .

Caso d'uso del modello	Descrizione
`semantic_search_with_local_model`	Configura la ricerca semantica e distribuisce un modello preaddestrato (). `msmarco-d istilbert-base-tas-b` Aggiunge un processore `neural_query_enricher` di ricerca che imposta un ID modello predefini to per le query neurali e crea un indice k-NN collegato chiamato ". my-nlp-index
`hybrid_search_with_local_model`	Configura la ricerca ibrida e implementa un modello preaddestrato (). `msmarco-d istilbert-base-tas-b` Aggiunge un processore `neural_query_enricher` di ricerca che imposta un ID modello predefini to per le query neurali e crea un indice k-NN collegato chiamato ". my-nlp-index

Configurazione delle autorizzazioni

Se crei un nuovo dominio con la versione 2.13 o successiva, le autorizzazioni sono già disponibili. Se abiliti il framework di flusso su un dominio di OpenSearch servizio preesistente con la versione 2.11 o precedente e poi esegui l'aggiornamento alla versione 2.13 o successiva, devi definire il ruolo. `flow_framework_manager` Gli utenti senza privilegi di amministratore devono essere mappati a questo ruolo in modo da gestire gli indici a caldo sui domini che utilizzano il controllo granulare degli

accessi. Per creare manualmente il ruolo `flow_framework_manager`, procedere nel seguente modo:

1. In OpenSearch Dashboards, vai su Sicurezza e scegli Autorizzazioni.
2. Scegliere Crea gruppo di operazioni e configurare i seguenti gruppi:

Group name (Nome gruppo)	Autorizzazioni
`flow_framework_full_access`	• `cluster:admin/opensearch/flow_framework/*` • `cluster_monitor`
`flow_framework_read_accesss`	• `cluster:admin/opensearch/flow_framework/workflow/get` • `cluster:admin/opensearch/flow_framework/workflow/search` • `cluster:admin/opensearch/flow_framework/workflow_state/get` • `cluster:admin/opensearch/flow_framework/workflow_state/search`

3. Scegliere Ruoli, quindi selezionare Crea ruolo.
4. Assegna un nome al ruolo flow_framework_manager.
5. Per Autorizzazioni cluster, selezionare `flow_framework_full_access` e `flow_framework_read_access`.
6. Per Indice, digitare `*`.
7. Per Autorizzazioni indice, selezionare `indices:admin/aliases/get`, `indices:admin/mappings/get` e `indices_monitor`.
8. Scegli Crea.
9. Dopo aver creato il ruolo, mappalo a qualsiasi ruolo utente o di backend che gestirà gli indici del framework di flusso.

Analisi di sicurezza per Amazon OpenSearch Service

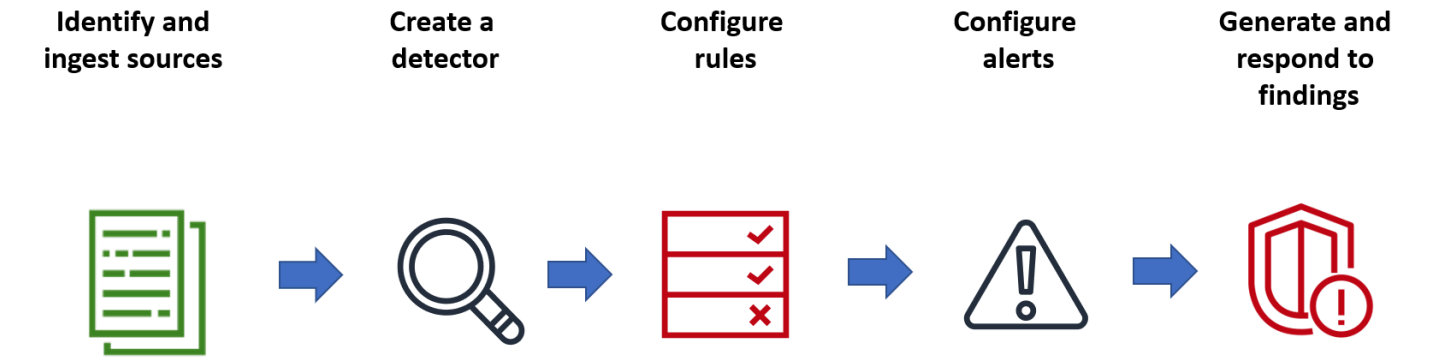
Security Analytics è una OpenSearch soluzione che offre visibilità sull'infrastruttura dell'organizzazione, monitora le attività anomale, rileva potenziali minacce alla sicurezza in tempo reale e attiva avvisi verso destinazioni preconfigurate. Puoi monitorare le attività dannose dai registri degli eventi di sicurezza valutando continuamente le regole di sicurezza e rivedendo i risultati di sicurezza generati automaticamente. Inoltre, Security Analytics può generare avvisi automatici e inviarli a un canale di notifica specifico, come Slack o e-mail.

Puoi utilizzare il plug-in Security Analytics per rilevare le minacce più comuni out-of-the-box e generare informazioni critiche sulla sicurezza dai registri degli eventi di sicurezza esistenti, come i registri del firewall, i registri di Windows e i registri di controllo dell'autenticazione. Per utilizzare Security Analytics, sul tuo dominio deve essere in esecuzione la OpenSearch versione 2.5 o successiva.

> **Note**
>
> Questa documentazione fornisce una breve panoramica di Security Analytics for Amazon OpenSearch Service. Definisce i concetti chiave e fornisce i passaggi per configurare le autorizzazioni. Per una documentazione completa, tra cui una guida alla configurazione, un riferimento all'API e un riferimento a tutte le impostazioni disponibili, consulta Security Analytics nella OpenSearch documentazione.

Componenti e concetti di analisi della sicurezza

Numerosi strumenti e funzionalità forniscono le basi per il funzionamento di Security Analytics. I componenti principali che compongono il plug-in includono rilevatori, tipi di registro, regole, risultati e avvisi.



Tipi di log

OpenSearch supporta diversi tipi di log e fornisce out-of-the-box mappature per ogni tipo. Si specifica il tipo di registro e si configura un intervallo di tempo quando si crea un rilevatore, e da lì Security Analytics attiva automaticamente un set di regole pertinenti che vengono eseguite in quell'intervallo.

Rilevatori

I rilevatori identificano una serie di minacce alla sicurezza informatica per un tipo di registro nei tuoi indici di dati. È possibile configurare il rilevatore in modo da utilizzare sia regole personalizzate che regole Sigma preconfezionate che valutano gli eventi che si verificano nel sistema. Il rilevatore genera quindi risultati di sicurezza a partire da questi eventi. Per ulteriori informazioni sui rilevatori, vedere Creazione di rilevatori nella documentazione. OpenSearch

Regolamento

Le regole di rilevamento delle minacce definiscono le condizioni che i rilevatori applicano ai dati di registro acquisiti per identificare un evento di sicurezza. Security Analytics supporta l'importazione, la creazione e la personalizzazione di regole per soddisfare le vostre esigenze e fornisce anche regole Sigma preconfezionate e open source per rilevare le minacce più comuni dai log. Security Analytics associa molte regole a una base di conoscenze in continua crescita di tattiche e tecniche degli avversari gestita dall'organizzazione MITRE ATT&CK. Puoi utilizzare sia le OpenSearch dashboard che le API per creare e utilizzare le regole. Per ulteriori informazioni sulle regole, consulta Lavorare con le regole nella OpenSearch documentazione.

Risultati

Quando un rilevatore abbina una regola a un evento di registro, genera un risultato. Ogni risultato include una combinazione unica di regole selezionate, un tipo di registro e una gravità della regola. I risultati non indicano necessariamente minacce imminenti all'interno del sistema, ma isolano sempre un evento di interesse. Per ulteriori informazioni sui risultati, consulta Lavorare con i risultati nella OpenSearch documentazione.

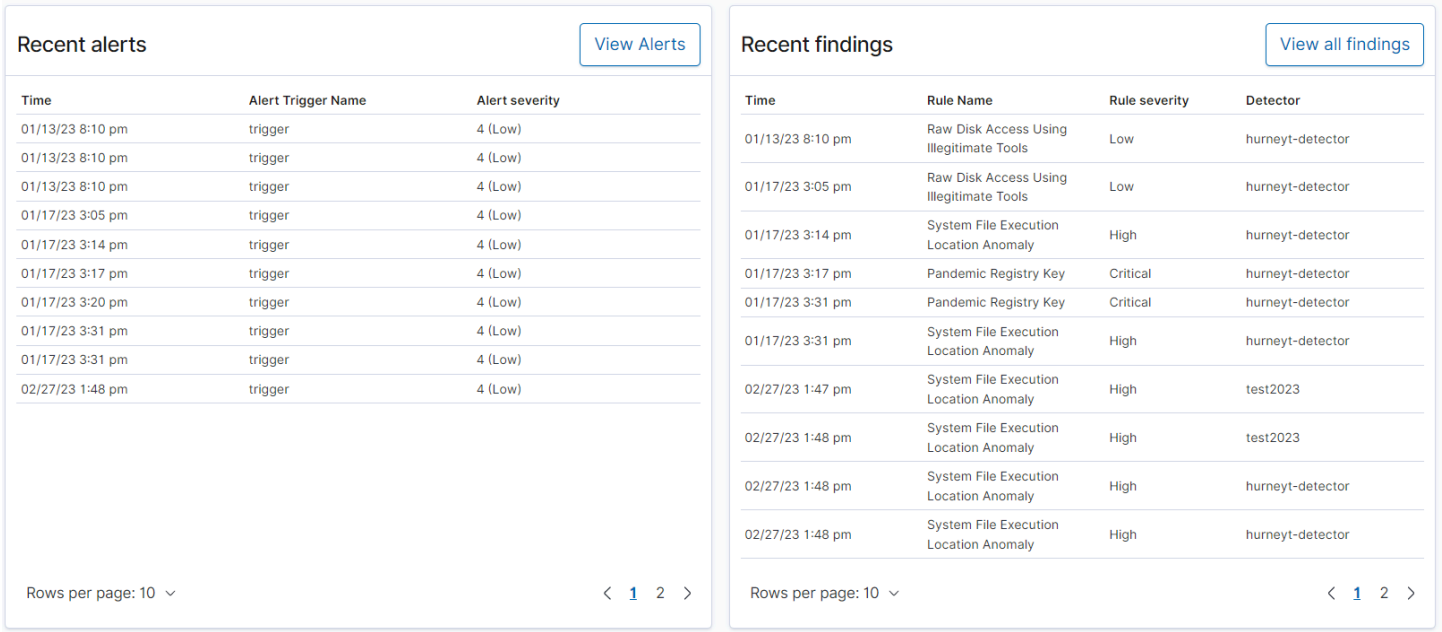
Avvisi

Quando si crea un rilevatore, è possibile specificare una o più condizioni che attivano un avviso. Un avviso è una notifica inviata a un canale preferito, come Slack o e-mail. Puoi impostare l'avviso in modo che venga attivato quando il rilevatore soddisfa una o più regole e puoi personalizzare il messaggio di notifica. Per ulteriori informazioni sugli avvisi, consulta Lavorare con gli avvisi nella documentazione. OpenSearch

Esplorazione dell'analisi della sicurezza

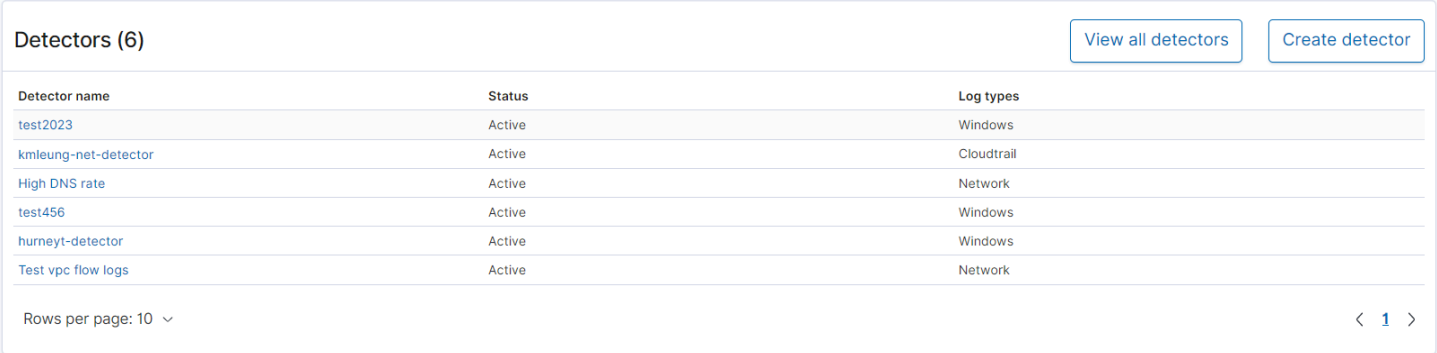
Puoi utilizzare OpenSearch le dashboard per visualizzare e ottenere informazioni dettagliate sul tuo plug-in Security Analytics. La visualizzazione Panoramica fornisce informazioni quali risultati e conteggio degli avvisi, scoperte e avvisi recenti, regole di rilevamento frequenti e un elenco dei rilevatori. È possibile visualizzare una visualizzazione riepilogativa composta da più visualizzazioni. Il grafico seguente, ad esempio, mostra l'andamento dei risultati e degli avvisi per vari tipi di log in un determinato periodo di tempo.

Più in basso nella pagina, puoi esaminare i risultati e gli avvisi più recenti.



Inoltre, puoi vedere una distribuzione delle regole attivate più frequentemente tra tutti i rilevatori attivi. Questo può aiutarti a rilevare e indagare su diversi tipi di attività dannose tra i tipi di registro.

Infine, è possibile visualizzare lo stato dei rilevatori configurati. Da questo pannello, puoi anche accedere al flusso di lavoro per la creazione del rilevatore.



Per configurare la configurazione di Security Analytics, crea delle regole con la pagina Regole e usale per scrivere i rilevatori nella pagina Rilevatori. Per una visualizzazione più mirata dei risultati di Security Analytics, puoi utilizzare le pagine Risultati e Avvisi.

Configurazione delle autorizzazioni

Se abiliti Security Analytics su un dominio di OpenSearch servizio preesistente, il `security_analytics_manager` ruolo potrebbe non essere definito nel dominio. Gli utenti senza privilegi di amministratore devono essere mappati a questo ruolo in modo da gestire gli indici a caldo sui domini che utilizzano il controllo granulare degli accessi. Per creare manualmente il ruolo `security_analytics_manager`, procedere nel seguente modo:

1. In OpenSearch Dashboard, vai su Sicurezza e scegli Autorizzazioni.
2. Scegliere Crea gruppo di operazioni e configurare i seguenti gruppi:

Group name (Nome gruppo)	Autorizzazioni
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/*
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. Scegliere Ruoli, quindi selezionare Crea ruolo.
4. Assegna un nome al ruolo security_analytics_manager.

5. Per Autorizzazioni cluster, selezionare `security_analytics_full_access` e `security_analytics_read_access`.
6. Per Indice, digitare `*`.
7. Per le autorizzazioni di indicizzazione, seleziona e. `indices:admin/mapping/put` `indices:admin/mappings/get`
8. Scegli Crea.
9. Dopo aver creato il ruolo, associalo a qualsiasi ruolo utente o di backend che gestirà gli indici di Security Analytics.

Risoluzione dei problemi

Nessun errore di indice di questo tipo

Se non hai rilevatori e apri la dashboard di Security Analytics, potresti vedere una notifica in basso a destra che dice`[index_not_found_exception] no such index [.opensearch-sap-detectors-config]`. Puoi ignorare questa notifica, che scompare nel giro di pochi secondi e non verrà più visualizzata una volta creato un rilevatore.

Osservabilità in Amazon Service OpenSearch

L'installazione predefinita di OpenSearch Dashboards for Amazon OpenSearch Service include il plug-in Observability, che puoi utilizzare per visualizzare eventi basati sui dati utilizzando Piped Processing Language (PPL) per esplorare, scoprire e interrogare i dati archiviati in. OpenSearch Il plug-in richiede 1.2 o versione successiva. OpenSearch

Il plug-in Observability offre un'esperienza unificata per la raccolta e il monitoraggio di parametri, registri e tracce provenienti da origini dati comuni. La raccolta e il monitoraggio dei dati in un unico posto consentono l' end-to-end osservabilità completa dell'intera infrastruttura.

> **Note**
>
> Questa documentazione fornisce una breve panoramica di Observability in Service. OpenSearch Per una documentazione completa del plugin Observability, incluse le autorizzazioni, vedi Observability.

Il processo di esplorazione dei dati è diverso per ogni persona. Se non conosci l'esplorazione dei dati e la creazione di visualizzazioni, ti consigliamo di provare un flusso di lavoro come il seguente.

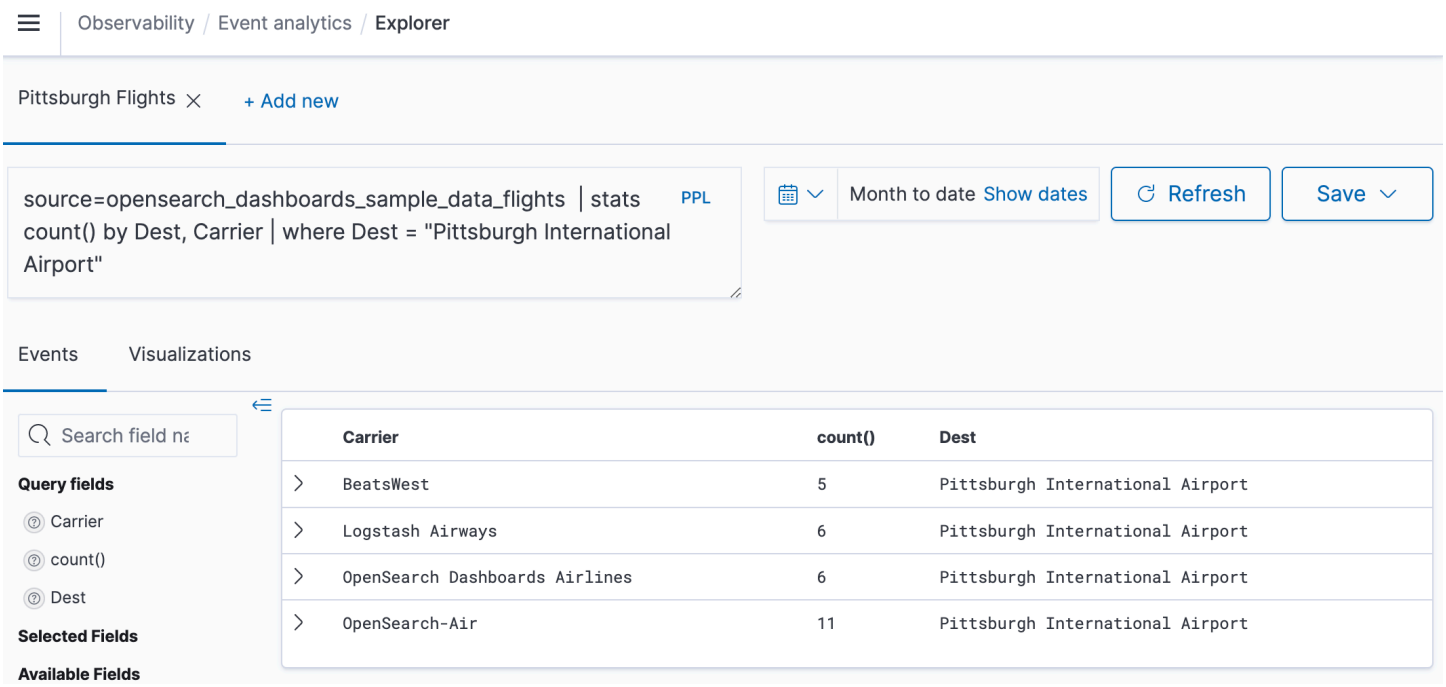
Esplora i dati con l'analisi dei dati degli eventi

Per iniziare, supponiamo che tu stia raccogliendo dati sui voli nel tuo dominio di OpenSearch servizio e desideri scoprire quale compagnia aerea ha avuto il maggior numero di voli in arrivo all'aeroporto internazionale di Pittsburgh il mese scorso. Scrivi la seguente query PPL:

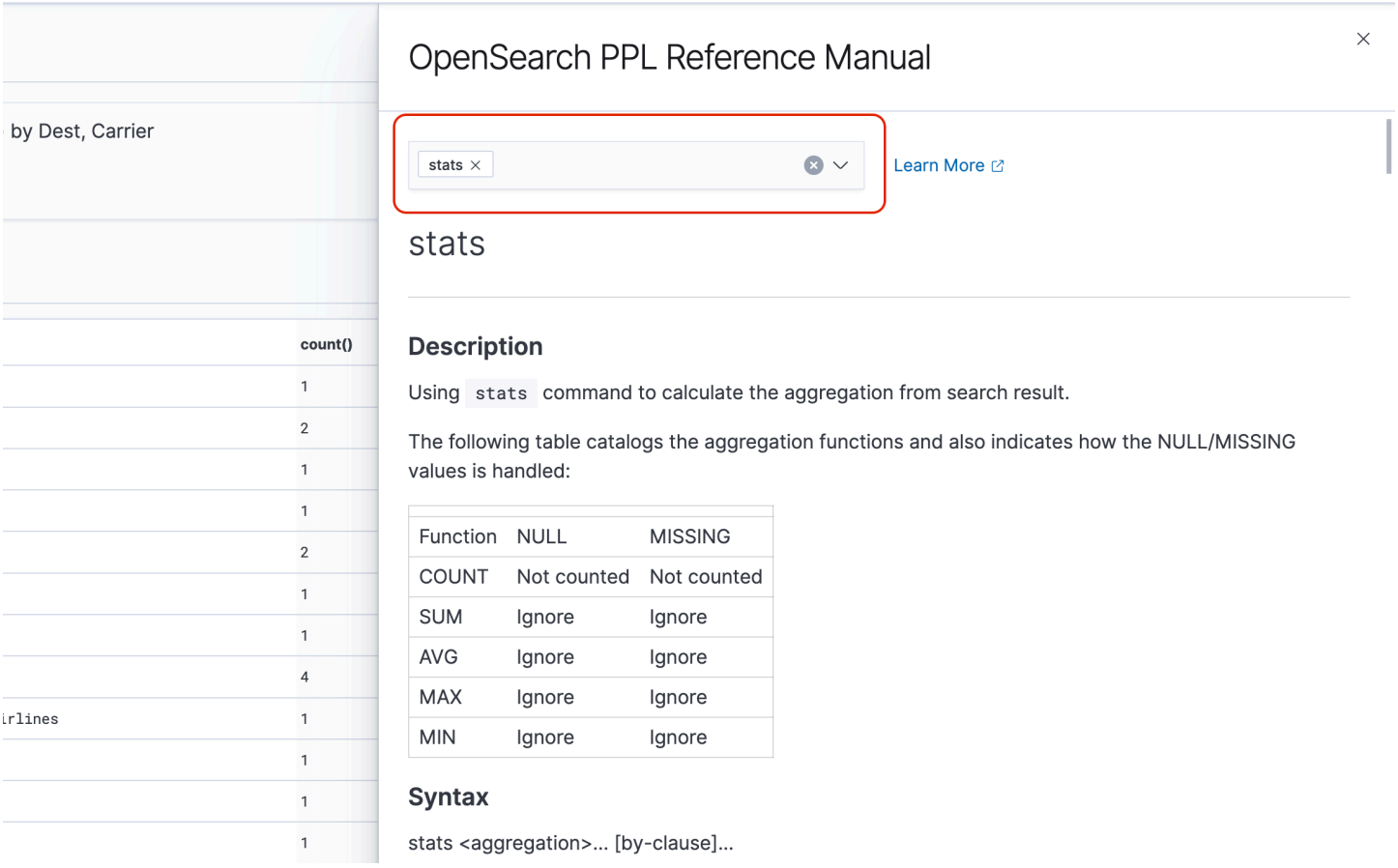
```
source=opensearch_dashboards_sample_data_flights |
    stats count() by Dest, Carrier |
    where Dest = "Pittsburgh International Airport"
```

Questa query estrae i dati dall'indice denominato `opensearch_dashboards_sample_data_flights`. Quindi usa il comando `stats` per ottenere un numero totale di voli e raggrupparlo in base all'aeroporto di destinazione e al vettore. Infine, utilizza la clausola `where` per filtrare i risultati dei voli in arrivo all'aeroporto internazionale di Pittsburgh.

Ecco come appaiono i dati quando vengono visualizzati nell'ultimo mese:



È possibile scegliere il pulsante PPL nell'editor di query per ottenere informazioni sull'utilizzo ed esempi per ogni comando PPL:



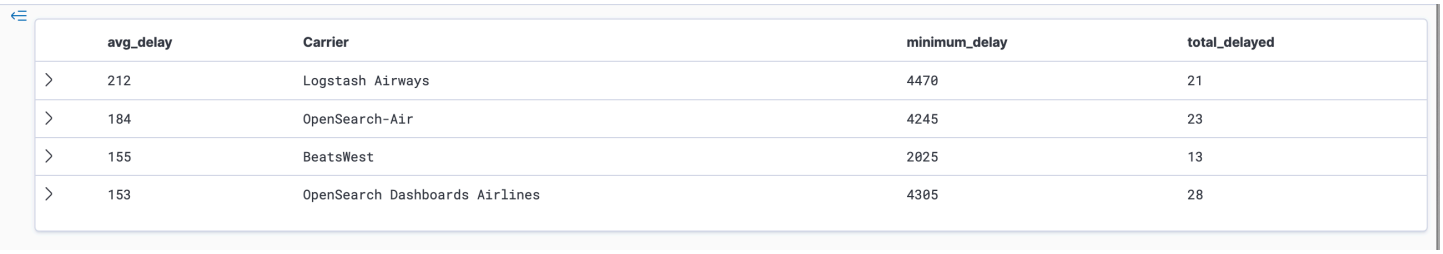
Osserviamo il seguente esempio più complesso, che richiede informazioni sui ritardi dei voli:

```
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
```

Ogni comando nella query influisce sull'output finale:

- `source=opensearch_dashboards_sample_data_flights` - estrae i dati dallo stesso indice dell'esempio precedente
- `where FlightDelayMin > 0` - filtra i dati sui voli in ritardo
- `stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier` - per ogni vettore, ottiene il tempo di ritardo minimo totale e il conteggio totale dei voli in ritardo
- `eval avg_delay=minimum_delay / total_delayed` - calcola il tempo medio di ritardo per ciascun vettore dividendo il tempo minimo di ritardo per il numero totale di voli in ritardo
- `sort - avg_delay` - ordina i risultati in base al ritardo medio in ordine decrescente

Con questa query, puoi determinare che OpenSearch Dashboards Airlines ha, in media, meno ritardi.



	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

Puoi trovare ulteriori query PPL di esempio in Query e visualizzazioni nella pagina Analisi dei dati degli eventi.

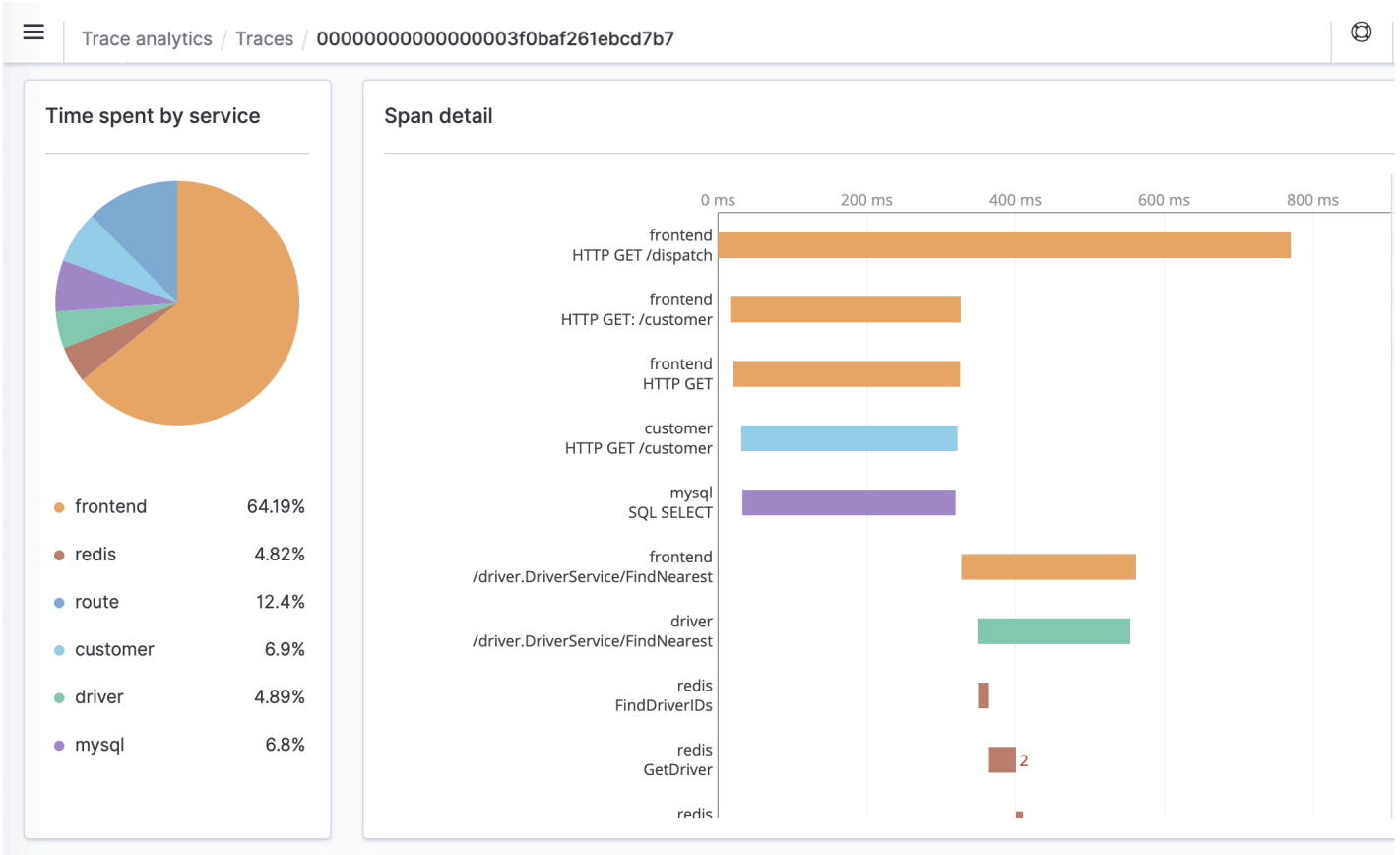
Creazione di visualizzazioni

Dopo aver eseguito una query corretta dei dati che ti interessano, puoi salvare queste query come visualizzazioni:

Quindi aggiungi queste visualizzazioni a pannelli operativi per confrontare diverse parti di dati. Utilizzare il plug-in notebook per combinare diverse visualizzazioni e blocchi di codice che puoi condividere con i membri del team.

Approfondisci con Trace Analytics

Trace Analytics offre un modo per visualizzare il flusso di eventi nei OpenSearch dati per identificare e risolvere i problemi di prestazioni nelle applicazioni distribuite.



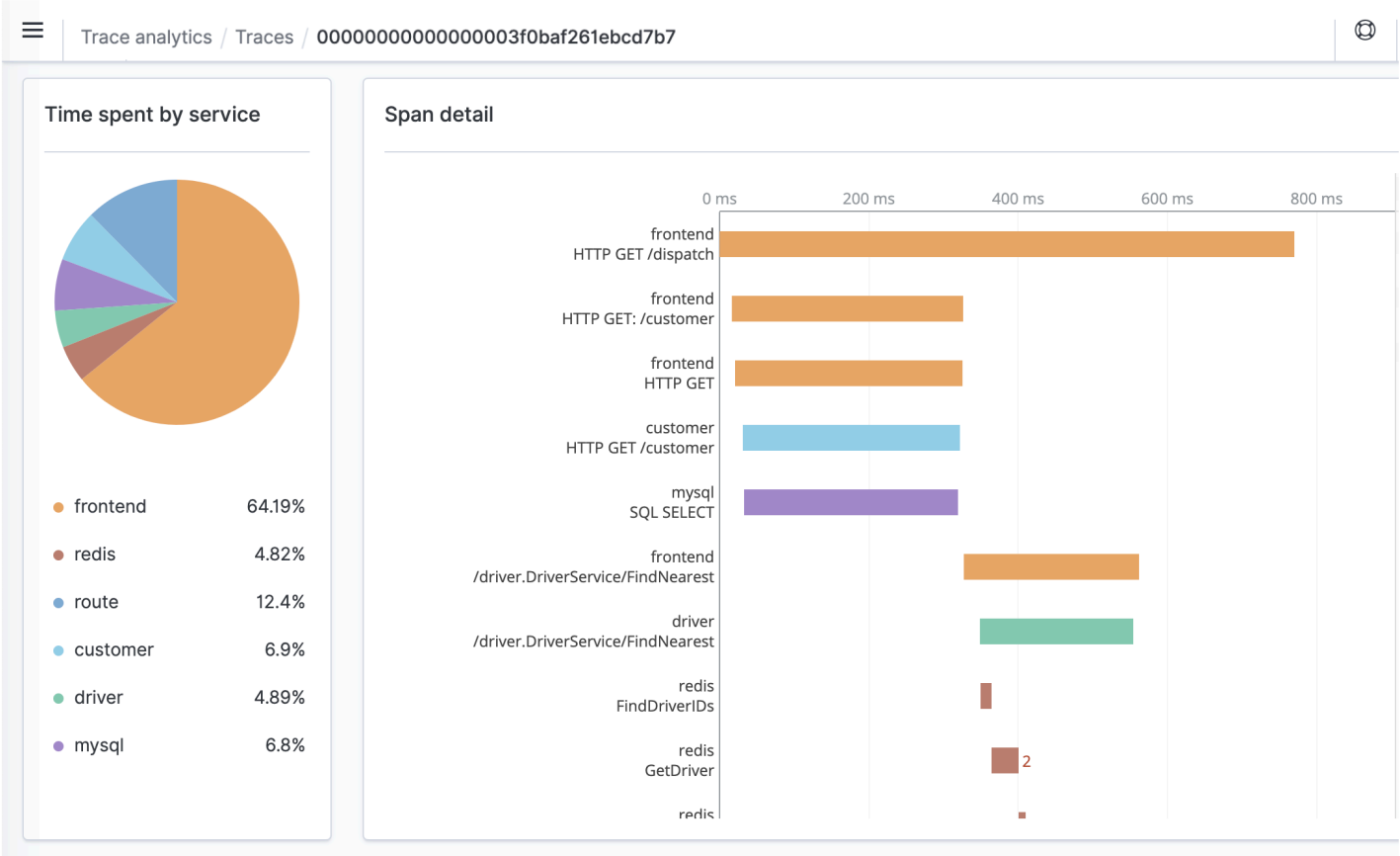
Trace Analytics per Amazon OpenSearch Service

Puoi utilizzare Trace Analytics, che fa parte del plug-in OpenSearch Observability, per analizzare i dati di traccia provenienti da applicazioni distribuite. Trace Analytics richiede Elasticsearch 7.9 OpenSearch o versione successiva.

In un'applicazione distribuita, una singola operazione, ad esempio un utente che fa clic su un pulsante, può attivare una serie estesa di eventi. Ad esempio, il front-end dell'applicazione potrebbe chiamare un servizio di back-end, che a sua volta chiama un altro servizio, che esegue una query su un database, che elabora la query e restituisce un risultato. Quindi il primo servizio di back-end invia una conferma al front-end, che aggiorna l'interfaccia utente.

È possibile utilizzare Analisi di traccia per visualizzare questo flusso di eventi e identificare i problemi legati alle prestazioni.

> **Note**
>
> Questa documentazione fornisce una breve panoramica di Trace Analytics. Per una documentazione completa, consulta Trace Analytics nella OpenSearch documentazione open source.



Prerequisiti

Trace Analytics richiede l'aggiunta di strumentazione all'applicazione e la generazione di dati di traccia utilizzando una libreria OpenTelemetry supportata come Jaeger o Zipkin. Questo passaggio si verifica completamente al di fuori del Servizio. OpenSearch La AWS Distro for OpenTelemetry documentation contiene esempi di applicazioni per molti linguaggi di programmazione che possono aiutarti a iniziare, tra cui Java, Python, Go e. JavaScript

Dopo aver aggiunto la strumentazione all'applicazione, OpenTelemetryCollector riceve i dati dall'applicazione e li formatta in dati. OpenTelemetry Visualizzate l'elenco dei ricevitori su. GitHub AWS Distro for OpenTelemetry include un ricevitore per. AWS X-Ray

Infine, è possibile utilizzare OpenSearch Ingestione di Amazon per formattare i OpenTelemetry dati per utilizzarli con OpenSearch.

OpenTelemetry Configurazione di esempio di Collector

Per utilizzare OpenTelemetry Collector con OpenSearch Ingestione di Amazon, prova la seguente configurazione di esempio:

```
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]
```

OpenSearch Configurazione di esempio di ingestione

Per inviare dati di traccia a un dominio di OpenSearch servizio, prova il seguente esempio di configurazione della pipeline di OpenSearch Ingestion. Per istruzioni su come creare una pipeline, vedere. the section called “Creazione di pipeline”

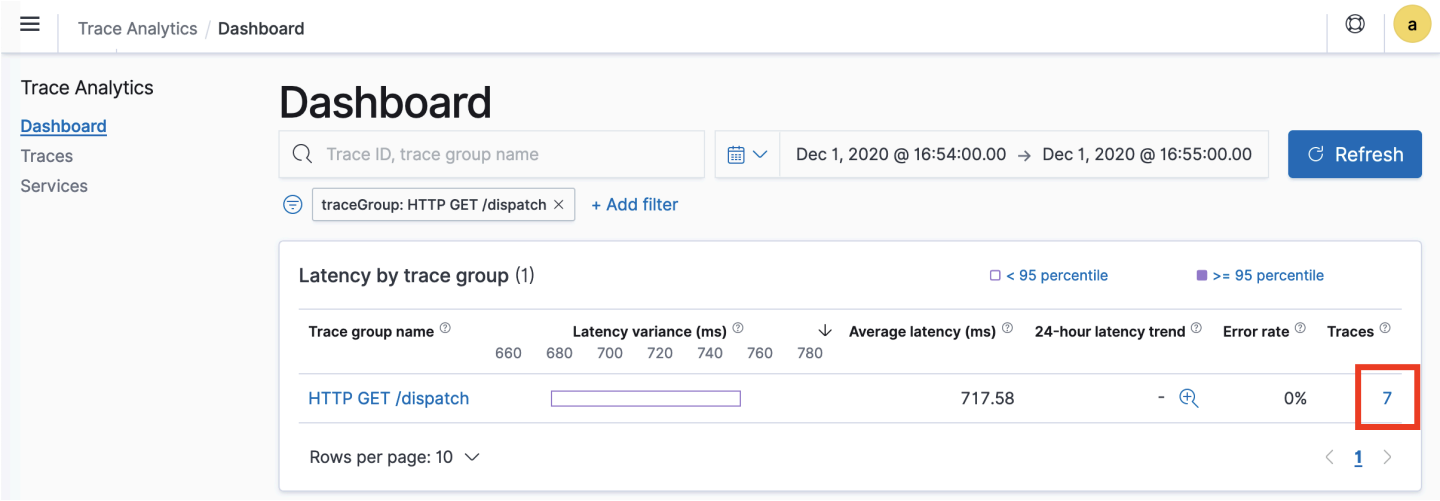
```
version: "2"
otel-trace-pipeline:
```

```
  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"
```

Il ruolo della pipeline specificato nell'`sts_role_arn`opzione deve disporre delle autorizzazioni di scrittura per il sink. Per istruzioni su come configurare le autorizzazioni per il ruolo pipeline, consulta. the section called “Configurazione di ruoli e utenti”

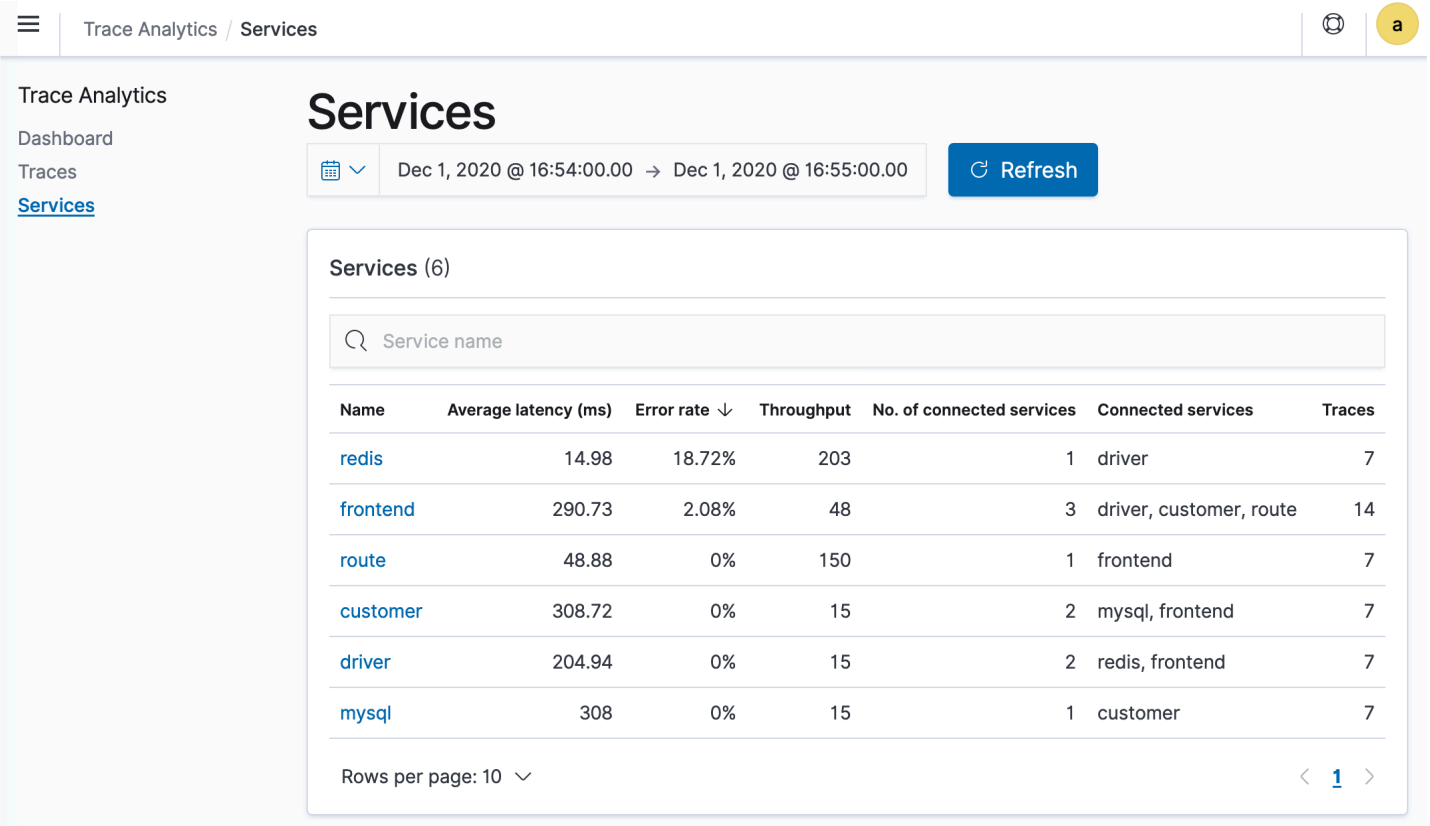
Esplorazione dei dati di traccia

La vista Pannello di controllo raggruppa le tracce in base al metodo HTTP e al percorso in modo da poter visualizzare la latenza media, il tasso di errore e le tendenze associati a una particolare operazione. Per una vista più mirata, provare a filtrare in base al nome del gruppo di traccia.



Per eseguire il drill-down delle tracce che costituiscono un gruppo di traccia, scegliere il numero di tracce nella colonna di destra. Quindi scegliere una singola traccia per un riepilogo dettagliato.

La vista Servizi riporta tutti i servizi dell'applicazione, oltre a una mappa interattiva che mostra come i vari servizi si connettono tra loro. A differenza del pannello di controllo (che consente di identificare i problemi in base all'operazione), la mappa del servizio consente di identificare i problemi in base al servizio. Provare a ordinare in base al tasso di errore o alla latenza per avere un'idea delle potenziali aree problematiche dell'applicazione.



Interrogazione dei dati OpenSearch di Amazon Service utilizzando il linguaggio di elaborazione Piped

Piped Processing Language (PPL) è un linguaggio di query che consente di utilizzare la sintassi pipe (|) per interrogare i dati archiviati in Amazon Service. OpenSearch PPL richiede Elasticsearch 7.9 OpenSearch o versione successiva.

> **Note**
>
> Questa documentazione fornisce una breve panoramica di PPL for Amazon OpenSearch Service. Per i passaggi dettagliati e un riferimento completo ai comandi, consulta PPL nella documentazione open source OpenSearch .

La sintassi PPL è costituita da comandi delimitati da un carattere pipe (|) dove i dati fluiscono da sinistra a destra attraverso ogni pipeline. Ad esempio, la sintassi PPL per trovare il numero di host con errori HTTP 403 o 503, aggregarli per host e ordinarli nell'ordine di impatto, è la seguente:

```
source = dashboards_sample_data_logs | where response='403' or response='503' | stats
 count(request) as request_count by host, response | sort -request_count
```

Per iniziare, scegli Query Workbench in OpenSearch Dashboards e seleziona PPL. Utilizzare l'operazione `bulk` per indicizzare alcuni dati di esempio:

```
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"}
```

L'esempio seguente restituisce `firstname` e `lastname` per i documenti in un indice di account con `age` maggiore di 18:

```
search source=accounts | where age > 18 | fields firstname, lastname
```

Risposta di esempio

id	firstname	lastname
0	Amber	Duke
1	Hattie	Bond
2	Nanette	Bates
3	Dale	Adams

È possibile utilizzare un set completo di comandi di sola lettura come `search`, `where`, `fields`, `rename`, `dedup`, `stats`, `sort`, `eval`, `head`, `top` e `rare`. Il plug-in PPL supporta tutte le funzioni SQL, compresi gli operatori matematici, trigonometrici, data-ora, stringa, aggregati e le espressioni avanzate. Per saperne di più, consulta il manuale di riferimento OpenSearch PPL.

Best practice operative per Amazon OpenSearch Service

Questo capitolo fornisce le best practice per la gestione dei domini Amazon OpenSearch Service e include linee guida generali che si applicano a molti casi d'uso. Ogni carico di lavoro è unico, con caratteristiche uniche, quindi nessun suggerimento generico è adatto per ogni caso d'uso. La best practice più importante consiste nell'implementare, testare e ottimizzare i domini in un ciclo continuo per trovare la configurazione, la stabilità e il costo ottimali per il tuo carico di lavoro.

Argomenti

Monitoraggio e avvisi

Le seguenti best practice si applicano al monitoraggio dei domini OpenSearch di servizio.

Configura CloudWatch gli allarmi

OpenSearch Il servizio invia metriche sulle prestazioni ad Amazon. CloudWatch Esamina regolarmente i parametri del cluster e dell'istanza e configura gli CloudWatch allarmi consigliati in base alle prestazioni del carico di lavoro.

Abilitazione della pubblicazione dei log

OpenSearch Il servizio espone i log degli OpenSearch errori, gli slow log di ricerca, gli slow log di indicizzazione e i log di controllo in Amazon Logs. CloudWatch I log di ricerca lenti, i log di

indicizzazione lenti e i log di errore sono utili per la risoluzione dei problemi relativi alle prestazioni e alla stabilità. I log di verifica, disponibili solo se abiliti il controllo granulare degli accessi, monitorano l'attività dell'utente. Per ulteriori informazioni, consulta Logs nella documentazione. OpenSearch

I log di ricerca lenti e i log di indicizzazione lenti sono uno strumento importante per comprendere e risolvere i problemi delle prestazioni delle operazioni di ricerca e indicizzazione. Abilita la distribuzione di log lenti di ricerca e di indice per tutti i domini di produzione. È inoltre necessario configurare le soglie di registrazione, altrimenti i registri CloudWatch non verranno acquisiti.

Strategia di partizione

Gli shard distribuiscono il carico di lavoro tra i nodi di dati del dominio di servizio. OpenSearch Gli indici configurati correttamente possono contribuire a migliorare le prestazioni complessive del dominio.

Quando invii dati a OpenSearch Service, invii tali dati a un indice. Un indice è analogo a una tabella di database, con documenti come le righe e campi come le colonne. Quando crei l'indice, dici OpenSearch quanti shard primari vuoi creare. Gli shard primari sono partizioni indipendenti dell'intero set di dati. OpenSearch Il servizio distribuisce automaticamente i dati tra gli shard primari di un indice. Puoi inoltre configurare le repliche dell'indice. Ogni partizione di replica comprende un set completo di copie delle partizioni primarie per quell'indice.

OpenSearch Il servizio mappa gli shard per ogni indice tra i nodi di dati del cluster. Questo assicura che le partizioni primarie e di replica per l'indice risiedano su nodi di dati diversi. La prima replica garantisce la presenza di due copie dei dati nell'indice. Dovresti sempre usare almeno una replica. Le repliche aggiuntive forniscono ridondanza e capacità di lettura aggiuntive.

OpenSearch invia richieste di indicizzazione a tutti i nodi di dati che contengono frammenti che appartengono all'indice. Invia le richieste di indicizzazione prima ai nodi di dati che contengono partizioni primarie e poi ai nodi di dati che contengono partizioni di replica. Le richieste di ricerca vengono indirizzate dal nodo coordinatore a una partizione primaria o di replica per tutte le partizioni appartenenti all'indice.

Ad esempio, per un indice con cinque partizioni primarie e una replica, ogni richiesta di indicizzazione interessa 10 partizioni. Le richieste di ricerca, invece, vengono inviate a n partizioni, dove n è il numero di partizioni primarie. Per un indice con cinque partizioni primarie e una replica, ogni query di ricerca interessa cinque partizioni (primarie o di replica) da quell'indice.

Determinazione del numero di partizioni e di nodi di dati

Utilizza le seguenti best practice per determinare il numero di partizioni e nodi di dati per il tuo dominio.

Dimensione delle partizioni: la dimensione dei dati su disco è il risultato diretto della dimensione dei dati di origine e cambia man mano che indicizzi più dati. Il source-to-index rapporto può variare notevolmente, da 1:10 a 10:1 o più, ma in genere è di circa 1:1,10. Puoi utilizzare questo rapporto per prevedere la dimensione dell'indice su disco. Puoi inoltre indicizzare alcuni dati e recuperare le dimensioni effettive dell'indice per determinare il rapporto per il tuo carico di lavoro. Una volta ottenuta una dimensione dell'indice prevista, imposta un numero di partizioni in modo che ogni partizione abbia una dimensione compresa tra 10 e 30 GiB (per i carichi di lavoro di ricerca) o tra 30 e 50 GiB (per i carichi di lavoro dei log). 50 GiB dovrebbe essere il massimo; assicurati di pianificare la crescita.

Conteggio partizioni: la distribuzione delle partizioni sui nodi di dati ha un grande impatto sulle prestazioni di un dominio. Quando disponi di indici con più partizioni, prova a rendere il conteggio delle partizioni un multiplo pari del conteggio dei nodi di dati. Ciò aiuta a garantire che le partizioni siano distribuite uniformemente tra i nodi di dati e previene i nodi ad accesso frequente. Ad esempio, se disponi di 12 partizioni primarie, il numero di nodi di dati deve essere 2, 3, 4, 6 o 12. Tuttavia, il numero delle partizioni è secondario rispetto alla dimensione delle partizioni; se disponi di 5 GiB di dati, dovresti comunque usare una singola partizione.

Partizioni per nodo di dati: il numero totale di partizioni che un nodo può contenere è proporzionale alla memoria heap JVM (Java Virtual Machine) del nodo. Punta a 25 partizioni o meno per GiB di memoria heap. Ad esempio, un nodo con 32 GiB di memoria heap non deve contenere più di 800 partizioni. Sebbene la distribuzione delle partizioni possa variare in base ai modelli di carico di lavoro, esiste un limite di 1.000 partizioni per nodo. L'API cat/allocation fornisce una visualizzazione rapida del numero di partizioni e dello storage totale delle partizioni tra i nodi di dati.

Rapporto partizione/CPU: quando una partizione è coinvolta in una richiesta di indicizzazione o ricerca, utilizza una vCPU per elaborare la richiesta. Come best practice, utilizza un punto di scala iniziale di 1,5 vCPU per partizione. Se il tuo tipo di istanza presenta 8 vCPU, imposta il conteggio dei nodi di dati in modo che ogni nodo non abbia più di sei partizioni. Si tratta di un'approssimazione. Assicurati di testare il carico di lavoro e dimensionare il cluster di conseguenza.

Per suggerimenti sul volume di storage, la dimensione delle partizioni e il tipo di istanza, consulta le seguenti risorse:

- the section called “Dimensionamento dei domini”
- the section called “Scala in petabyte”

Evitare l'asimmetria di storage

L'asimmetria di archiviazione si verifica quando uno o più nodi all'interno di un cluster detengono una percentuale maggiore di archiviazione per uno o più indici rispetto agli altri. L'utilizzo non uniforme della CPU, la latenza intermittente e irregolare e l'accodamento non uniforme tra i nodi di dati sono tutte indicazioni di asimmetria di archiviazione. Per determinare se sono presenti problemi di asimmetria, consulta le seguenti sezioni sulla risoluzione dei problemi:

- the section called “Asimmetria di partizioni e storage di nodi”
- the section called “Asimmetria di partizioni e storage di indici”

Stabilità

Le seguenti procedure consigliate si applicano al mantenimento di un dominio di servizio stabile e integro. OpenSearch

Tieniti aggiornato con OpenSearch

Aggiornamenti del software del servizio

OpenSearch Il servizio rilascia regolarmente aggiornamenti software che aggiungono funzionalità o migliorano in altro modo i tuoi domini. Gli aggiornamenti non modificano né la versione del motore Elasticsearch OpenSearch né quella del motore Elasticsearch. Ti consigliamo di pianificare un orario ricorrente per eseguire l'operazione dell'DescribeDomainAPI e di avviare un aggiornamento del software di servizio, se lo è. `UpdateStatus` `ELIGIBLE` Se non aggiorni il dominio entro un determinato periodo di tempo (in genere due settimane), il OpenSearch Servizio esegue automaticamente l'aggiornamento.

OpenSearch aggiornamenti di versione

OpenSearch Il servizio aggiunge regolarmente il supporto per le versioni gestite dalla community di. OpenSearch Effettua sempre l'upgrade alle OpenSearch versioni più recenti quando sono disponibili.

OpenSearch Il servizio aggiorna contemporaneamente entrambe le OpenSearch OpenSearch dashboard (o Elasticsearch e Kibana se il dominio utilizza un motore legacy). Se il cluster dispone di

nodi master dedicati, gli aggiornamenti vengono completati senza tempi di inattività. In caso contrario, il cluster potrebbe non rispondere per diversi secondi dopo l'aggiornamento mentre elegge un nodo principale. OpenSearch I dashboard potrebbero non essere disponibili durante alcuni o tutti gli upgrade.

Ci sono due modi per aggiornare un dominio:

- Aggiornamento in loco: questa opzione è più semplice perché si mantiene lo stesso cluster.
- Aggiornamento di snapshot/ripristino: questa opzione è ideale per testare nuove versioni su un nuovo cluster o per eseguire la migrazione tra cluster

Indipendentemente dal processo di aggiornamento utilizzato, ti consigliamo di mantenere un dominio destinato esclusivamente allo sviluppo e al test e di aggiornarlo alla nuova versione prima di aggiornare il dominio di produzione. Quando crei il dominio di test, scegli Development and testing (Sviluppo e test) per il tipo di implementazione. Assicurati di aggiornare tutti i client alle versioni compatibili subito dopo l'aggiornamento del dominio.

Migliora le prestazioni delle istantanee

Per evitare che l'istantanea rimanga bloccata durante l'elaborazione, il tipo di istanza per il nodo master dedicato deve corrispondere al numero di shard. Per ulteriori informazioni, consulta the section called “Scelta dei tipi di istanza per nodi principali dedicati”. Inoltre, ogni nodo non deve avere più dei 25 shard consigliati per GiB di memoria heap Java. Per ulteriori informazioni, consulta the section called “Scelta del numero di partizioni”.

Abilitare nodi principali dedicati

I nodi principali dedicati migliorano la stabilità del cluster. Un nodo principale dedicato esegue attività di gestione del cluster ma non conserva dati di indice né risponde a richieste del client. Questo offload delle attività di gestione del cluster aumenta la stabilità del dominio e consente di apportare modifiche alla configurazione senza avere tempi di inattività.

Abilita e utilizza tre nodi principali dedicati per una stabilità ottimale del dominio in tre zone di disponibilità. L'implementazione con Multi-AZ con Standby configura tre nodi master dedicati per te. Per suggerimenti sul tipo di istanza, consulta the section called “Scelta dei tipi di istanza per nodi principali dedicati”.

Esecuzione dell'implementazione in più zone di disponibilità

Per prevenire la perdita di dati e ridurre al minimo i tempi di inattività del cluster in caso di interruzione del servizio, puoi distribuire i nodi tra due o tre zone di disponibilità nella stessa Regione AWS. La migliore pratica consiste nell'implementare Multi-AZ with Standby, che configura tre zone di disponibilità, con due zone attive e una che funge da standby, e con due shard di replica per indice. Questa configurazione consente a OpenSearch Service di distribuire gli shard di replica su AZ diversi rispetto ai corrispondenti shard primari. Non sono previsti costi di trasferimento dei dati tra zone di disponibilità per le comunicazioni dei cluster tra zone di disponibilità.

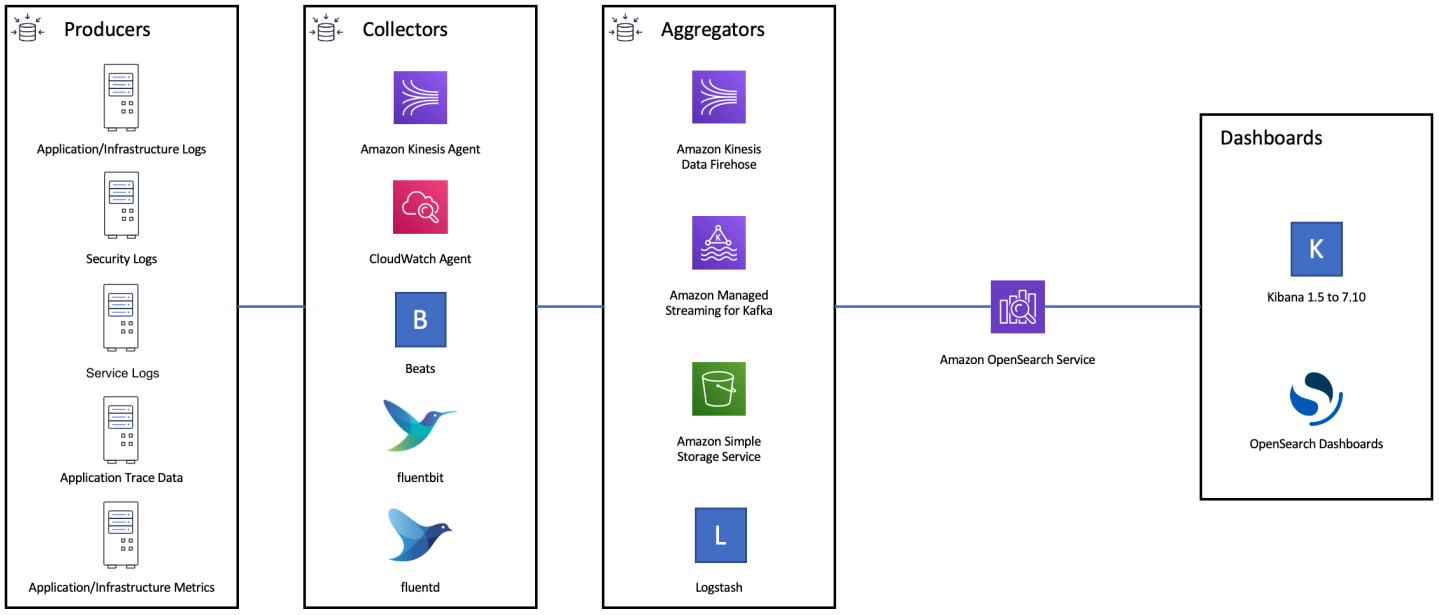
Le zone di disponibilità sono più posizioni isolate all'interno di ogni regione . Con una configurazione a due zone di disponibilità, perdere una zona di disponibilità significa perdere metà della capacità totale del dominio. Il passaggio a tre zone di disponibilità riduce ulteriormente l'impatto della perdita di una singola zona di disponibilità.

Controllo del flusso di importazione e del buffering

Consigliamo di limitare il numero complessivo delle richieste utilizzando l'operazione API _bulk. È più efficace inviare una richiesta `_bulk` contenente 5.000 documenti anziché inviare 5.000 richieste contenenti un singolo documento.

Per una stabilità operativa ottimale, a volte è necessario limitare o addirittura sospendere il flusso upstream delle richieste di indicizzazione. Limitare la percentuale di richieste di indicizzazione è un meccanismo importante per gestire picchi imprevisti o occasionali nelle richieste che potrebbero altrimenti sovraccaricare il cluster. Valuta la possibilità di creare un meccanismo di controllo del flusso nella tua architettura upstream.

Il diagramma seguente mostra più opzioni di componenti per un'architettura di importazione dei log. Configura il livello di aggregazione per avere spazio sufficiente per il buffering dei dati in ingresso per picchi di traffico improvvisi e brevi interventi di manutenzione del dominio.



Creare mappature per i carichi di lavoro di ricerca

Per i carichi di lavoro di ricerca, crea mappature che definiscono il modo in cui OpenSearch archivia e indicizza i documenti e i relativi campi. Imposta `dynamic` su `strict` per evitare l'aggiunta accidentale di nuovi campi.

```
PUT my-index
{
  "mappings": {
    "dynamic": "strict",
    "properties": {
      "title": { "type" : "text" },
      "author": { "type" : "integer" },
      "year": { "type" : "text" }
    }
  }
}
```

Utilizzare modelli di indici

È possibile utilizzare un modello di indice per spiegare OpenSearch come configurare un indice al momento della creazione. Configura i modelli di indice prima di creare gli indici. Quindi, quando crei un indice, l'indice eredita le impostazioni e le mappature dal modello. Puoi applicare più di un modello a un singolo indice, quindi puoi specificare le impostazioni in un modello e le mappature in un altro.

Questa strategia consente un modello per le impostazioni comuni su più indici e modelli separati per impostazioni e mappature più specifiche.

Le seguenti impostazioni sono particolarmente utili per la configurazione nei modelli:

- Numero di partizioni primarie e di replica
- Intervallo di aggiornamento (con quale frequenza aggiornare e rendere disponibili per la ricerca le modifiche recenti all'indice)
- Controllo dinamico delle mappature
- Mappature di campi esplicite

Il seguente modello di esempio contiene ognuna di queste impostazioni:

```
{
   "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"
         }
      }
   }
}
```

Anche se cambiano raramente, avere impostazioni e mappature definite centralmente OpenSearch è più semplice da gestire rispetto all'aggiornamento di più client upstream.

Gestire gli indici con Index State Management

Se gestisci log o dati di serie temporali, ti consigliamo di utilizzare Index State Management (ISM). ISM consente di automatizzare attività regolari di gestione del ciclo di vita degli indici. Con ISM, puoi creare policy che attivano i rollover degli alias degli indici, eseguire snapshot degli indici, spostare gli indici tra i livelli di archiviazione ed eliminare gli indici precedenti. Puoi persino usare le operazioni di rollover di ISM come strategia alternativa di gestione del ciclo di vita dei dati per evitare asimmetrie di partizioni.

In primo luogo, configura una policy ISM. Per un esempio, consulta the section called “Policy di esempio”. Quindi, collega la policy a uno o più indici. Se includi un campo modello ISM nella policy, OpenSearch Service applica automaticamente la policy a qualsiasi indice che corrisponda al modello specificato.

Rimuovere gli indici inutilizzati

Esamina regolarmente gli indici nel tuo cluster e identifica quelli che non sono in uso. Esegui uno snapshot di questi indici in modo che siano archiviati in S3, quindi eliminali. Quando rimuovi gli indici inutilizzati, riduci il numero di partizioni e si consente una distribuzione dell'archiviazione e un utilizzo delle risorse più bilanciati tra i nodi. Anche quando sono inattivi, gli indici consumano alcune risorse durante le attività interne di manutenzione degli indici.

Anziché eliminare manualmente gli indici inutilizzati, puoi utilizzare ISM per eseguire automaticamente un'istantanea ed eliminare gli indici dopo un certo periodo di tempo.

Utilizzare più domini per un'elevata disponibilità

Per ottenere un'elevata disponibilità oltre un tempo di attività del 99,9% in più regioni, prendi in considerazione l'utilizzo di due domini. Per set di dati piccoli o che cambiano lentamente, puoi configurare la replica tra cluster in modo da mantenere un modello attivo-passivo. In questo modello è scritto solo il dominio leader, da cui possono essere letti entrambi i domini. Per set di dati più grandi e dati che cambiano rapidamente, configura la distribuzione doppia nella pipeline di importazione, in modo che tutti i dati vengano scritti indipendentemente in entrambi i domini in un modello attivo-attivo.

Progetta le tue applicazioni upstream e downstream tenendo presente il failover. Assicurati di testare il processo di failover insieme ad altri processi di ripristino di emergenza.

Prestazioni

Le seguenti best practice si applicano all'ottimizzazione dei domini per ottenere prestazioni ottimali.

Ottimizzare le dimensioni e la compressione delle richieste in blocco

Il dimensionamento in blocco dipende dai dati, dall'analisi e dalla configurazione del cluster, ma un buon punto di partenza è 3-5 MiB per ciascuna richiesta in blocco.

Invia richieste e ricevi risposte dai tuoi OpenSearch domini utilizzando la compressione gzip per ridurre la dimensione del payload di richieste e risposte. Puoi usare la compressione gzip con il client OpenSearch Python o includendo le seguenti intestazioni dal lato client:

- `'Accept-Encoding': 'gzip'`
- `'Content-Encoding': 'gzip'`

Per ottimizzare le dimensioni delle richieste in blocco, inizia con una richiesta in blocco di 3 MiB. Quindi, aumentane lentamente la dimensione finché le prestazioni di indicizzazione non smettono di migliorare.

> **Note**
>
> Per abilitare la compressione gzip sui domini che eseguono Elasticsearch versione 6.x, devi impostare `http_compression.enabled` a livello di cluster. Questa impostazione è vera per impostazione predefinita nelle versioni 7.x di Elasticsearch e in tutte le versioni di. OpenSearch

Ridurre le dimensioni delle risposte alle richieste in blocco

Per ridurre la dimensione delle OpenSearch risposte, escludi i campi non necessari con il parametro. `filter_path` Assicurati di non escludere i campi necessari per identificare o provare nuovamente le richieste non riuscite. Per maggiori informazioni ed esempi, consulta the section called “Riduzione delle dimensioni della risposta”.

Ottimizzare gli intervalli di aggiornamento

OpenSearch gli indici alla fine hanno una consistenza di lettura. Un'operazione di aggiornamento rende disponibili per la ricerca tutti gli aggiornamenti eseguiti su un indice. L'intervallo di

aggiornamento predefinito è di un secondo, il che significa che OpenSearch esegue un aggiornamento ogni secondo durante la scrittura di un indice.

Meno frequentemente si aggiorna un indice (intervallo di aggiornamento più elevato), migliori sono le prestazioni complessive di indicizzazione. L'aumento dell'intervallo di aggiornamento comporta un ritardo maggiore tra l'aggiornamento dell'indice e la disponibilità dei nuovi dati per la ricerca. Imposta l'intervallo di aggiornamento al livello più alto che puoi tollerare per migliorare le prestazioni complessive.

Consigliamo di impostare il parametro `refresh_interval` per tutti gli indici su 30 secondi o più.

Abilitare la regolazione automatica

Auto-Tune utilizza i parametri di prestazioni e utilizzo del OpenSearch cluster per suggerire modifiche alle dimensioni delle code, alle dimensioni della cache e alle impostazioni della macchina virtuale Java (JVM) sui nodi. Queste modifiche facoltative migliorano la velocità e la stabilità del cluster. È possibile ripristinare le impostazioni predefinite OpenSearch del servizio in qualsiasi momento. La regolazione automatica è abilitata per impostazione predefinita sui nuovi domini a meno che non venga esplicitamente disabilitata.

Consigliamo di abilitare la regolazione automatica su tutti i domini e di impostare una finestra di manutenzione ricorrente o di rivedere periodicamente i relativi suggerimenti.

Sicurezza

Le seguenti best practice si applicano alla protezione dei domini.

Abilitare il controllo granulare degli accessi

Il controllo granulare degli accessi consente di controllare chi può accedere a determinati dati all'interno di un dominio di servizio. OpenSearch Rispetto al controllo degli accessi generalizzato, il controllo granulare degli accessi fornisce a ciascun cluster, indice, documento e campo la propria policy specifica per l'accesso. I criteri di accesso possono essere basati su una serie di fattori, tra cui il ruolo della persona che richiede l'accesso e l'azione che intende eseguire sui dati. Ad esempio, potresti concedere a un utente l'accesso per scrivere su un indice, mentre a un altro potrebbe essere concesso l'accesso solo per leggere i dati sull'indice senza apportare alcuna modifica.

Il controllo granulare degli accessi consente ai dati con requisiti di accesso diversi di esistere nello stesso spazio di storage senza incorrere in problemi di sicurezza o conformità.

Si consiglia di abilitare il controllo granulare degli accessi sui domini.

Distribuire domini all'interno di un VPC

Posizionare il dominio del OpenSearch servizio all'interno di un cloud privato virtuale (VPC) consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno del VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie a loro isolamento logico, i domini che si trovano all'interno di un VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici.

Consigliamo di creare domini all'interno di un VPC.

Applicare una policy di accesso restrittiva

Anche se il tuo dominio è implementato all'interno di un VPC, è meglio implementare la sicurezza a più livelli. Assicurati di controllare la configurazione delle tue attuali policy di accesso.

Applica una politica di accesso restrittiva basata sulle risorse ai tuoi domini e segui il principio del privilegio minimo quando concedi l'accesso all'API di configurazione e alle operazioni dell'API. OpenSearch Come regola generale, evita di utilizzare il principale utente anonimo`"Principal": {"AWS": "*" }` nelle policy di accesso.

Esistono tuttavia alcune situazioni in cui è accettabile utilizzare una policy di accesso aperto, ad esempio quando abiliti il controllo degli accessi granulare. Una policy di accesso aperto può consentirti di accedere al dominio nei casi in cui la firma delle richieste è difficile o impossibile, ad esempio da determinati client e strumenti.

Abilitare la crittografia dei dati a riposo

OpenSearch I domini di servizio offrono la crittografia dei dati inattivi per impedire l'accesso non autorizzato ai dati. Encryption at rest utilizza AWS Key Management Service (AWS KMS) per archiviare e gestire le chiavi di crittografia e l'algoritmo Advanced Encryption Standard con chiavi a 256 bit (AES-256) per eseguire la crittografia.

Se il dominio archivia i dati sensibili, abilita la crittografia dei dati a riposo.

Abilita la crittografia node-to-node

La ode-to-node crittografia N fornisce un ulteriore livello di sicurezza oltre alle funzionalità di sicurezza predefinite di OpenSearch Service. Implementa Transport Layer Security (TLS) per tutte le

comunicazioni tra i nodi che vengono forniti all'interno. OpenSearch Nessuna ode-to-node crittografia, tutti i dati inviati al dominio del OpenSearch servizio tramite HTTPS rimangono crittografati in transito mentre vengono distribuiti e replicati tra i nodi.

Se il tuo dominio memorizza dati sensibili, abilita node-to-node la crittografia.

Monitora con AWS Security Hub

Monitora l'utilizzo del OpenSearch Servizio in relazione alle migliori pratiche di sicurezza utilizzando AWS Security Hub. Security Hub utilizza controlli di sicurezza per valutare le configurazioni delle risorse e gli standard di sicurezza per aiutarti a rispettare vari framework di conformità. Per ulteriori informazioni sull'utilizzo di Security Hub per valutare le risorse del OpenSearch Servizio, vedere Amazon OpenSearch Service i controlli nella Guida per l'AWS Security Hub utente.

Ottimizzazione dei costi

Le seguenti best practice si applicano all'ottimizzazione e al risparmio sui costi OpenSearch del Servizio.

Utilizzare tipi di istanza di ultima generazione

OpenSearch Service adotta sempre nuovi tipi di istanze Amazon EC2 che offrono prestazioni migliori a un costo inferiore. Si consiglia di utilizzare sempre istanze di ultima generazione.

Non utilizzare istanze T2 o `t3.small` per i domini di produzione in quanto possono diventare instabili in presenza di carichi pesanti sostenuti. Le istanze `r6g.large` sono un'opzione per piccoli carichi di lavoro di produzione (sia come nodi di dati che come nodi principali dedicati).

Utilizzo dei volumi gp3 di Amazon EBS più recenti

OpenSearch i nodi di dati richiedono uno storage a bassa latenza e ad alto throughput per fornire indicizzazione e query rapide. Utilizzando i volumi gp3 Amazon EBS, ottieni prestazioni di base (IOPS e velocità di trasmissione effettiva) più elevate a un costo inferiore del 9,6% rispetto al tipo di volume gp2 Amazon EBS offerto in precedenza. È possibile fornire IOPS evelocità di trasmissione effettiva aggiuntivi indipendentemente dalle dimensioni del volume tramite gp3. Questi volumi sono inoltre più stabili rispetto ai volumi della generazione precedente in quanto non utilizzano crediti di espansione. Il tipo di volume gp3 raddoppia anche i limiti di dimensione del volume del tipo di per-data-node volume gp2. Con questi volumi più grandi, è possibile ridurre il costo dei dati passivi aumentando la quantità di spazio di archiviazione per nodo di dati.

Utilizzo UltraWarm e conservazione a freddo dei dati di registro delle serie temporali

Se li utilizzi OpenSearch per l'analisi dei log, trasferisci i dati in una cella frigorifera per ridurre i costi. UltraWarm Utilizza Index State Management (ISM) per migrare i dati tra livelli di storage e gestire la conservazione dei dati.

UltraWarmoffre un modo conveniente per archiviare grandi quantità di dati di sola lettura in Service. OpenSearch UltraWarm utilizza Amazon S3 per lo storage, il che significa che i dati sono immutabili e ne è necessaria solo una copia. Paghi solo per lo spazio di archiviazione equivalente alla dimensione delle partizioni primarie negli indici. Le latenze per le UltraWarm query crescono con la quantità di dati S3 necessari per soddisfare la query. Dopo che i dati sono stati memorizzati nella cache dei nodi, le query sugli indici hanno prestazioni simili alle query sugli UltraWarm indici caldi.

Lo storage a freddo è supportato anche da S3. Quando è necessario interrogare dati non aggiornati, è possibile collegarli in modo selettivo ai nodi esistenti. UltraWarm I cold data comportano gli stessi costi di storage gestito UltraWarm, ma gli oggetti in cold storage non consumano le risorse dei UltraWarm nodi. Pertanto, la conservazione a freddo offre una notevole capacità di archiviazione senza influire sulle dimensioni o sul numero dei UltraWarm nodi.

UltraWarm diventa conveniente quando si dispone di circa 2,5 TiB di dati da migrare dallo storage a caldo. Monitora il tasso di riempimento e pianifica di spostare gli indici UltraWarm prima di raggiungere quel volume di dati.

Rivedere i suggerimenti per le istanze riservate

Considera l'acquisto di istanze riservate (RI) dopo aver ottenuto una buona linea guida sulle prestazioni e sul consumo di calcolo. Gli sconti partono dal 30% circa per prenotazioni di 1 anno senza anticipo e possono aumentare fino al 50% per tutti gli impegni anticipati di 3 anni.

Dopo aver osservato un funzionamento stabile per almeno 14 giorni, consulta di nuovo la sezione Suggerimenti sulle istanze riservate in Cost Explorer. L'intestazione Amazon OpenSearch Service mostra consigli di acquisto del RI specifici e risparmi previsti.

Dimensionamento dei domini Amazon OpenSearch Service

Non esiste un metodo perfetto per dimensionare i domini di Amazon OpenSearch Service. Tuttavia, partendo da una comprensione delle tue esigenze di storage, del servizio e di OpenSearch se stesso, puoi fare una stima iniziale approfondita delle tue esigenze hardware. Questa stima può essere

utilizzata come punto di partenza per l'aspetto più importante del dimensionamento dei domini: testarli con carichi di lavoro rappresentativi e monitorare le prestazioni.

Argomenti

Calcolo dei requisiti di archiviazione

La maggior parte dei OpenSearch carichi di lavoro rientra in una delle due grandi categorie:

- Indice di lunga durata: scrivi codice che elabora i dati in uno o più OpenSearch indici e quindi aggiorna tali indici periodicamente man mano che i dati di origine cambiano. Alcuni esempi comuni riguardano la ricerca su siti Web, documenti ed e-commerce.
- Indici in sequenza: i dati fluiscono in modo continuo in un set di indici temporanei, con un periodo di indicizzazione e una finestra di conservazione, ad esempio un set di indici giornalieri che viene conservato per due settimane. Alcuni esempi comuni sono le analisi di log, l'elaborazione delle serie temporali e le analisi clickstream.

Per i carichi di lavoro dell'indice di lunga durata, è possibile esaminare i dati di origine sul disco e determinare facilmente la quantità di spazio di archiviazione che consuma. Se i dati provengono da più origini, devi aggiungere tali origini.

Per gli indici in sequenza, puoi moltiplicare la quantità di dati generati durante un periodo di tempo rappresentativo dal periodo di conservazione. Ad esempio, se generi 200 MiB di dati di log all'ora, questi corrispondono a 4,7 GiB al giorno, 66 GiB di dati in qualsiasi momento, se disponi di un periodo di retention di due settimane.

Le dimensioni dei dati di origine, tuttavia, sono solo un aspetto delle esigenze di archiviazione. È·necessario anche considerare quanto segue:

- Numero di repliche: ogni replica è una copia completa di un indice e richiede la stessa quantità di spazio su disco. Per impostazione predefinita, ogni OpenSearch indice ha una replica. Ne consigliamo almeno una per evitare la perdita di dati. Le repliche, inoltre, migliorano le prestazioni di ricerca, perciò potresti volerne di più se hai un carico di lavoro gravoso in lettura. Utilizzare `PUT /my-index/_settings` per aggiornare l'impostazione `number_of_replicas` per l'indice.

- OpenSearch sovraccarico di indicizzazione: la dimensione su disco di un indice varia. La dimensione totale dei dati di origine e dell'indice spesso è pari al 110% dell'origine, dove l'indice rappresenta fino al 10% dei dati di origine. Dopo l'indicizzazione dei dati, è possibile utilizzare l'API `_cat/indices?v` e il valore `pri.store.size` per calcolare il sovraccarico esatto. `_cat/allocation?v` fornisce anche un riepilogo utile.
- Spazio riservato per il sistema operativo: per impostazione predefinita, Linux riserva il 5% del file system per l'utente `root` per i processi critici, il ripristino del sistema e per evitare problemi di frammentazione del disco.
- OpenSearch Sovraccarico del OpenSearch servizio: il servizio riserva il 20% dello spazio di archiviazione di ogni istanza (fino a 20 GiB) per fusioni di segmenti, log e altre operazioni interne.

  Data la dimensione massima di 20 GiB, la quantità totale di spazio riservato può variare notevolmente in funzione del numero di istanze nel tuo dominio. Ad esempio, un dominio può avere tre istanze `m6g.xlarge.search`, ognuna con 500 GiB di spazio di archiviazione, per un totale di 1,46 TiB. In questo caso, il totale di spazio riservato è solo 60 GiB. Un altro dominio può avere 10 istanze `m3.medium.search`, ognuna con 100 GiB di spazio di archiviazione, per un totale di 0,98 TiB. In questo caso, il totale di spazio riservato è di 200 GiB, anche se il primo dominio è il 50% più grande.

  Nella formula seguente, applichiamo una stima "nel peggiore dei casi" per un sovraccarico. Questa stima include spazio libero aggiuntivo per ridurre al minimo l'impatto degli errori dei nodi e delle interruzioni delle zone di disponibilità.

Riepilogando, se si dispone di 66 GiB di dati in qualsiasi momento e si desidera una replica, il requisito di archiviazione minimo è più vicino a 66* 2* 1,1/0,95/0,8 = 191 GiB. Puoi generalizzare il calcolo come indicato di seguito:

Dati di origine* (1+ numero di repliche) * (1+ sovraccarico di indicizzazione)/(1 - spazio riservato Linux)/(1 - sovraccarico del servizio) = requisito minimo di archiviazione OpenSearch

In alternativa, puoi utilizzare questa versione semplificata:

Dati di origine * (1 + Numero di repliche) * 1,45 = Requisito di minimo di archiviazione

Lo spazio di archiviazione insufficiente è una delle cause più comuni di instabilità del cluster. Pertanto quando scegli tipi di istanze, numero di istanze e volumi di archiviazione dovresti controllare i numeri.

Esistono altre considerazioni di archiviazione:

- Se i requisiti di archiviazione minimi superano 1 PB, consultare the section called “Scala in petabyte”.
- Se disponi di indici in sequenza e desideri utilizzare un'architettura a caldo/ad accesso frequente, consulta the section called “UltraWarm archiviazione”.

Scelta del numero di partizioni

Dopo aver individuato i requisiti di archiviazione, è possibile esaminare la strategia di indicizzazione. Per impostazione predefinita, in OpenSearch Service, ogni indice è suddiviso in cinque shard primari e una replica (per un totale di 10 shard). Questo comportamento è diverso da quello open source OpenSearch, che utilizza per impostazione predefinita uno shard primario e uno di replica. Poiché non è possibile modificare facilmente il numero di partizioni primarie per un indice esistente, è necessario decidere il numero di partizioni prima di indicizzare il primo documento.

L'obiettivo generale della scelta di un numero di partizioni è distribuire un indice in modo uniforme su tutti i nodi di dati del cluster. Tuttavia, queste partizioni non devono essere troppo grandi o troppo numerose. Una buona regola è cercare di mantenere le dimensioni delle partizioni tra 10 e 30 GiB per i carichi di lavoro in cui la latenza di ricerca è un obiettivo chiave delle prestazioni e 30-50 GiB per i carichi di lavoro pesanti in termini di scrittura, come l'analisi dei log.

Gli shard di grandi dimensioni possono rendere difficile il ripristino in caso di guasto, ma poiché ogni shard utilizza una certa quantità di CPU e memoria, avere troppi shard di piccole dimensioni può causare problemi di prestazioni ed errori di memoria insufficiente. OpenSearch In altre parole, gli shard devono essere sufficientemente piccoli da consentire all'istanza di OpenSearch Service sottostante di gestirli, ma non così piccoli da sovraccaricare inutilmente l'hardware.

Ad esempio, se disponi di 66 GiB di dati. Non si prevede che il numero aumenti nel corso del tempo e si desidera mantenere le dimensioni delle partizioni attorno a 30 GiB ciascuna. Il numero di partizioni perciò deve essere circa 66* 1,1/30 = 3. Puoi generalizzare il calcolo come indicato di seguito:

(Dati di origine + Spazio per crescere) * (1 + Gestione indicizzazione)/Dimensione desiderata della partizione = Numero approssimativo di partizioni primarie

Questa equazione aiuta a compensare la crescita dei dati nel tempo. Se si prevede che quegli stessi 66 GiB di dati quadruplicheranno l'anno successivo, il numero approssimativo di partizioni sarà (66+198) * 1,1/30 = 10. Ricorda, tuttavia, che non disponi ancora di questi 198 GiB di dati aggiuntivi. Verificare che la preparazione per il futuro non crei partizioni inutilmente piccole che consumano enormi quantità di CPU e memoria nel presente. In questo caso, 66* 1,1/10 partizioni = 7,26 GiB

per partizione. Queste partizioni consumeranno risorse aggiuntive e sono inferiori all'intervallo di dimensione consigliato. Potreste prendere in considerazione l'idea di optare per middle-of-the-road un approccio a sei shard, che vi lascerà con shard da 12 GiB oggi e shard da 48 GiB in futuro. Quindi, si potrebbe iniziare con tre partizioni e reindicizzare i dati quando le partizioni superano i 50 GiB.

Un problema molto meno comune comporta la limitazione del numero di partizioni per nodo. Se si dimensionano le partizioni in modo appropriato, in genere si esaurisce lo spazio su disco molto prima di rispettare questo limite. Ad esempio, un'istanza `m6g.large.search` ha una dimensione massima del disco di 512 GiB. Se si rimane al di sotto dell'80% di utilizzo del disco e si dimensionano le partizioni a 20 GiB, può ospitare circa 20 partizioni. Elasticsearch 7. x e versioni successive, e tutte le versioni di OpenSearch, hanno un limite di 1.000 shard per nodo. Per regolare il numero massimo di partizioni per nodo, configura l'impostazione `cluster.max_shards_per_node`. Per un esempio, consulta Impostazioni del cluster.

Il dimensionamento appropriato delle partizioni mantiene l'utente quasi sempre al di sotto di questo limite, ma è anche possibile considerare il numero di partizioni per ogni GiB di heap Java. Su un dato nodo, non avere più di 25 partizioni per GiB di heap Java. Ad esempio, un'istanza `m5.large.search` ha una memoria heap di 4 GiB, quindi ogni nodo non deve avere più di 100 partizioni. A quel numero di partizioni, ogni partizione ha una dimensione di circa 5 GiB, il che è ben al di sotto della nostra raccomandazione.

Scelta del tipo di istanza e test

Dopo aver calcolato i requisiti di archiviazione e scelto il numero di partizioni di cui si ha bisogno, è possibile iniziare a prendere decisioni sull'hardware. I requisiti hardware variano in modo significativo in base al carico di lavoro, ma possiamo comunque offrire alcune raccomandazioni di base.

In generale, i limiti di archiviazione per ogni tipo di istanza si mappano sulla quantità di CPU e memoria di cui si potrebbe aver bisogno per i carichi di lavoro leggeri. Ad esempio, un'istanza `m6g.large.search` dispone di dimensioni di volume EBS massime di 512 GiB, 2 core vCPU e 8 GiB di memoria. Se il cluster dispone di molte partizioni, esegue aggregazioni fiscali, aggiorna frequentemente i documenti o elabora un numero elevato di query, tali risorse potrebbero non essere sufficienti per le tue esigenze. Se ritieni che il tuo cluster rientri in una di queste categorie, prova a partire da una configurazione più vicina a 2 core vCPU e 8 GiB di memoria per ogni 100 GiB di archiviazione.

> **Tip**
>
> Per un riepilogo delle risorse hardware allocate a ciascun tipo di istanza, consulta i prezzi di Amazon OpenSearch Service.

Tuttavia, anche tali risorse potrebbero essere insufficienti. Alcuni OpenSearch utenti segnalano di aver bisogno di molte più risorse per soddisfare i propri requisiti. Trovare l'hardware appropriato per il tuo carico di lavoro significa fare una stima iniziale efficace, effettuare test con carichi di lavoro rappresentativi, apportare eventuali modifiche ed effettuare nuovamente il test.

Fase 1: Esecuzione di una stima iniziale

Per iniziare, consigliamo un minimo di tre nodi per evitare potenziali OpenSearch problemi, come uno stato cerebrale diviso (quando un'interruzione della comunicazione porta a un cluster con due nodi principali). Se si dispone di tre nodi master dedicati, consigliamo un minimo di due nodi di dati per la replica.

Fase 2: Calcolo dei requisiti di archiviazione per nodo

Se hai un requisito di archiviazione di 184 GiB e il numero minimo raccomandato di tre nodi, per trovare la quantità di spazio di archiviazione richiesta da ogni nodo puoi utilizzare l'equazione 184/3 = 61 GiB. In questo esempio, puoi selezionare tre istanze `m6g.large.search`, di cui ognuna utilizza un volume di archiviazione EBS di 90 GiB in modo da disporre di una rete di sicurezza e di spazio per la crescita nel corso del tempo. Questa configurazione fornisce 6 core vCPU e 24 GiB di memoria, quindi è ideale per i carichi di lavoro più leggeri.

Per un esempio più sostanziale, considerare un requisito di archiviazione di 14 TiB e un carico di lavoro pesante. In questo caso, è possibile scegliere di avviare il test con 2* 144 = 288 core vCPU e 8* 144 = 1152 GiB di memoria. Questi numeri portano a circa 18 istanze `i3.4xlarge.search`. Se non è necessaria un'archiviazione veloce locale, puoi anche testare 18 istanze `r6g.4xlarge.search`, ciascuna con un volume di archiviazione EBS di 1 TiB.

Se il cluster include centinaia di terabyte di dati, consulta the section called “Scala in petabyte”.

Fase 3: Esecuzione di test rappresentativi

Dopo aver configurato il cluster, puoi aggiungere gli indici utilizzando il numero di shard calcolato in precedenza, eseguire alcuni test rappresentativi sui client utilizzando un set di dati realistico e monitorare le CloudWatch metriche per vedere come il cluster gestisce il carico di lavoro.

Fase 4: Riuscita o iterazione

Se le prestazioni soddisfano le tue esigenze, i test hanno esito positivo e le CloudWatch metriche sono normali, il cluster è pronto per l'uso. Ricorda di impostare CloudWatch allarmi per rilevare un utilizzo non corretto delle risorse.

Se le prestazioni non sono accettabili, i test hanno esito negativo o `CPUUtilization` o `JVMMemoryPressure` sono elevati, potrebbe essere necessario scegliere un altro tipo di istanza (o aggiungere istanze) e continuare il test. Man mano che aggiungi istanze, riequilibra OpenSearch automaticamente la distribuzione degli shard in tutto il cluster.

Poiché è più semplice misurare le capacità in eccesso di un cluster con più potenza rispetto al disavanzo di uno con meno potenza, consigliamo di iniziare con un cluster di dimensioni maggiori rispetto alle tue esigenze. Successivamente, suggeriamo di testare e ridimensionare fino a un cluster efficiente che disponga di risorse aggiuntive per garantire operazioni stabili durante i periodi di maggiore attività.

I cluster di produzione o i cluster con stati complessi traggono vantaggio dai nodi master dedicati, che migliorano le prestazioni e l'affidabilità del cluster.

Scalabilità in petabyte in Amazon Service OpenSearch

I domini Amazon OpenSearch Service offrono storage collegato fino a 3 PB. È possibile configurare un dominio con 200 `i3.16xlarge.search` tipi di istanza, ognuna con un'archiviazione di 15 TB. A causa dell'enorme differenza in scala, le raccomandazioni per i domini di queste dimensioni differiscono dalle nostre raccomandazioni generali. In questa sezione sono riportate le considerazioni sulla creazione di domini, sui costi, sull'archiviazione e sulle dimensioni delle partizioni.

Anche se questa sezione di frequente fa riferimento ai tipi di istanza `i3.16xlarge.search`, è possibile utilizzare diversi altri tipi di istanza per raggiungere 1 PB di archiviazione di dominio totale.

Creazione di domini

I domini di queste dimensioni superano il limite predefinito di 80 istanze per dominio. Per richiedere un aumento del limite fino a 200 istanze per dominio, aprire una pratica nel Centro assistenzaAWS.

Prezzi

Prima di creare un dominio di queste dimensioni, consulta la pagina dei prezzi di Amazon OpenSearch Service per assicurarti che i costi associati corrispondano alle tue aspettative.

Esamina the section called “UltraWarm archiviazione” per vedere se un'architettura a caldo si adatta al tuo caso d'uso.

Archiviazione

I tipi di istanza `i3` sono stati appositamente progettati per fornire un'archiviazione non-volatile memory express (NVMe) locale rapida. Poiché questo storage locale tende a offrire vantaggi in termini di prestazioni rispetto ad Amazon Elastic Block Store, i volumi EBS non sono un'opzione quando si selezionano questi tipi di istanze in OpenSearch Service. Se si preferisce una archiviazione EBS, utilizzare un altro tipo di istanza, ad esempio `r6.12xlarge.search`.

Dimensioni e conteggio di partizioni

Una OpenSearch linea guida comune è quella di non superare i 50 GB per shard. Considerato il numero di partizioni necessarie per gestire domini di grandi dimensioni e le risorse disponibili per le istanze `i3.16xlarge.search`, consigliamo una dimensione della partizione pari a 100 GB.

Ad esempio, se si dispone di 450 TB di dati di origine e si desidere una replica, il requisito di archiviazione minimo è più vicino a 450 TB* 2* 1,1/0,95 = 1,04 PB. Per una spiegazione del calcolo, consulta the section called “Calcolo dei requisiti di archiviazione”. Anche se 1,04 PB/15 TB = 70 istanze, è possibile selezionare 90 o più istanze `i3.16xlarge.search` per garantire una rete di sicurezza per l'archiviazione, gestire i guasti dei nodi e tenere conto di alcune variazioni nella quantità di dati nel tempo. Ogni istanza aggiunge altri 20 GiB al requisito di archiviazione minimo, ma per dischi di queste dimensioni, questi 20 GiB sono quasi trascurabili.

Controllare il numero di shard è complicato. OpenSearch gli utenti spesso ruotano gli indici su base giornaliera e conservano i dati per una o due settimane. In questo caso, può essere utile distinguere tra partizioni "attive" e "inattive". Le partizioni attive sono attivamente oggetto di operazioni di lettura o scrittura. Le partizioni inattive potrebbero servire le richieste occasionali di lettura, ma sono fondamentalmente inattive. In generale, è consigliabile mantenere il numero di partizioni attive al di sotto di alcune migliaia. Se il numero di partizioni attive si avvicina a 10.000, potrebbero emergere rischi considerevoli in termini di prestazioni e stabilità.

Per calcolare il numero di partizioni primarie, utilizzare questa formula: 450.000 GB* 1,1/100 GB per partizione = 4.950 partizioni. Raddoppiando il numero per tenere conto delle repliche, raggiungiamo 9.900 partizioni, il che diventa motivo di grande preoccupazione se tutte le partizioni sono attive. Tuttavia, se si ruotano gli indici e solo 1/7° o 1/14° delle partizioni è attivo in un dato giorno (1.414 o 707 partizioni, rispettivamente), il cluster potrebbe funzionare perfettamente. Come sempre, la fase più importante del dimensionamento e della configurazione del dominio è eseguire il test rappresentativo del client utilizzando un set di dati realistico.

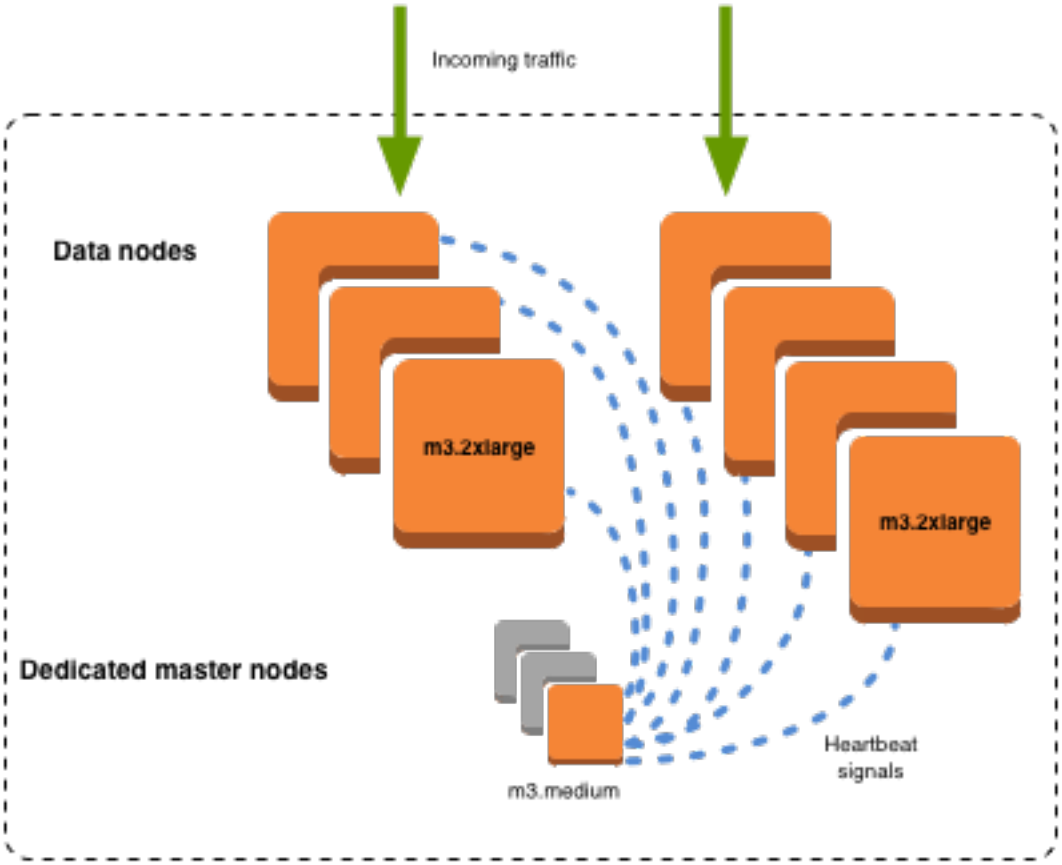
Nodi master dedicati in Amazon OpenSearch Service

Amazon OpenSearch Service utilizza nodi master dedicati per aumentare la stabilità del cluster. Un nodo master dedicato esegue task di gestione cluster ma non conserva dati né risponde a richieste di caricamento dei dati. L'offload dei task di gestione del cluster aumenta la stabilità del dominio. Come tutti gli altri tipi di nodo, per ogni nodo principale dedicato si paga una tariffa oraria.

I nodi master dedicati eseguono le seguenti attività di gestione del cluster:

- Monitora tutti i nodi del cluster.
- Monitora il numero di indici nel cluster.
- Monitora il numero di partizioni appartenenti a ciascun indice.
- Gestisci le informazioni di instradamento per i nodi del cluster.
- Aggiorna lo stato del cluster dopo aver apportato modifiche allo stato, ad esempio la creazione di un indice e l'aggiunta o la rimozione di nodi nel cluster.
- Replica le modifiche allo stato del cluster in tutti i nodi del cluster.
- Monitora l'integrità di tutti i nodi del cluster inviando segnali heartbeat, segnali periodici che monitorano la disponibilità dei nodi di dati nel cluster.

L'illustrazione seguente mostra un dominio OpenSearch di servizio con 10 istanze. Sette delle istanze sono nodi di dati e tre sono nodi master dedicati. È attivo solo uno dei nodi principali dedicati. I due nodi principali dedicati grigi attenderanno come backup nel caso in cui il nodo principale dedicato attivo riporti un errore. Tutte le richieste di caricamento dati vengono elaborate dai sette nodi di dati e su tutte le attività di gestione del cluster viene effettuato l'offload al nodo master dedicato attivo.



Scelta del numero di nodi principali dedicati

Si consiglia di utilizzare Multi-AZ con Standby, che aggiunge tre nodi master dedicati a ciascun dominio del servizio di produzione. OpenSearch Se utilizzi Multi-AZ senza Standby o Single-AZ, consigliamo comunque tre nodi master dedicati. Non scegliere mai un numero pari di nodi principali dedicati. Quando si sceglie il numero di nodi principali dedicati, tenere presente quanto segue:

- Un nodo master dedicato è esplicitamente vietato da OpenSearch Service perché non è disponibile alcun backup in caso di guasto. Se si prova a creare un dominio con un solo nodo principale dedicato, viene ricevuta un'eccezione di convalida.
- Se hai due nodi principali dedicati, allora il cluster non ha il quorum di nodi necessario per eleggere un nuovo nodo principale in caso di errore.

  Un quorum è il numero di nodi principali dedicati / 2 + 1 arrotondato per difetto al numero intero più vicino. In questo caso: 2 / 2 + 1 = 2. Poiché un nodo master dedicato non è andato a buon fine ed

esiste un solo backup, il cluster non dispone di un quorum e non è in grado di eleggere un nuovo master.

- Tre nodi master dedicati, il numero consigliato, offrono due nodi di backup in caso di guasto del nodo master e il quorum necessario (2) per eleggere un nuovo master.
- Quattro nodi principali dedicati non sono meglio di tre e possono causare problemi se utilizzi più zone di disponibilità.
  - Se un nodo master ha esito negativo, hai il quorum (3) per eleggere un nuovo master. Se due nodi hanno esito negativo, perdi il quorum, in modo analogo a quando disponi di tre nodi master dedicati.
  - In una configurazione con tre zone di disponibilità, due zone hanno un nodo principale dedicato e una zona ne ha due. Se l'AZ subisce un'interruzione, le restanti due AZ non dispongono del quorum necessario (3) per eleggere un nuovo principale.
- Avere cinque nodi master dedicati funziona così come tre e consente di perdere due nodi mantenendo un quorum. Ma poiché solo un nodo principale dedicato è attivo in un dato momento, questa configurazione implica pagare per quattro nodi inattivi. Molti clienti ritengono che questo livello di protezione failover sia eccessivo.

Se un cluster ha un numero pari di nodi idonei per il master OpenSearch e le versioni di Elasticsearch 7. x e versioni successive ignorano un nodo in modo che la configurazione di voto sia sempre un numero dispari. In questo caso, quattro nodi master dedicati sono essenzialmente equivalenti a tre (e due a uno).

> **Note**
>
> Se il cluster non ha il quorum necessario per eleggere un nuovo nodo master, le richieste di lettura e scrittura al cluster non andranno a buon fine. Questo comportamento è diverso da quello OpenSearch predefinito.

Scelta dei tipi di istanza per nodi principali dedicati

Sebbene i nodi master dedicati non elaborino le richieste di ricerca e di interrogazione, la loro dimensione è strettamente correlata alla dimensione dell'istanza e al numero di istanze, indici e frammenti che possono gestire. Per i cluster di produzione, consigliamo almeno i seguenti tipi di istanza per nodi master dedicati.

Queste raccomandazioni sono basate su carichi di lavoro tipici e possono variare in base alle tue esigenze. I cluster con molte partizioni o mappature di campi possono trarre vantaggio da tipi di istanze di dimensioni maggiori. Monitorare i parametri del nodo master dedicato per vedere se è necessario utilizzare un tipo di istanza di dimensioni maggiori.

Conteggio delle istanze	Dimensione della RAM del nodo principale	Numero massimo di partizioni supportato	Tipo di istanza consigliata per il nodo principale dedicato
1-10	8 GiB	10K	`m5.large.search` o `m6g.large.search`
11-30	16 GiB	30K	`c5.2xlarge.search` o `c6g.2xlarge.search`
31-75	32 GiB	40K	`r5.xlarge.search` o `r6g.xlarge.search`
76-125	64 GiB	75K	`r5.2xlarge.search` o `r6g.2xlarge.search`
126-200	128 GiB	75K	`r5.4xlarge.search` o `r6g.4xlarge.search`

- Per informazioni su come alcune modifiche di configurazione possono influenzare sui nodi master dedicati, consulta the section called “Modifiche di configurazione”.
- Per chiarimenti sui limiti del numero di istanze, consulta Quote di dominio e istanze del OpenSearch servizio.

- Per ulteriori informazioni su tipi di istanze specifici, tra cui vCPU, memoria e prezzi, consulta i prezzi di Amazon OpenSearch Service.

CloudWatch Allarmi consigliati per Amazon Service OpenSearch

CloudWatch gli allarmi eseguono un'azione quando una CloudWatch metrica supera un valore specificato per un certo periodo di tempo. Ad esempio, potresti voler AWS inviarti un'e-mail se lo stato di salute del cluster dura più `red` di un minuto. Questa sezione include alcuni allarmi consigliati per Amazon OpenSearch Service e come rispondere ad essi.

Puoi distribuire automaticamente questi allarmi utilizzando. AWS CloudFormationPer uno stack di esempio, consulta il relativo repository. GitHub

> **Note**
>
> Se distribuisci lo CloudFormation stack, gli `KMSKeyInaccessible` allarmi `KMSKeyError` and esisteranno in `Insufficient Data` uno stato perché queste metriche vengono visualizzate solo se un dominio riscontra un problema con la sua chiave di crittografia.

Per ulteriori informazioni sulla configurazione degli allarmi, consulta Creating Amazon CloudWatch Alarms nella Amazon CloudWatch User Guide.

Allarme	Problema
`ClusterStatus.red` il massimo è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	Almeno una partizioni primaria e le relative repliche non sono assegnate a un nodo. Per informazioni, consulta the section called “Cluster in stato rosso”.
`ClusterStatus.yellow` il massimo è >= 1 per 1 minuto, 5 volte consecutive	Almeno una partizione di replica non è allocata per un nodo. Per informazioni, consulta the section called “Stato giallo del cluster”.

Allarme	Problema
`FreeStorageSpace` minimo è <= 20480 per 1 minuto, 1 periodo di tempo consecutivo	Un nodo nel cluster è legato ai 20 GiB di spazio di archiviazione gratuito. Per informazioni, consulta the section called “Mancanza di spazio di archiviazione disponibile”. Tale valore viene espresso in MiB, perciò anziché su 20480, consigliamo di impostarlo al 25% dello spazio di archiviazione per ogni nodo.
`ClusterIndexWritesBlocked` è >= 1 per 5 minuti, 1 periodo di tempo consecutivo	Il cluster sta bloccando le richieste di scrittura. Per informazioni, consulta the section called “ClusterBlockException”.
`Nodes` minimo è x per 1 giorno, 1 periodo di tempo consecutivo	x è il numero di nodi del cluster. Questo allarme indica che almeno un nodo nel cluster è stato irraggiungibile per un giorno. Per informazioni, consulta the section called “Nodi cluster con errori”.

`AutomatedSnapshotFailure` il massimo è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	Uno snapshot automatico ha restituito un errore. Questo errore è spesso il risultato di uno stato del cluster rosso. Per informazioni, consulta the section called “Cluster in stato rosso”.
	
	Per un riepilogo di tutti gli snapshot automatici e alcune informazioni sui fallimenti, è possibile provare una delle seguenti richieste:
	
	`GET domain_endpoint /_snapshot/cs-automated/_all`
	`GET domain_endpoint /_snapshot/cs-automated-enc/_all`

`CPUUtilization` o `WarmCPUUtilization` massimo è >= 80% per 15 minuti, 3 periodi di tempo consecutivi	A volte può verificarsi un utilizzo della CPU al 100%, ma un uso elevato e sostenuto può rappresentare un problema. Consigliamo di utilizzare tipi di istanza più grandi o aggiungere istanze.

Allarme	Problema
`JVMMemory Pressure` il massimo è >= 95% per 1 minuto, 3 volte consecutive	Sui cluster potrebbero verificarsi errori di esaurimento della memoria nel caso in cui l'utilizzo aumenti. Prendi in considerazione la possibilità di scalare verticalmente. OpenSearch Il servizio utilizza metà della RAM di un'istanza per l'heap Java, fino a una dimensione dell'heap di 32 GiB. Puoi scalare le istanze verticalmente fino a 64 GiB di RAM e poi scalare orizzontalmente aggiungendo le istanze.
`OldGenJVM MemoryPressure` il massimo è >= 80% per 1 minuto, 3 volte consecutive	
`MasterCPU Utilization` il massimo è >= 50% per 15 minuti, 3 periodi di tempo consecutivi	Potresti utilizzare tipi di istanza di dimensioni maggiori per i tuoi nodi master dedicati. A causa del loro ruolo nella stabilità del cluster e nelle distribuzioni blu/verde, i nodi master dedicati devono avere un utilizzo ridotto della CPU rispetto ai nodi di dati.
`MasterJVM MemoryPressure` il massimo è >= 95% per 1 minuto, 3 volte consecutive	
`MasterOld GenJVMMem oryPressure` il massimo è >= 80% per 1 minuto, 3 volte consecutive	
`KMSKeyError` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	La chiave di AWS KMS crittografia utilizzata per crittografare i dati inattivi nel dominio è disabilitata. Riabilitala per ripristinare le normali operazioni. Per ulteriori informazioni, consultare the section called “Crittografia a riposo”.

Allarme	Problema
`KMSKeyInaccessible` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	La chiave di AWS KMS crittografia utilizzata per crittografare i dati archiviati nel dominio è stata eliminata o ha revocato le sue concessioni al Servizio. OpenSearch Non è possibile recuperare i domini che sono in questo stato. Se hai uno snapshot manuale, puoi utilizzarlo per migrare a un nuovo dominio. Per ulteriori informazioni, consulta the section called “Crittografia a riposo”.
`shards.active` è >= 30000 per 1 minuto, 1 periodo di tempo consecutivo	Il numero totale di partizioni primarie e di replica attive è maggiore di 30.000. È possibile che gli indici vengano ruotati troppo frequentemente. Prendi in considerazione l'utilizzo di ISM per rimuovere gli indici una volta raggiunta un'età specifica.
Allarmi `5xx` >= 10% di `OpenSearchRequests`	Uno o più nodi di dati potrebbero essere sovraccarichi o le richieste non vengono completate entro il periodo di timeout inattivo. Considera il passaggio a tipi di istanza più grandi o di aggiungere più nodi al cluster. Conferma che stai seguendo le best practice per l'architettura di partizioni e cluster.
`MasterReachableFromNode` il massimo è < 1 per 5 minuti, 1 volta consecutiva	Questo avviso indica che il nodo principale è stato arrestato o non è raggiungibile. Questi errori sono in genere il risultato di un problema di connettività di rete o di AWS dipendenza.
`ThreadpoolWriteQueue` medio è >= 100 per 1 minuto, 1 periodo di tempo consecutivo	Il cluster sta riscontrando un'elevata concorrenza di indicizzazione. Esamina e controlla le richieste di indicizzazione o aumenta le risorse del cluster.
`ThreadpoolSearchQueue` medio è >= 500 per 1 minuto, 1 periodo di tempo consecutivo	Il cluster sta riscontrando un'elevata concorrenza di ricerca. Considera il dimensionamento del cluster. È inoltre possibile aumentare le dimension i della coda di ricerca, ma un aumento eccessivo può causare errori di memoria.

Allarme	Problema
`Threadpool SearchQueue` massimo è >= 5000 per 1 minuto, 1 periodo di tempo consecutivo	
L'aumento di `Threadpool SearchRejected` SUM è >=1 {espressione matematica DIFF ()} per 1 minuto, 1 volta consecutiva	Questi allarmi ti informano di problemi di dominio che potrebbero influire sulle prestazioni e sulla stabilità.
L'aumento di `Threadpool WriteRejected` SUM è >=1 {espressione matematica DIFF ()} per 1 minuto, 1 volta consecutiva	

> **Note**
>
> Se si desidera soltanto visualizzare i parametri, consultare the section called “Monitoraggio dei parametri del cluster”.

Altri allarmi che potresti prendere in considerazione

Valuta la possibilità di configurare i seguenti allarmi a seconda delle funzionalità di OpenSearch servizio che utilizzi regolarmente.

Allarme	Problema
`WarmFreeStorageSpace` è >= 10%	Hai raggiunto il 10% del tuo accumulo di calore totale gratuito. `WarmFreeStorageSpace` misura la somma dello spazio di archiviazione caldo libero in MiB. UltraWarm utilizza Amazon S3 anziché dischi collegati.
`HotToWarmMigrationQueueSize` è >= 20 per 1 minuto, 3 periodi di tempo consecutivi	Un numero elevato di indici passa contemporaneamente dallo storage a caldo a quello di storage. UltraWarm Considera il dimensionamento del cluster.
`HotToWarmMigrationSuccessLatency` è >= 1 giorno, 1 periodo di tempo consecutivo	Configura questo allarme in modo da ricevere una notifica se la latenza x di `HotToWarmMigrationSuccessCount` è superiore a 24 ore, se stai cercando di utilizzare indici giornalieri.
`WarmJVMMemoryPressure` il massimo è >= 95% per 1 minuto, 3 volte consecutive	Sui cluster potrebbero verificarsi errori di esaurimento della memoria nel caso in cui l'utilizzo aumenti. Prendi in considerazione la possibilità di scalare verticalmente. OpenSearch Il servizio utilizza metà della RAM di un'istanza per l'heap Java, fino a una dimensione dell'heap di 32 GiB. Puoi scalare le istanze verticalmente fino a 64 GiB di RAM e poi scalare orizzontalmente aggiungendo le istanze.
`WarmOldGenJVMMemoryPressure` il massimo è >= 80% per 1 minuto, 3 volte consecutive	
`WarmToColdMigrationQueueSize` è >= 20 per 1 minuto,	Un numero elevato di indici sta passando contemporaneamente dalla conservazione a freddo. UltraWarm Considera il dimensionamento del cluster.

Allarme	Problema
3 periodi di tempo consecutivi	
`HotToWarmMigrationFailureCount` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	Le migrazioni potrebbero non riuscire durante gli snapshot, le rilocazioni di partizioni o le fusioni forzate. Gli errori durante gli snapshot o il trasferimento di partizioni sono in genere dovuti a errori dei nodi o a problemi di connettività S3. La mancanza di spazio su disco è solitamente la causa sottostante degli errori di unioni forzate.
`WarmToColdMigrationFailureCount` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	Le migrazioni in genere falliscono quando i tentativi di migrazione dei metadati dell'indice nell'archiviazione a freddo non riescono. È possibile che si verifichino degli errori anche durante la rimozione dello stato del cluster di indice a caldo.
`WarmToColdMigrationLatency` è >= 1 giorno, 1 periodo di tempo consecutivo	Configura questo allarme in modo da ricevere una notifica se la latenza x di `WarmToColdMigrationSuccessCount` è superiore a 24 ore, se stai cercando di utilizzare indici giornalieri.
`AlertingDegraded` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	L'indice di avviso è rosso oppure uno o più nodi non sono pianificati.
`ADPluginUnhealthy` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	Il plugin di rilevamento delle anomalie non funziona correttamente a causa di alti tassi di errore o perché uno degli indici utilizzati è rosso.

Allarme	Problema
`AsynchronousSearchFailureRate` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	Almeno una ricerca asincrona non è riuscita nell'ultimo minuto, il che significa che il nodo coordinatore non è riuscito. Il ciclo di vita di una richiesta di ricerca asincrona viene gestito esclusivamente sul nodo del coordinatore, quindi se il coordinatore si interrompe, la richiesta non riesce.
`AsynchronousSearchStoreHealth` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	L'integrità dell'archivio delle risposte di ricerca asincrona nell'indice persistente è rossa. È possibile che si stiano memorizzando risposte asincrone di grandi dimensioni, che possono destabilizzare un cluster. Cerca di limitare le risposte di ricerca asincrone a 10 MB o meno.
`SQLUnhealthy` è >= 1 per 1 minuto, 3 periodi di tempo consecutivi	Il plugin SQL restituisce 5 codici di risposta xx o passa una query DSL non valida a. OpenSearch Risolvi i problemi relativi alle richieste che i client stanno facendo al plug-in.
`LTRStatus.red` è >= 1 per 1 minuto, 1 periodo di tempo consecutivo	Almeno uno degli indici necessari per eseguire il plug-in Learning to Rank (Imparare a classificare) ha partizioni primarie mancanti e non è funzionante.

Riferimento generale per Amazon OpenSearch Service

Amazon OpenSearch Service supporta una varietà di istanze, operazioni, plug-in e altre risorse.

Argomenti

Tipi di istanze supportati in Amazon OpenSearch Service

Amazon OpenSearch Service supporta i seguenti tipi di istanze. Non tutte le regioni supportano tutti i tipi di istanze. Per i dettagli sulla disponibilità, consulta i prezzi OpenSearch di Amazon Service.

Per informazioni su quale tipo di istanza è appropriato per il tuo caso d'uso, consulta the section called “Dimensionamento dei domini”, the section called “Quote delle dimensioni dei volumi EBS” e the section called “Quote di rete”.

Tipi di istanza della generazione attuale

Per prestazioni ottimali, ti consigliamo di utilizzare i seguenti tipi di istanza quando crei nuovi domini OpenSearch di servizio.

Tipo di istanza	Istanze	Restrizioni
O 1	`or1.medium.search` `or1.large.search`	• I tipi di istanza OR1 richiedono la versione OpenSearch 2.11 o successiva. • Le istanze OR1 sono compatibili solo con i nodi master di altri tipi di istanze Graviton (C6g, M6g, R6g).

Tipo di istanza	Istanze	Restrizioni
	or1.xlarge.search or1.2xlarge.search or1.4xlarge.search or1.8xlarge.search or1.12xlarge.search or1.16xlarge.search	

Tipo di istanza	Istanze	Restrizioni

Im4gn	`im4gn.large.search`
	
	`im4gn.xlarge.search`
	
	`im4gn.2xlarge.search`
	
	`im4gn.4xlarge.search`
	
	`im4gn.8xlarge.search`
	
	`im4gn.16xlarge.search`
		• I tipi di istanza Im4gn richiedono Elasticsearch 7.9 o versione successiva o qualsiasi versione di e non supportano i volumi di archiviazione EBS. OpenSearch
		• Le istanze Im4gn sono compatibili solo con altri tipi di istanze Graviton (C6g, M6g, R6g, R6gd). Non è possibile combinare istanze Graviton e non Graviton nello stesso cluster.

Tipo di istanza	Istanze	Restrizioni

C5	`c5.large.search`
	`c5.xlarge.search`
	`c5.2xlarge.search`
	`c5.4xlarge.search`
	`c5.9xlarge.search`
	`c5.18xlarge.search`
		I tipi di istanza C5 richiedono Elasticsearch 5.1 o versione successiva o qualsiasi versione di. OpenSearch

Tipo di istanza	Istanze	Restrizioni

C6g	`c6g.large.search`
	`c6g.xlarge.search`
	`c6g.2xlarge.search`
	`c6g.4xlarge.search`
	`c6g.8xlarge.search`
	`c6g.12xlarge.search`
		• I tipi di istanza C6g richiedono Elasticsearch 7.9 o versione successiva o qualsiasi versione di. OpenSearch
		• Le istanze C6g sono compatibili solo con altri tipi di istanze Graviton (Im4gn, M6g, R6g, R6gd). Non è possibile combinare istanze Graviton e non Graviton nello stesso cluster.

Tipo di istanza	Istanze	Restrizioni

I3	`i3.large.search`
	`i3.xlarge.search`
	`i3.2xlarge.search`
	`i3.4xlarge.search`
	`i3.8xlarge.search`
	`i3.16xlarge.search`
		I tipi di istanza I3 richiedono Elasticsearch 5.1 o versione successiva o qualsiasi versione di e non supportano i volumi di archiviazione EBS. OpenSearch

M5	`m5.large.search`
	`m5.xlarge.search`
	`m5.2xlarge.search`
	`m5.4xlarge.search`
	`m5.12xlarge.search`
		I tipi di istanza M5 richiedono Elasticsearch 5.1 o versione successiva o qualsiasi versione di. OpenSearch

Tipo di istanza	Istanze	Restrizioni

M6g	`m6g.large.search`
	`m6g.xlarge.search`
	`m6g.2xlarge.search`
	`m6g.4xlarge.search`
	`m6g.8xlarge.search`
	`m6g.12xlarge.search`
		• I tipi di istanza M6g richiedono Elasticsearch 7.9 o versione successiva o qualsiasi versione di. OpenSearch
		• Le istanze M6g sono compatibili solo con altri tipi di istanze Graviton (Im4gn, C6g, R6g, R6gd). Non è possibile combinare istanze Graviton e non Graviton nello stesso cluster.

Tipo di istanza	Istanze	Restrizioni

R5	`r5.large.search`
	`r5.xlarge.search`
	`r5.2xlarge.search`
	`r5.4xlarge.search`
	`r5.12xlarge.search`
		I tipi di istanza R5 richiedono Elasticsearch 5.1 o versione successiva o qualsiasi versione di. OpenSearch

Tipo di istanza	Istanze	Restrizioni

R6g	`r6g.large.search`
	`r6g.xlarge.search`
	`r6g.2xlarge.search`
	`r6g.4xlarge.search`
	`r6g.8xlarge.search`
	`r6g.12xlarge.search`
		• I tipi di istanza R6g richiedono Elasticsearch 7.9 o versione successiva o qualsiasi versione di. OpenSearch
		• Le istanze R6g sono compatibili solo con altri tipi di istanze Graviton (Im4gn, C6g, M6g, R6gd). Non è possibile combinare istanze Graviton e non Graviton nello stesso cluster.

Tipo di istanza	Istanze	Restrizioni

R6gd	`r6gd.large.search`
	`r6gd.xlarge.search`
	`r6gd.2xlarge.search`
	`r6gd.4xlarge.search`
	`r6gd.8xlarge.search`
	`r6gd.12xlarge.search`
	`r6gd.16xlarge.search`
		• I tipi di istanza R6gd richiedono Elasticsearch 7.9 o versione successiva o qualsiasi versione di e non supportano i volumi di archiviazione EBS. OpenSearch
		• Le istanze R6gd sono compatibili solo con altri tipi di istanze Graviton (Im4gn, C6g, M6g, R6g). Non è possibile combinare istanze Graviton e non Graviton nello stesso cluster.

Tipo di istanza	Istanze	Restrizioni
T3	`t3.small.search` `t3.medium.search`	• I tipi di istanza T3 richiedono Elasticsearch 5.6 o versione successiva o qualsiasi versione di. OpenSearch • Puoi utilizzare i tipi di istanza T3 solo se il tuo dominio viene fornito senza standby. Per ulteriori informazioni, consulta the section called “Multi-AZ senza Standby”. • Puoi utilizzare i tipi di istanze T3 solo se il numero di istanze per il tuo dominio è pari o inferiore a 10. • I tipi di istanze T3 non supportano UltraWarm storage, cold storage o Auto-Tune.

Tipi di istanza di generazioni precedenti

OpenSearch Il servizio offre tipi di istanze della generazione precedente per gli utenti che hanno ottimizzato le proprie applicazioni in base a tali applicazioni e non hanno ancora effettuato l'aggiornamento. Si consiglia di utilizzare i tipi di istanza della generazione corrente per ottenere le migliori prestazioni, ma continuiamo a supportare i seguenti tipi di istanza della generazione precedente.

Tipo di istanza	Istanze	Restrizioni

C4	`c4.large.search`
	`c4.xlarge.search`
	`c4.2xlarge.search`
	`c4.4xlarge.search`	

Tipo di istanza	Istanze	Restrizioni
	`c4.8xlarge.search`	
I2	`i2.xlarge.search` `i2.2xlarge.search`	

M3	`m3.medium.search`
	`m3.large.search`
	`m3.xlarge.search`
	`m3.2xlarge.search`
		• I tipi di istanze M3 non supportano la crittografia dei dati a riposo, il controllo granulare degli accessi o la ricerca tra cluster.
		• I tipi di istanze M3 hanno restrizioni aggiuntive in base alla OpenSearch versione. Per ulteriori informazioni, consulta the section called “Tipo di istanza M3 non valido”.

M4	`m4.large.search`
	`m4.xlarge.search`
	`m4.2xlarge.search`
	`m4.4xlarge.search`
	`m4.10xlarge.search`	

Tipo di istanza	Istanze	Restrizioni

R3	`r3.large.search`
	`r3.xlarge.search`
	`r3.2xlarge.search`
	`r3.4xlarge.search`
	`r3.8xlarge.search`
		I tipi di istanza R3 non supportano la crittografia dei dati a riposo o il controllo granulare degli accessi.

R4	`r4.large.search`
	`r4.xlarge.search`
	`r4.2xlarge.search`
	`r4.4xlarge.search`
	`r4.8xlarge.search`
	`r4.16xlarge.search`	

Tipo di istanza	Istanze	Restrizioni

T2	`t2.micro.search`
	`t2.small.search`
	`t2.medium.search`
		• Puoi utilizzare i tipi di istanza T2 solo se il conteggio delle istanze per il tuo dominio è pari al massimo a 10.
		• Il tipo di istanza `t2.micro.search` supporta solo Elasticsearch 1.5 e 2.3.
		• I tipi di istanze T2 non supportano la crittografia dei dati inattivi, il controllo granulare degli accessi, UltraWarm lo storage, la conservazione a freddo, la ricerca tra cluster o Auto-Tune.

> **Tip**
>
> Consigliamo di utilizzare tipi di istanze differenti per nodi principali dedicati e nodi di dati.

Funzionalità per versione del motore in Amazon OpenSearch Service

Molte funzionalità OpenSearch del servizio richiedono una OpenSearch versione minima o una versione precedente di Elasticsearch OSS. Se si soddisfa la versione minima di una funzionalità ma la funzionalità non è disponibile nel dominio, aggiornare il software di servizio del dominio.

Caratteristica	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
Supporto per VPC	1.0	1
Richiedere HTTPS per tutto il traffico verso il dominio		

Caratteristica	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
Supporto Multi-AZ		
Nodi master dedicati		
Pacchetti personalizzati		
Endpoint personalizzati		
Pubblicazione di log lenti		
Pubblicazione dei log di errori	1	5.1
Crittografia dei dati a riposo		
Autenticazione Cognito per dashboard OpenSearch		
Aggiornamenti sul posto		

Caratteristica	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
Supporto curatore	Non incluso	5.1
Snapshot automatiche orarie	1	5.3
Nessuna crittografia ode-to-node	1	6.0
Supporto client REST Java di livello elevato		
Compressione delle richieste HTTP e delle risposte		
Avviso	1	6.2
SQL	1	6,5
Funzionalità di ricerca tra cluster	1	6.7
Controllo granulare degli accessi		

Caratteristica	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
Autenticazione SAML per dashboard OpenSearch		
Regolazione automatica		
Reindicizzazione remota		
UltraWarm	1	6.8
Index State Management		
k-NN per distanza euclidea	1	7.1
Rilevamento di anomalie	1	7.4
k-NN per similitudine del coseno	1	7.7
Learning to Rank		

Caratteristica	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
Piped Processing Language (PPL)	1	7.9
OpenSearch Dashboard, report		
OpenSearch Pannelli di controllo Trace Analytics		
Istanze Graviton basate su ARM		
Archiviazione a freddo		
Distanza di marcia, distanza di norma L1 e scripting painless per k-NN	1	7.10
Ricerca asincrona		

Caratteristica	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
Trasformazioni degli indici	1	Non incluso
Replica tra cluster	1.1	7,10
ML Commons	1.3	Non incluso
Notifiche	2.3	Non incluso
Ricerca puntuale nel tempo	2.5	Non incluso
Pipeline di ricerca	2.9	Non incluso
Connettori per l'apprendimento automatico	2.9	Non incluso
Ricerca semantica multimodale	2.11	Non incluso
Origini di dati Direct-Query per Amazon S3	2.11	Non incluso

Per informazioni sui plugin, che abilitano alcune di queste funzionalità e funzionalità aggiuntive, vedere the section called “Plug-in per versione motore”. Per informazioni sull' OpenSearch API per ogni versione, consulta. the section called “Operazioni supportate”

Plugin per versione del motore in Amazon Service OpenSearch

I domini Amazon OpenSearch Service sono preconfezionati con i plug-in della community. OpenSearch Il servizio distribuisce e gestisce automaticamente i plug-in per te, ma distribuisce plug-in diversi a seconda della versione OpenSearch o del sistema operativo Elasticsearch precedente che scegli per il tuo dominio.

La tabella seguente elenca i plugin per OpenSearch versione, nonché le versioni compatibili del precedente sistema operativo Elasticsearch. Include solo i plugin con cui è possibile interagire, non è esaustivo. OpenSearch Il servizio utilizza plug-in aggiuntivi per abilitare le funzionalità di base del servizio, come il plug-in S3 Repository per le istantanee e il plug-in OpenSearchPerformance Analyzer per l'ottimizzazione e il monitoraggio. Per un elenco completo di tutti i plug-in in esecuzione sul dominio, effettuare la seguente richiesta:

```
GET _cat/plugins?v
```

Plug-in	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
ICU Analysis	1	Incluso in tutti i domini
Japanese (kuromoji) Analysis		
Phonetic Analysis	1	2.3
Analisi coreano Seunjeon	1	5.1

Plug-in	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
Smart Chinese Analysis		
Stempel Polish Analysis		
Ingest Attachment Processor		
Ingest User Agent Processor		
Mapper Murmur3		
Mapper Size	1	5.3
Ukrainian Analysis		
OpenSearch avvisare	1	6.2
OpenSearch SQL	1	6,5
OpenSearch sicurezza	1	6.7

Plug-in	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
OpenSearch Index State Management	1	6.8
OpenSearch k-NN	1	7.1
OpenSearch rilevamento di anomalie	1	7.4
IK (Chinese) Analysis	1	7.7
Vietnamese Analysis		
Thai analysis		
Learning to Rank		
OpenSearch ricerca asincrona	1	7.10
OpenSearch replica tra cluster	1.1	7.10

Plug-in	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
OpenSearch osservabilità	1.2	Non supportato
Analisi Nori	1.3	Non supportato
Analisi Pinyin	1.3	Non supportato
STConvert	1.3	Non supportato
Analisi Sudachi	1.3	Non supportato
ML Commons	1.3	Non supportato
OpenSearch notifiche	2.3	Non supportato
Analisi della sicurezza	2.5	Non supportato
Ricerca neurale	2.9	Non supportato
Amazon Personalizza il posizionamento nelle ricerche	2.9	Non supportato
Analisi ebraica	2.11	Non supportato

Plug-in	Versione minima richiesta OpenSearch	Versione minima richiesta di Elasticsearch
HanLP	2.11	Non supportato

Plugin opzionali

Oltre ai plugin preinstallati di default, Amazon OpenSearch Service supporta diversi plugin opzionali per l'analisi del linguaggio. Puoi utilizzare AWS Management Console e AWS CLI per associare un plug-in a un dominio, dissociare un plug-in da un dominio ed elencare tutti i plug-in. Un pacchetto di plugin opzionale è compatibile con una OpenSearch versione specifica e può essere associato solo a domini con quella versione.

Nota che per il plugin Sudachi, quando riassoci un file di dizionario, questo non si riflette immediatamente sul dominio. Il dizionario si aggiorna quando viene eseguita la successiva distribuzione blu/verde sul dominio come parte di una modifica della configurazione o di un altro aggiornamento. In alternativa, puoi creare un nuovo pacchetto con i dati aggiornati, creare un nuovo indice utilizzando questo nuovo pacchetto, reindicizzare l'indice esistente nel nuovo indice e quindi eliminare il vecchio indice. Se preferisci utilizzare l'approccio di reindicizzazione, utilizza un alias di indice in modo da evitare interruzioni del traffico.

I plugin opzionali utilizzano il tipo di pacchetto. `ZIP-PLUGIN` Per ulteriori informazioni sui plugin opzionali, consulta. the section called “Pacchetti personalizzati”

Operazioni supportate in Amazon OpenSearch Service

OpenSearch Il servizio supporta molte versioni OpenSearch e versioni precedenti di Elasticsearch OSS. Le sezioni seguenti mostrano le operazioni supportate dal OpenSearch servizio per ogni versione.

Argomenti

- Differenze significative tra le API
- OpenSearch versione 2.13
- OpenSearch versione 2.11
- OpenSearch versione 2.9
- OpenSearch versione 2.7

- OpenSearch versione 2.5
- OpenSearch versione 2.3
- OpenSearch versione 1.3
- OpenSearch versione 1.2
- OpenSearch versione 1.1
- OpenSearch versione 1.0
- Elasticsearch versione 7.10
- Elasticsearch versione 7.9
- Elasticsearch versione 7.8
- Elasticsearch versione 7.7
- Elasticsearch versione 7.4
- Elasticsearch versione 7.1
- Elasticsearch versione 6.8
- Elasticsearch versione 6.7
- Elasticsearch versione 6.5
- Elasticsearch versione 6.4
- Elasticsearch versione 6.3
- Elasticsearch versione 6.2
- Elasticsearch versione 6.0
- Elasticsearch versione 5.6
- Elasticsearch versione 5.5
- Elasticsearch versione 5.3
- Elasticsearch versione 5.1
- Elasticsearch versione 2.3
- Elasticsearch versione 1.5

Differenze significative tra le API

Impostazioni e statistiche

OpenSearch Il servizio accetta solo richieste `_cluster/settings` PUT all'API che utilizzano il modulo di impostazioni «flat». Rifiuta le richieste che utilizzano il modulo delle impostazioni espanse.

```
// Accepted
PUT _cluster/settings
{
  "persistent" : {
    "action.auto_create_index" : false
  }
}

// Rejected
PUT _cluster/settings
{
  "persistent": {
    "action": {
      "auto_create_index": false
    }
  }
}
```

Il client Java REST di alto livello utilizza il modulo espanso, quindi se è necessario inviare richieste di impostazioni, utilizzare il client di basso livello.

Prima di Elasticsearch 5.3, l'`_cluster/settings`API sui domini di OpenSearch servizio supportava solo il `PUT` metodo HTTP, non il metodo. `GET` OpenSearch e le versioni successive di Elasticsearch supportano il `GET` metodo, come mostrato nell'esempio seguente:

```
GET https://domain-name.region.es.amazonaws.com/_cluster/settings?pretty
```

Ecco un esempio di ritorno:

```
{
  "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"
      }
    }
  }
}
```

Se confronti le risposte di un OpenSearch cluster open source e OpenSearch Service per determinate API di impostazioni e statistiche, potresti notare la mancanza di campi. OpenSearch Il servizio oscura determinate informazioni che rivelano i componenti interni del servizio, come il percorso dei dati del file system da cui proviene `_nodes/stats` o il nome e la versione del sistema operativo da. `_nodes`

Riduzione

L'API `_shrink` può impedire aggiornamenti, modifiche di configurazione ed eliminazioni di domini. Ne sconsigliamo l'utilizzo su domini che eseguono Elasticsearch versioni 5.3 o 5.1. Queste versioni contengono un baco che impedisce il ripristino snapshot di indici ridotti.

Se utilizzi l'`_shrink`API su altre o OpenSearch versioni di Elasticsearch, fai la seguente richiesta prima di iniziare l'operazione di compattazione:

```
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
  }
}
```

Quindi effettua le seguenti richieste al termine dell'operazione di riduzione:

```
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 versione 2.13

Per la OpenSearch versione 2.13, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
- `/_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/pipeline`
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`

- 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.search.request.slowlog.level
- cluster.search.request.slowlog.threshold.warn
- cluster.search.request.slowlog.threshold.info
- cluster.search.request.slowlog.threshold.debug
- cluster.search.request.slowlog.threshold.trace

- /_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
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

OpenSearch versione 2.11

Per la OpenSearch versione 2.11, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio *`index-name`* `/_forcemerge` , *`index-name`* `/update/`*`id`* e *`index-name`* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/pipeline`
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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/_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`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.

4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

OpenSearch versione 2.9

Per la OpenSearch versione 2.9, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
- `/_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`
- `/_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]

- 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/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_validate

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

OpenSearch versione 2.7

Per OpenSearch 2.7, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.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`
- `/_plugins/_security`
- `/_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.total.limit
- cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

OpenSearch versione 2.5

Per OpenSearch 2.5, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` ,
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_refresh`
- `/_reindex` [1]
- `/_render`

/*index-name* /update/*id* e /*index-name* /_close).
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (eccetto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings per numerose proprietà[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
- /_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
- /_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

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

OpenSearch versione 2.3

Per OpenSearch 2.3, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_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`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ml`
- `_plugins/_notifications`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.

4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called "Differenze significative tra le API". Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called "Riduzione".

OpenSearch versione 1.3

Per OpenSearch 1.3, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
- `/_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`
- `/_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`

  - 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/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

OpenSearch versione 1.2

Per OpenSearch 1.2, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.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`
- `/_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`

  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

OpenSearch versione 1.1

Per OpenSearch 1.1, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio `/index-name /_forcemerge` ,
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_refresh`
- `/_reindex` [1]
- `/_render`

/*index-name* /update/*id* e /*index-name* /_close).
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (eccetto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings per numerose proprietà[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
- /_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
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

OpenSearch versione 1.0

Per la OpenSearch versione 1.0, OpenSearch Service supporta le seguenti operazioni. Per informazioni sulla maggior parte delle operazioni, consulta il riferimento all'API OpenSearch REST o il riferimento all'API per il plug-in specifico.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_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`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_plugins/_transforms`
- `/_percolate`
- `/_rank_eval`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.

4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called "Differenze significative tra le API". Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called "Riduzione".

Elasticsearch versione 7.10

Per Elasticsearch 7.10, OpenSearch Service supporta le seguenti operazioni.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_index_template`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_asynchronous_search`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_ppl`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template` [6]
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_plugins/_replication`
- `/_rank_eval`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.
6. I modelli di indice legacy (`_template`) sono stati sostituiti da modelli componibili (`_index_template`) a partire da Elasticsearch 7.8. I modelli componibili hanno la precedenza sui modelli legacy. Se nessun modello componibile corrisponde a un determinato indice, un modello legacy può comunque corrispondere ed essere applicato. L'`_template`operazione funziona ancora nelle versioni successive di Elasticsearch OSS, ma le chiamate GET ai due tipi di modello restituiscono risultati diversi. OpenSearch

Elasticsearch versione 7.9

Per Elasticsearch 7.9, OpenSearch Service supporta le seguenti operazioni.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_ppl`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_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` [6]
- `/_update_by_query` [1]
- `/_validate`

  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle OpenSearch operazioni generiche supportate dal OpenSearch servizio e non include le operazioni supportate specifiche del plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.
6. I modelli di indice legacy (`_template`) sono stati sostituiti da modelli componibili (`_index_template`) a partire da Elasticsearch 7.8. I modelli componibili hanno la precedenza sui modelli legacy. Se nessun modello componibile corrisponde a un determinato indice, un modello legacy può comunque corrispondere ed essere applicato. L'`_template`operazione funziona ancora nelle versioni successive di Elasticsearch OSS, ma le chiamate GET ai due tipi di modello restituiscono risultati diversi. OpenSearch

Elasticsearch versione 7.8

Per Elasticsearch 7.8, OpenSearch Service supporta le seguenti operazioni.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-*
- `/_cluster/state`
- `/_cluster/stats`
- `/_refresh`
- `/_reindex` [1]

name /_forcemerge , /*index-name* /update/*id* e /*index-name* /_close).
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (eccetto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings per numerose proprietà[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
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_index_template [6]
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione /_tasks insieme a queste altre operazioni per verificare il corretto completamento delle richieste.

2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.
6. I modelli di indice legacy (`_template`) sono stati sostituiti da modelli componibili (`_index_template`) a partire da Elasticsearch 7.8. I modelli componibili hanno la precedenza sui modelli legacy. Se nessun modello componibile corrisponde a un determinato indice, un modello legacy può comunque corrispondere ed essere applicato. L'`_template`operazione funziona ancora nelle versioni successive di Elasticsearch OSS, ma le chiamate GET ai due tipi di modello restituiscono risultati diversi. OpenSearch

Elasticsearch versione 7.7

Per Elasticsearch 7.7, OpenSearch Service supporta le seguenti operazioni.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 7.4

Per Elasticsearch 7.4, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`).
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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/_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. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 7.1

Per Elasticsearch 7.1, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */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`
- `/_mapping`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`

- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di

Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.

5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 6.8

Per Elasticsearch 6.8, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio `/index-name /_forcemerge` e `/index-name /update/id`) tranne `/index-name /_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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`
- `cluster.blocks.read_only`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 6.7

Per Elasticsearch 6.7, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */index-name* `/_close`.
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]

- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate

il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch

3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 6.5

Per Elasticsearch 6.5, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio `/index-name /_forcemerge` e `/index-name /update/id`) tranne `/index-name /_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
- `/_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`
- `/_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.search.shard_count.limit • indices.breaker.fielddata.limit • indices.breaker.request.limit • indices.breaker.total.limit	• /_rank_eval	

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 6.4

Per Elasticsearch 6.4, Service supporta le seguenti operazioni. OpenSearch

• Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */index-name* `/_close`.	• `/_cluster/state` • `/_cluster/stats` • `/_count` • `/_delete_by_query` [1] • `/_explain`	• `/_refresh` • `/_reindex` [1] • `/_render` • `/_rollover` • `/_scripts` [3]

- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch

3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 6.3

Per Elasticsearch 6.3, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */index-name* `/_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.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`

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 6.2

Per Elasticsearch 6.2, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */index-name* `/_close`.
- `/_alias`
- `/_aliases`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`

- /_all
- /_analyze
- /_bulk
- /_cat (eccetto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings per numerose proprietà[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione /_tasks insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per /_search/scroll con un corpo del messaggio devono specificare il valore "Content-Length" nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei scroll_id valori, utilizzate il corpo della richiesta, non la stringa di query, per passare scroll_id i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di

Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.

5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 6.0

Per Elasticsearch 6.0, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio `/index-name /_forcemerge` e `/index-name /update/id`) tranne `/index-name /_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[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`
- `/_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`

- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 5.6

Per Elasticsearch 5.6, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */index-name* `/_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [5]
- `/_snapshot`

- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.

5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 5.5

Per Elasticsearch 5.5, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */index-name* `/_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.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`

- indices.breaker.total.limit

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Per considerazioni sull'uso degli script, consulta the section called “Altre risorse supportate”.
4. Riferimento al metodo PUT. Per informazioni sul metodo GET, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
5. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 5.3

Per Elasticsearch 5.3, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */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`
- `/_mapping`
- `/_render`
- `/_rollover`
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[4]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`

- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà[3]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al servizio. OpenSearch
3. Riferimento al metodo `PUT`. Per informazioni sul metodo `GET`, consulta the section called “Differenze significative tra le API”. Questo elenco si riferisce solo alle operazioni generiche di Elasticsearch supportate da OpenSearch Service e non include le operazioni supportate dai plug-in per il rilevamento delle anomalie, ISM e così via.
4. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 5.1

Per Elasticsearch 5.1, Service supporta le seguenti operazioni. OpenSearch

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forcemerge` e */index-name* `/update/`*id*) tranne */index-name* `/_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` per numerose proprietà (solo PUT):
  - `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`
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [3]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Le modifiche di configurazione del cluster potrebbero interrompere queste operazioni prima del loro completamento. È consigliabile usare l'operazione `/_tasks` insieme a queste altre operazioni per verificare il corretto completamento delle richieste.
2. Le richieste DELETE per `/_search/scroll` con un corpo del messaggio devono specificare il valore `"Content-Length"` nell'intestazione HTTP. La maggior parte dei client aggiunge questa intestazione di default. Per evitare problemi con = i caratteri nei `scroll_id` valori, utilizzate il corpo della richiesta, non la stringa di query, per passare `scroll_id` i valori al OpenSearch servizio.
3. Per informazioni, consulta the section called “Riduzione”.

Elasticsearch versione 2.3

Per Elasticsearch 2.3, OpenSearch Service supporta le seguenti operazioni.

- Tutte le operazioni nel percorso dell'indice (ad esempio */index-name* `/_forceme rge` e */index-name* `/_recovery`) tranne */index-name* `/_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cache/clear` (solo indice)
- `/_cat` (eccetto `/_cat/nodeattrs`)
- `/_cluster/health`
- `/_cluster/settings` per numerose proprietà (solo PUT):
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `threadpool.get.queue_size`
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_render`
- `/_search`
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_template`

- `threadpool.bulk.queue_size`
- `threadpool.index.queue_size`
- `threadpool.percolate.queue_size`
- `threadpool.search.queue_size`
- `threadpool.suggest.queue_size`

Elasticsearch versione 1.5

Per Elasticsearch 1.5, OpenSearch Service supporta le seguenti operazioni.

- Tutte le operazioni nel percorso dell'indice, ad esempio */index-name* `/_optimize` e */index-name* `/_warmer`, tranne */index-name* `/_close`.
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat`
- `/_cluster/health`
- `/_cluster/settings` per numerose proprietà (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`
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_plugin/kibana3`
- `/_plugin/migration`
- `/_refresh`
- `/_search`
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_template`

- `threadpool.percolate.queue_size`
- `threadpool.search.queue_size`
- `threadpool.suggest.queue_size`

Quote OpenSearch del servizio Amazon

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica.

Per visualizzare le quote per i domini e le istanze di OpenSearch servizio, Amazon OpenSearch Serverless e Amazon OpenSearch Ingestion, consulta le quote di Amazon OpenSearch Service nel. Riferimenti generali di AWS

Per visualizzare le quote per OpenSearch Service in AWS Management Console, apri la console Service Quotas. Nel riquadro di navigazione, scegli AWS servizi e seleziona Amazon OpenSearch Service. Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas.

Argomenti

- UltraWarm quote di archiviazione
- Quote delle dimensioni dei volumi EBS
- Quote di rete
- Quote di dimensioni condivise
- Quota dei processi Java
- Quota della policy di dominio

UltraWarm quote di archiviazione

La tabella seguente elenca i tipi di UltraWarm istanza e la quantità massima di storage che ogni tipo può utilizzare. Per ulteriori informazioni su UltraWarm, vederethe section called “UltraWarm archiviazione”.

Tipo di istanza	Spazio di archiviazione massimo
`ultrawarm1.medium.search`	1,5 TiB
`ultrawarm1.large.search`	20 TiB

Quote delle dimensioni dei volumi EBS

La tabella seguente mostra le dimensioni minime e massime dei volumi EBS per ogni tipo di istanza supportato dal OpenSearch servizio. Per informazioni sui tipi di istanza che includono lo storage delle istanze e dettagli hardware aggiuntivi, consulta i prezzi OpenSearch di Amazon Service.

- Se si sceglie l'archiviazione magnetica per Tipo di volume EBS quando si crea il dominio, la dimensione massima del volume è di 100 GiB per tutti i tipi di istanza tranne `t2.small` e `t2.medium` e tutte le istanze Graviton (M6g, C6g, R6g, and R6gd), che non supportano l'archiviazione magnetica. Per le dimensioni massime elencate nella seguente tabella, selezionare una delle opzioni SSD.
- Alcuni tipi di istanze di generazioni precedenti includono l'archiviazione dell'istanza, ma supportano anche l'archiviazione EBS. Se si sceglie l'archiviazione EBS per uno di questi tipi di istanze, tenere presente che i volumi di archiviazione non sono cumulativi. È possibile utilizzare un volume EBS o l'archiviazione dell'istanza, non entrambi.

Tipo di istanza	Dimensione minima EBS	Dimensione massima EBS (gp2)	Dimensione massima EBS (gp3)
`t2.micro.search`	10 GiB	35 GiB	N/D
`t2.small.search`	10 GiB	35 GiB	N/D
`t2.medium.search`	10 GiB	35 GiB	N/D
`t3.small.search`	10 GiB	100 GiB	100 GiB
`t3.medium.search`	10 GiB	200 GiB	200 GiB

Tipo di istanza	Dimensione minima EBS	Dimensione massima EBS (gp2)	Dimensione massima EBS (gp3)
m3.medium.search	10 GiB	100 GiB	N/D
m3.large.search	10 GiB	512 GiB	N/D
m3.xlarge.search	10 GiB	512 GiB	N/D
m3.2xlarge.search	10 GiB	512 GiB	N/D
m4.large.search	10 GiB	512 GiB	N/D
m4.xlarge.search	10 GiB	1 TiB	N/D
m4.2xlarge.search	10 GiB	1,5 TiB	N/D
m4.4xlarge.search	10 GiB	1,5 TiB	N/D
m4.10xlarge.search	10 GiB	1,5 TiB	N/D
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

Tipo di istanza	Dimensione minima EBS	Dimension e massima EBS (gp2)	Dimensione massima EBS (gp3)
m6g.12xlarge.search	10 GiB	9 TiB	18 TiB
c4.large.search	10 GiB	100 GiB	N/D
c4.xlarge.search	10 GiB	512 GiB	N/D
c4.2xlarge.search	10 GiB	1 TiB	N/D
c4.4xlarge.search	10 GiB	1,5 TiB	N/D
c4.8xlarge.search	10 GiB	1,5 TiB	N/D
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/D

Tipo di istanza	Dimensione minima EBS	Dimensione massima EBS (gp2)	Dimensione massima EBS (gp3)
r3.xlarge.search	10 GiB	512 GiB	N/D
r3.2xlarge.search	10 GiB	512 GiB	N/D
r3.4xlarge.search	10 GiB	512 GiB	N/D
r3.8xlarge.search	10 GiB	512 GiB	N/D
r4.large.search	10 GiB	1 TiB	N/D
r4.xlarge.search	10 GiB	1,5 TiB	N/D
r4.2xlarge.search	10 GiB	1,5 TiB	N/D
r4.4xlarge.search	10 GiB	1,5 TiB	N/D
r4.8xlarge.search	10 GiB	1,5 TiB	N/D
r4.16xlarge.search	10 GiB	1,5 TiB	N/D
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

Tipo di istanza	Dimensione minima EBS	Dimension e massima EBS (gp2)	Dimensione massima EBS (gp3)
r6g.8xlarge.search	10 GiB	8 TiB	16 TiB
r6g.12xlarge.search	10 GiB	12 TiB	24 TiB
r6gd.large.search	N/D	N/D	N/D
r6gd.xlarge.search	N/D	N/D	N/D
r6gd.2xlarge.search	N/D	N/D	N/D
r6gd.4xlarge.search	N/D	N/D	N/D
r6gd.8xlarge.search	N/D	N/D	N/D
r6gd.12xlarge.search	N/D	N/D	N/D
r6gd.16xlarge.search	N/D	N/D	N/D
i2.xlarge.search	10 GiB	512 GiB	N/D
i2.2xlarge.search	10 GiB	512 GiB	N/D
i3.large.search	N/D	N/D	N/D
i3.xlarge.search	N/D	N/D	N/D
i3.2xlarge.search	N/D	N/D	N/D
i3.4xlarge.search	N/D	N/D	N/D
i3.8xlarge.search	N/D	N/D	N/D
i3.16xlarge.search	N/D	N/D	N/D
or1.medium.search	20 GiB	N/D	768 GiB
or1.large.search	20 GiB	N/D	15,32 GiB

Tipo di istanza	Dimensione minima EBS	Dimensione massima EBS (gp2)	Dimensione massima EBS (gp3)
or1.xlarge.search	20 GiB	N/D	3 TiB
or1.2xlarge.search	20 GiB	N/D	6 TiB
or1.4xlarge.search	20 GiB	N/D	12 TiB
or1.8xlarge.search	20 GiB	N/D	16 TiB
or1.12xlarge.search	20 GiB	N/D	24 TiB
or1.16xlarge.search	20 GiB	N/D	36 TiB
im4gn.large.search	N/D	N/D	N/D
im4gn.xlarge.search	N/D	N/D	N/D
im4gn.2xlarge.search	N/D	N/D	N/D
im4gn.4xlarge.search	N/D	N/D	N/D
im4gn.8xlarge.search	N/D	N/D	N/D
im4gn.16xlarge.search	N/D	N/D	N/D

Quote di rete

La tabella seguente mostra la dimensione massima dei payload delle richieste HTTP.

Tipo di istanza	Dimensione massima dei payload delle richieste HTTP
t2.micro.search	10 MiB
t2.small.search	10 MiB
t2.medium.search	10 MiB

Tipo di istanza	Dimensione massima dei payload delle richieste HTTP
t3.small.search	10 MiB
t3.medium.search	10 MiB
m3.medium.search	10 MiB
m3.large.search	10 MiB
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

Tipo di istanza	Dimensione massima dei payload delle richieste HTTP
m6g.2xlarge.search	100 MiB
m6g.4xlarge.search	100 MiB
m6g.8xlarge.search	100 MiB
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

Tipo di istanza	Dimensione massima dei payload delle richieste HTTP
c6g.2xlarge.search	100 MiB
c6g.4xlarge.search	100 MiB
c6g.8xlarge.search	100 MiB
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

Tipo di istanza	Dimensione massima dei payload delle richieste HTTP
r5.2xlarge.search	100 MiB
r5.4xlarge.search	100 MiB
r5.12xlarge.search	100 MiB
r6g.large.search	100 MiB
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

Tipo di istanza	Dimensione massima dei payload delle richieste HTTP
r6gd.12xlarge.search	100 MiB
r6gd.16xlarge.search	100 MiB
i2.xlarge.search	100 MiB
i2.2xlarge.search	100 MiB
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

Tipo di istanza	Dimensione massima dei payload delle richieste HTTP
or1.12xlarge.search	100 MiB
or1.16xlarge.search	100 MiB
im4gn.large.search	100 MiB
im4gn.xlarge.search	100 MiB
im4gn.2xlarge.search	100 MiB
im4gn.4xlarge.search	100 MiB
im4gn.8xlarge.search	100 MiB
im4gn.16xlarge.search	100 MiB

Quote di dimensioni condivise

La sezione seguente elenca le dimensioni massime degli shard per varie famiglie di istanze.

Tipo di istanza	Multi-AZ senza Standby	Multi-AZ con Standby
5R, 5C, 5M	N/D	65 GiB
I3	N/D	65 GiB
6 g, 6 g, 6 g, 6 g	N/D	65 GiB
O 1	100 GiB	65 GiB

Tipo di istanza	Multi-AZ senza Standby	Multi-AZ con Standby
Im4gn	N/D	65 GiB

Per richiedere un aumento della quota, contatta il AWS Supporto.

Quota dei processi Java

OpenSearch Il servizio limita i processi Java a una dimensione dell'heap di 32 GiB. Gli utenti esperti possono specificare la percentuale di heap utilizzata per i dati del campo. Per ulteriori informazioni, consultare the section called “Impostazioni avanzate del cluster” e the section called “JVM OutOfMemoryError”.

Quota della policy di dominio

OpenSearch Il servizio limita le politiche di accesso sui domini a 100 KiB.

Istanze riservate nel servizio OpenSearch di Amazon

Le istanze riservate (RI) nel servizio OpenSearch di Amazon offrono sconti notevoli rispetto alle istanze on demand standard. Le istanze sono identiche; le IR rappresentano solo uno sconto di fatturazione applicato alle istanze on demand nel tuo account. Per le applicazioni di lunga durata con utilizzo prevedibile, le IR sono in grado di offrire notevoli risparmi nel corso del tempo.

Le istanze riservate di OpenSearch Service richiedono termini da uno o tre anni e presentano tre opzioni di pagamento che interessano il tasso di sconto:

- Nessun pagamento anticipato: non è previsto alcun pagamento anticipato. Paghi una tariffa oraria scontata per ogni ora entro il termine.
- Pagamento anticipato parziale: si paga una parte dei costi in anticipo e una tariffa oraria scontata per ogni ora entro il termine.
- Pagamento anticipato totale: di paga l'intero costo in anticipo. Non paghi una tariffa oraria per il termine.

In linea generale, un pagamento anticipato maggiore implica uno sconto maggiore. Non è possibile annullare le istanze riservate: quando vengono prenotate, ci si impegna a pagare per l'intero termine. I pagamenti anticipati non sono rimborsabili.

Le istanze riservate non sono flessibili; si applicano solo al tipo di istanza esatto che si riserva. Ad esempio, una prenotazione per otto istanze `c5.2xlarge.search` non si applica a sedici istanze `c5.xlarge.search` o quattro istanze `c5.4xlarge.search`. Per i dettagli completi, consultare Prezzi del servizio OpenSearch di Amazon e Domande frequenti.

Argomenti

- Acquisto di istanze riservate (console)
- Acquisto di istanze riservate (AWS CLI)
- Acquisto di istanze riservate (SDK AWS)
- Analisi dei costi

Acquisto di istanze riservate (console)

La console ti consente di visualizzare le istanze riservate esistenti e acquistarne di nuove.

Per acquistare una prenotazione

1. Andare all'indirizzo https://aws.amazon.com e quindi scegliere Sign In to the Console (Accedi alla console).
2. In Analisi, scegliere Amazon OpenSearch Service.
3. Scegli Locazioni di istanze riservate dal pannello di navigazione.

   In questa pagina, è possibile visualizzare le prenotazioni esistenti. Se si dispone di numerose prenotazioni, è possibile filtrarle per identificarle più facilmente e visualizzare una determinata prenotazione.

   > **Tip**
   >
   > Se il collegamento Locazioni di istanze riservate non è visibile, crea un dominio nella Regione AWS.

4. Scegli Ordina istanza riservata.
5. Fornisci un nome descrittivo univoco.
6. Scegli un tipo di istanza e il numero di istanze. Per le linee guida, consulta the section called “Dimensionamento dei domini”.

7. Scegliere la durata del termine e l'opzione di pagamento. Esaminare attentamente le informazioni di pagamento.
8. Seleziona Next (Successivo).
9. Rivedere attentamente il riepilogo dell'acquisto. Le istanze riservate acquistate non sono rimborsabili.
10. Scegliere Ordina.

Acquisto di istanze riservate (AWS CLI)

AWS CLI dispone di comandi per la visualizzazione delle offerte, l'acquisto di una prenotazione e la visualizzazione delle prenotazioni. Il comando e la risposta di esempio seguenti mostrano le offerte per una determinata Regione 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"
    }
  ]
}
```

Per la spiegazione di ogni valore restituito, consultare la tabella riportata di seguito.

Campo	Descrizione
`FixedPrice`	Il costo anticipato della prenotazione.

Campo	Descrizione
`ReservedInstanceOfferingId`	ID dell'offerta. Annotare questo valore se si desidera prenotare l'offerta.
`RecurringCharges`	La tariffa oraria per la prenotazione.
`UsagePrice`	Un campo legacy. Per OpenSearch Service, questo valore è sempre 0.
`PaymentOption`	Nessun pagamento anticipato, pagamento anticipato parziale o pagamento anticipato totale
`Duration`	Durata del termine in secondi: • 31536000 secondi corrispondono a 1 anno. • 94608000 secondi corrispondono a tre anni.
`InstanceType`	Il tipo di istanza per la prenotazione. Per informazioni sulle risorse hardware che sono allocate a ciascun tipo di istanza, consultare Prezzi del servizio OpenSearch di Amazon.
`CurrencyCode`	La valuta per `FixedPrice` e `RecurringChargeAmount`.

Nell'esempio successivo viene acquistata una prenotazione:

```
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"
}
```

Infine, è possibile elencare le prenotazioni per una determinata regione utilizzando l'esempio seguente:

```
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` è l'Unix epoch, che è il numero di secondi trascorsi dalla mezzanotte UTC del 1° gennaio 1970. Ad esempio, l'epoch 1522872571 sono le 20:09:31 UTC del 4 aprile 2018. È possibile utilizzare convertitori online.

Per ulteriori informazioni sui comandi utilizzati negli esempi precedenti, consultare Riferimento ai comandi AWS CLI.

Acquisto di istanze riservate (SDK AWS)

Gli SDK AWS (ad eccezione degli SDK Android e iOS) supportano tutte le operazioni definite nella Documentazione di riferimento delle API del servizio OpenSearch di Amazon incluso quanto segue:

- `DescribeReservedInstanceOfferings`
- `PurchaseReservedInstanceOffering`
- `DescribeReservedInstances`

Questo script di esempio utilizza il client Python di basso livello OpenSearchService dal AWS SDK for Python (Boto3) per l'acquisto di istanze riservate. È necessario fornire un valore per `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)
```

Per ulteriori informazioni sull'installazione e sull'uso degli SDK AWS, consultare Software Development Kit AWS.

Analisi dei costi

Cost Explorer è uno strumento gratuito che è possibile utilizzare per visualizzare i dati di spesa per gli ultimi 13 mesi. L'analisi di questi dati consente di individuare le tendenze e comprendere se le IR sono adatte al proprio caso d'uso. Se si dispone già di IR, è possibile raggrupparle perPurchase Option (Opzione di acquisto) e mostrare i costi ammortizzati per confrontare la spesa con le spese per le istanze on demand. È anche possibile impostare i budget di utilizzo per verificare di usare appieno le istanze riservate. Per ulteriori informazioni, consultare Analisi dei costi con Cost Explorer nella Guida per l'utente di AWS Billing.

Altre risorse supportate in Amazon OpenSearch Service

Questo argomento descrive le risorse aggiuntive supportate da Amazon OpenSearch Service.

bootstrap.memory_lock

OpenSearch Il servizio `bootstrap.memory_lock` abilita l'accesso`opensearch.yml`, che blocca la memoria JVM e impedisce al sistema operativo di scambiarla su disco. Ciò vale per tutti i tipi di istanze supportati, tranne che per le seguenti:

- `t2.micro.search`
- `t2.small.search`
- `t2.medium.search`
- `t3.small.search`
- `t3.medium.search`

Modulo di scripting

OpenSearch Il servizio supporta lo scripting per Elasticsearch 5. domini x e successivi. Il servizio non supporta lo scripting per le versioni 1.5 o 2.3.

Le opzioni di scripting supportate includono le seguenti:

- Painless
- Lucene Expressions
- Mustache

Per i domini Elasticsearch 5.5 e versioni successive e per tutti i OpenSearch domini, OpenSearch Service supporta gli script archiviati utilizzando l'endpoint. `_scripts` I domini Elasticsearch 5.3 e 5.1 supportano solo gli script in linea.

Trasporto TLS

OpenSearch Il servizio supporta HTTP sulla porta 80 e HTTPS sulla porta 443, ma non supporta il trasporto TLS.

Tutorial di Amazon OpenSearch Service

Questo capitolo include diversi tutorial completi per iniziare a utilizzare Amazon OpenSearch Service, tra cui come eseguire la migrazione al servizio, creare una semplice applicazione di ricerca e creare una visualizzazione in OpenSearch Dashboards.

Argomenti

Tutorial: creazione e ricerca di documenti in Amazon OpenSearch Service

In questo tutorial, imparerai come creare e cercare un documento in Amazon OpenSearch Service. Aggiungi dati a un indice sotto forma di documento JSON. OpenSearch Il servizio crea un indice attorno al primo documento aggiunto.

Questo tutorial spiega come effettuare richieste HTTP per creare documenti, generare automaticamente un ID per un documento ed eseguire ricerche di base e avanzate sui documenti.

> **Note**
>
> Questo tutorial utilizza un dominio con accesso aperto. Per il massimo livello di sicurezza, ti consigliamo di inserire il dominio all'interno di un cloud privato virtuale (VPC).

Prerequisiti

Di seguito sono elencati i requisiti per questo tutorial:

- È necessario disporre di un Account AWS.
- È necessario disporre di un dominio OpenSearch di servizio attivo.

Aggiunta di un documento a un indice

Per aggiungere un documento a un indice, puoi utilizzare qualsiasi strumento HTTP, come Postman, CURL o OpenSearch la console Dashboards. Questi esempi presuppongono che tu stia utilizzando la console per sviluppatori in Dashboards. OpenSearch Se utilizzi uno strumento diverso, modificalo di conseguenza fornendo l'URL completo e le credenziali, se necessario.

Per aggiungere un documento a un indice

1. Vai all'URL delle OpenSearch dashboard per il tuo dominio. Puoi trovare l'URL nella dashboard del dominio nella console di OpenSearch servizio. L'URL segue il seguente formato:

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

2. Accedi utilizzando il nome utente e la password principali.
3. Apri il pannello di navigazione a sinistra e scegli Strumenti di sviluppo.
4. Il verbo HTTP per creare una nuova risorsa è PUT, e si utilizza per creare un nuovo documento e indice. Immettere il seguente comando nella console:

   ```
   PUT fruit/_doc/1
   {
     "name":"strawberry",
     "color":"red"
   }
   ```

   La richiesta PUT crea un indice denominato frutta e aggiunge un singolo documento all'indice con un ID pari a 1. Viene generata la risposta seguente:

   ```
   {
     "_index" : "fruit",
     "_type" : "_doc",
     "_id" : "1",
     "_version" : 1,
     "result" : "created",
     "_shards" : {
       "total" : 2,
       "successful" : 2,
       "failed" : 0
     },
     "_seq_no" : 0,
   ```

```
  "_primary_term" : 1
}
```

Creazione di ID generati automaticamente

OpenSearch Il servizio può generare automaticamente un ID per i tuoi documenti. Il comando per generare gli ID utilizza una richiesta POST invece di una richiesta PUT e non richiede alcun ID documento (rispetto alla richiesta precedente).

Inserisci la seguente richiesta nella console degli sviluppatori:

```
POST veggies/_doc
{
  "name":"beet",
  "color":"red",
  "classification":"root"
}
```

Questa richiesta crea un indice denominato verdure e aggiunge il documento all'indice. Viene generata la risposta seguente:

```
{
  "_index" : "veggies",
  "_type" : "_doc",
  "_id" : "3WgyS4IB5DLqbRIvLxtF",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Nota che il campo aggiuntivo `_id` nella risposta, indica che un ID è stato creato automaticamente.

> **Note**
>
> Non fornisci nulla dopo `_doc` nell'URL, dove normalmente va l'ID. Poiché stai creando un documento con un ID generato, non ne fornisci ancora uno. È riservato agli aggiornamenti.

Aggiornamento di un documento con un comando POST

Per aggiornare un documento, si utilizza un comando `POST` HTTP con il numero di ID.

In primo luogo, creare un documento con un ID di `42`:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow"
}
```

Quindi usa quell'ID per aggiornare il documento:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow",
  "classification":"berries"
}
```

Questo comando aggiorna il documento con il nuovo campo `classification`. Viene generata la risposta seguente:

```
{
  "_index" : "fruits",
  "_type" : "_doc",
  "_id" : "42",
  "_version" : 2,
  "result" : "updated",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
```

```
  "_seq_no" : 1,
  "_primary_term" : 1
}
```

> **Note**
>
> Se si tenta di aggiornare un documento che non esiste, OpenSearch Service crea il documento.

Esecuzione di operazioni in blocco

Puoi utilizzare il l'operazione API `POST _bulk` per eseguire più azioni su uno o più indici in una richiesta. I comandi di azione in blocco assumono il formato seguente:

```
POST /_bulk
<action_meta>\n
<action_data>\n
<action_meta>\n
<action_data>\n
```

Ogni azione richiede due righe di JSON. Innanzitutto, fornisci la descrizione o i metadati dell'azione. Nella riga successiva, fornisci i dati. Ogni parte è separata da una nuova riga (\n). Una descrizione dell'azione per un inserto potrebbe essere simile alla seguente:

```
{ "create" : { "_index" : "veggies", "_type" : "_doc", "_id" : "7" } }
```

E la riga successiva che contiene i dati potrebbe essere simile alla seguente:

```
{ "name":"kale", "color":"green", "classification":"leafy-green" }
```

Nel loro insieme, i metadati e i dati rappresentano una singola azione in un'operazione di blocco. È possibile eseguire molte operazioni in un'unica richiesta, ad esempio:

```
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" } }
```

Si noti che l'ultima azione è `delete`. Non ci sono dati che seguono l'azione `delete`.

Ricerca di documenti

Ora che i dati sono presenti nel cluster, è possibile cercarli. Ad esempio, potresti voler cercare tutte le verdure con la radice o ottenere il numero di tutte le verdure a foglia verde o trovare il numero di errori registrati all'ora.

Ricerche base

Una ricerca di base è simile a questa:

```
GET veggies/_search?q=name:l*
```

La richiesta genera una risposta JSON che contiene il documento sulla lattuga.

Ricerca avanzata

È possibile eseguire ricerche più avanzate fornendo le opzioni di query come JSON nel corpo della richiesta:

```
GET veggies/_search
{
  "query": {
    "term": {
      "name": "lettuce"
    }
  }
}
```

Questo esempio produce anche una risposta JSON con il documento sulla lattuga.

Ordinamento

È possibile eseguire più query di questo tipo utilizzando l'ordinamento. Innanzitutto, è necessario ricreare l'indice, poiché la mappatura automatica dei campi ha scelto tipi che non possono essere ordinati per impostazione predefinita. Inviare le richieste seguenti per eliminare e ricreare l'indice:

```
DELETE /veggies

PUT /veggies
{
   "mappings":{
      "properties":{
         "name":{
            "type":"keyword"
         },
         "color":{
            "type":"keyword"
         },
         "classification":{
            "type":"keyword"
         }
      }
   }
}
```

Quindi ripopolare l'indice con i dati:

```
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" }
```

Ora puoi cercare con un ordinamento. Questa richiesta aggiunge un ordinamento crescente in base alla classificazione:

```
GET veggies/_search
{
```

```
  "query" : {
    "term": { "color": "green" }
  },
  "sort" : [
      "classification"
  ]
}
```

Risorse correlate

Per ulteriori informazioni, consulta le seguenti risorse :

- Nozioni di base
- Indicizzazione dei dati
- Ricerca di dati

Tutorial: migrazione ad AmazonOpenSearchServizio

Le istantanee degli indici sono un metodo molto diffuso per eseguire la migrazione da un sistema autogestitoOpenSearcho cluster Elasticsearch precedente su AmazonOpenSearchServizio. In generale, il processo consiste nei seguenti passaggi:

1. Acquisire uno snapshot del cluster esistente e caricare lo snapshot in un bucket Amazon S3.
2. Crea unOpenSearchDominio del servizio.
3. DareOpenSearchAutorizzazioni di servizio per accedere al bucket e assicurarti di disporre delle autorizzazioni per lavorare con le istantanee.
4. Ripristina l'istantanea sulOpenSearchDominio del servizio.

Questa spiegazione passo per passo fornisce passaggi più dettagliati e opzioni alternative, ove applicabile.

Acquisizione e caricamento dello snapshot

Sebbene sia possibile utilizzare il plugin repository-s3 per eseguire snapshot direttamente in S3, è necessario installare il plugin su ogni nodo, modificare `opensearch.yml` (o `elasticsearch.yml` se si utilizza un cluster Elasticsearch), riavviare ogni nodo, aggiungere le credenziali AWS e infine

eseguire lo snapshot. Il plugin è una grande opzione per l'uso continuo o per la migrazione di cluster più grandi.

Per i cluster più piccoli, un approccio una tantum consiste nel prendere uno snapshot condiviso del file system e quindi utilizzare l'AWS CLI per caricarlo su S3. Se si dispone già di uno snapshot, andare al passaggio 4.

Per acquisire uno snapshot e caricarlo in Amazon S3

1. Aggiungi l'impostazione `path.repo` a `opensearch.yml` (o `Elasticsearch.yml`) su tutti i nodi e quindi riavvia ogni nodo.

   ```
   path.repo: ["/my/shared/directory/snapshots"]
   ```

2. Registra un repository di snapshot; questa operazione è necessaria prima di acquisire uno snapshot. Un repository è solo un percorso di storage: un file system condiviso, Amazon S3, File system distribuito Hadoop (HDFS) ecc. In questo caso, utilizzeremo un file system condiviso ("fs"):

   ```
   PUT _snapshot/my-snapshot-repo-name
   {
     "type": "fs",
     "settings": {
       "location": "/my/shared/directory/snapshots"
     }
   }
   ```

3. Acquisire lo snapshot:

   ```
   PUT _snapshot/my-snapshot-repo-name/my-snapshot-name
   {
     "indices": "migration-index1,migration-index2,other-indices-*",
     "include_global_state": false
   }
   ```

4. Installare AWS CLI ed eseguire `aws configure` per aggiungere le credenziali.

5. Passare alla directory snapshot. Quindi eseguire i seguenti comandi per creare un nuovo bucket S3 e caricare il contenuto della directory snapshot in quel bucket:

   ```
   aws s3 mb s3://bucket-name --region us-west-2
   ```

```
aws s3 sync . s3://bucket-name --sse AES256
```

A seconda delle dimensioni dello snapshot e della velocità della connessione Internet, questa operazione può richiedere un po' di tempo.

Creare un dominio

Sebbene la console sia il modo più semplice per creare un dominio, in questo caso, il terminale è già aperto e l'AWS CLI installata. Modificare il seguente comando per creare un dominio che si adatti alle proprie esigenze:

```
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
```

Così com'è, il comando crea un dominio accessibile a Internet con due nodi di dati, ciascuno con 100 GiB di archiviazione. Consente inoltre il controllo granulare degli accessi con l'autenticazione di base HTTP e tutte le impostazioni di crittografia. Usa ilOpenSearchConsole di servizio se è necessaria una configurazione di sicurezza più avanzata, ad esempio un VPC.

Prima di eseguire il comando, modificare il nome di dominio, le credenziali dell'utente master e il numero di account. Specifica lo stessoRegione AWSche hai usato per il bucket S3 e unOpenSearchVersione di /Elasticsearch compatibile con la tua istantanea.

> **Important**
>
> Gli snapshot sono compatibili con le versioni successive e solo con una versione principale. Ad esempio, non è possibile ripristinare un'istantanea da unOpenSearch1.xcluster su un Elasticsearch 7.xcluster, solo unOpenSearch1.xo 2.xgrappolo. Anche la versione minore conta. Non è possibile ripristinare un'istantanea da un cluster 5.3.3 autogestito su un sistema 5.3.2OpenSearchDominio del servizio. Ti consigliamo di scegliere la versione più recente diOpenSearcho Elasticsearch supportato dalla tua istantanea. Per una tabella delle versioni compatibili, consultare the section called “Utilizzo di uno snapshot per migrare i dati”.

Fornire le autorizzazioni al bucket S3.

Nella console AWS Identity and Access Management (IAM), creare un ruolo con le seguenti autorizzazioni e la relazione di trust. Durante la creazione del ruolo, scegliere S3 come Servizio AWS. Assegnare un nome al ruolo `OpenSearchSnapshotRole` in modo che sia facile da trovare.

Autorizzazioni

```
{
  "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/*"
      ]
    }
```

```
  ]
}
```

Relazione di attendibilità

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

Quindi assegna al tuo ruolo IAM personale le autorizzazioni per assumere `OpenSearchSnapshotRole`. Creare la policy seguente e collegarla alla propria identità.

Autorizzazioni

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
    }
  ]
}
```

Mappa il ruolo dell'istantanea inOpenSearchDashboard (se si utilizza un controllo di accesso granulare)

Se è stato abilitato il controllo granulare degli accessi, anche se si utilizza l'autenticazione di base HTTP per tutti gli altri scopi, poter utilizzare gli snapshot sarà necessario mappare il ruolo `manage_snapshots` al ruolo IAM.

Come concedere all'identità le autorizzazioni per l'utilizzo degli snapshot

1. Accedi alle dashboard utilizzando le credenziali dell'utente principale che hai specificato al momento della creazione delOpenSearchDominio del servizio. Puoi trovare l'URL delle dashboard nelOpenSearchConsole di servizio. Presenta il formato `https://domain-endpoint/_dashboards/`.
2. Dal menu principale scegliere Sicurezza, Ruoli e selezionare il ruolo manage_snapshots.
3. Scegliere Utenti mappati, Gestisci mappatura.
4. Aggiungere l'ARN del dominio del ruolo IAM personale nel campo appropriato. L'ARN deve avere uno dei seguenti formati:

   ```
   arn:aws:iam::123456789123:user/user-name
   ```

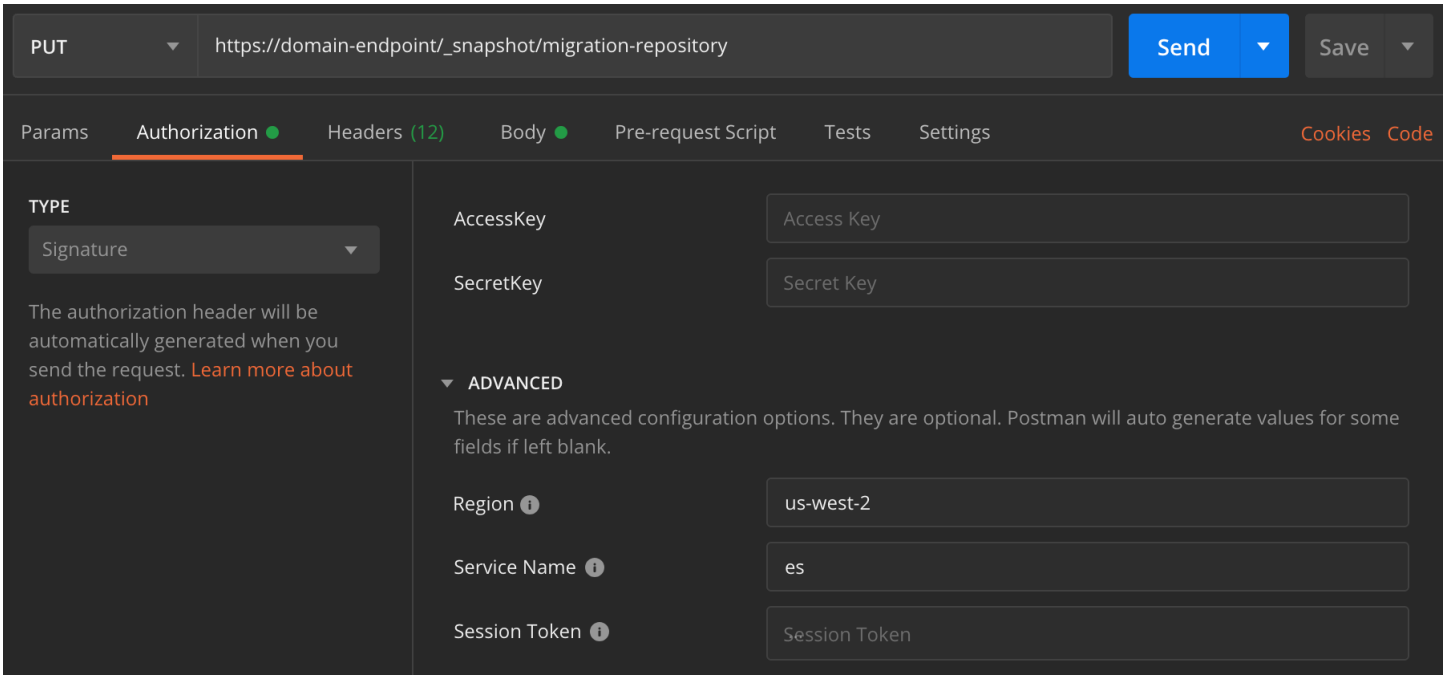
   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. Seleziona Map (Mappa) e verifica che il ruolo sia visualizzato in Mapped users (Utenti mappati).

Ripristino dello snapshot

A questo punto, hai due modi per accedere al tuoOpenSearchDominio del servizio: autenticazione di base HTTP con le credenziali dell'utente principale oAWSautenticazione utilizzando le tue credenziali IAM. Poiché le istantanee utilizzano Amazon S3, che non ha il concetto di utente principale, devi utilizzare le tue credenziali IAM per registrare l'archivio delle istantanee presso il tuoOpenSearchDominio del servizio.

La maggior parte dei linguaggi di programmazione dispone di librerie per facilitare la firma delle richieste, ma l'approccio più semplice consiste nell'utilizzare uno strumento comePostinoe inserisci le tue credenziali IAM nelAutorizzazionesezione.



Ripristinare lo snapshot

1. Indipendentemente da come si sceglie di firmare le richieste, il primo passo è registrare il repository:

```
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. Quindi elencare lo snapshot nel repository e trovare quello che si desidera ripristinare. A questo punto, continuare a usare Postman o passare a uno strumento come curl.

   Sintassi abbreviata

   ```
   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. Ripristinare lo snapshot:

   Sintassi abbreviata

```
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. Infine, verifica che gli indici siano ripristinati come previsto.

   Sintassi abbreviata

```
GET _cat/indices?v
```

   curl

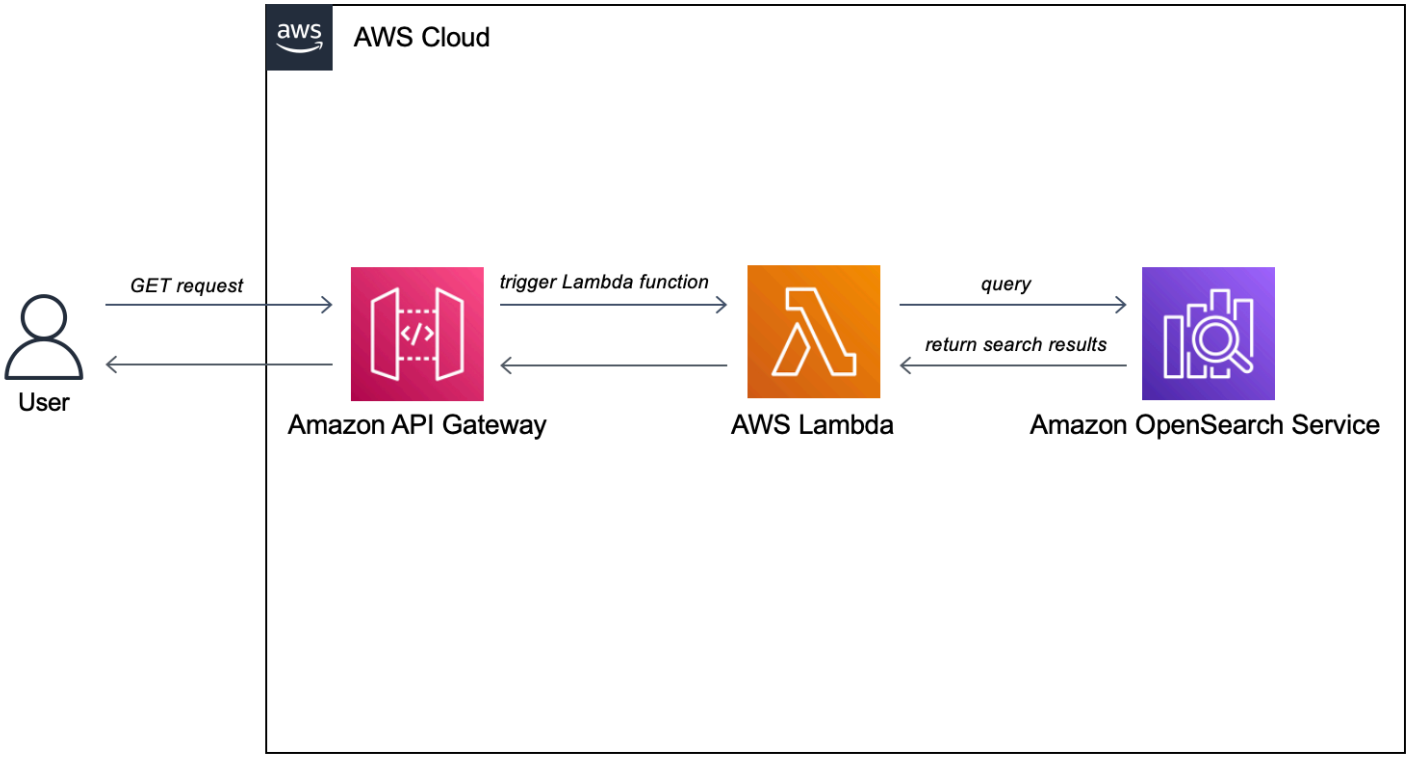
```
curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/_cat/
indices?v
```

A questo punto, la migrazione è completa. Potresti configurare i tuoi client per utilizzare il nuovoOpenSearchEndpoint del servizio,ridimensionare il dominioper soddisfare il tuo carico di lavoro, controlla il numero di shard per i tuoi indici, passa a unUtente master IAM, oppure inizia a creare visualizzazioni inOpenSearchPannelli di controllo.

Tutorial: creazione di un'applicazione di ricerca con Amazon OpenSearch Service

Un modo comune per creare un'applicazione di ricerca con Amazon OpenSearch Service consiste nell'utilizzare moduli Web per inviare le richieste degli utenti a un server. Quindi puoi autorizzare il server a chiamare direttamente le OpenSearch API e fare in modo che il server invii le richieste al servizio. OpenSearch Se desideri scrivere codice lato client che non si basa su un server, tuttavia, devi compensare per i rischi di sicurezza e prestazioni. Non è consigliabile consentire l'accesso pubblico e non firmato alle OpenSearch API. Gli utenti possono accedere a endpoint non protetti o influire sulle prestazioni del cluster tramite query eccessivamente estese (o troppe query).

Questo capitolo presenta una soluzione: usa Amazon API Gateway per limitare gli utenti a un sottoinsieme di OpenSearch API e AWS Lambda per firmare le richieste da API Gateway to OpenSearch Service.



> **Note**
>
> Si applicano i prezzi standard di API Gateway e Lambda, ma entro l'uso limitato di questo tutorial, i costi dovrebbero essere trascurabili.

Prerequisiti

Un prerequisito per questo tutorial è un OpenSearch dominio di servizio. Se non ne hai già uno, segui i passaggi in Creare un dominio di OpenSearch servizio per crearne uno.

Fase 1: Indicizzazione dei dati di esempio

Scaricare sample-movies.zip, decomprimerlo e utilizzare l'operazione dell'API _bulk per aggiungere i 5.000 documenti all'indice `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"}
...
```

Nota che quanto sopra è un comando di esempio con un piccolo sottoinsieme dei dati disponibili. Per eseguire l'`_bulk`operazione, è necessario copiare e incollare l'intero contenuto del `sample-movies` file. Per ulteriori istruzioni, vederethe section called “Opzione 2: Caricamento di più documenti”.

Puoi anche usare il seguente comando curl per ottenere lo stesso risultato:

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

Fase 2: Creare e distribuire la funzione Lambda

Prima di creare l'API in API Gateway, crea la funzione Lambda a cui passa le richieste.

Creazione della funzione Lambda

In questa soluzione, API Gateway passa le richieste a una funzione Lambda, che interroga il OpenSearch servizio e restituisce i risultati. Poiché questa funzione di esempio utilizza librerie esterne, è necessario creare un pacchetto di distribuzione e caricarlo su Lambda.

Per creare il pacchetto di implementazione

1. Apri un prompt dei comandi e crea una directory di progetto `my-opensearch-function`. Ad esempio, su macOS:

   ```
   mkdir my-opensearch-function
   ```

2. Passa alla directory del progetto `my-sourcecode-function`.

   ```
   cd my-opensearch-function
   ```

3. Copia il contenuto del seguente codice Python di esempio e salvalo in un nuovo file denominato. `opensearch-lambda.py` Aggiungi la tua regione e l'endpoint host al file.

   ```
   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. Installa le librerie esterne in una nuova `package` directory.

```
pip3 install --target ./package boto3
pip3 install --target ./package requests
pip3 install --target ./package requests_aws4auth
```

5. Crea un pacchetto di implementazione con le librerie installate nella directory principale. Il comando seguente genera un `my-deployment-package.zip` file nella directory del progetto.

```
cd package
zip -r ../my-deployment-package.zip .
```

6. Aggiungi il file `opensearch-lambda.py` alla radice del file .zip.

```
cd ..
zip my-deployment-package.zip opensearch-lambda.py
```

Per ulteriori informazioni sulla creazione di funzioni Lambda e sui pacchetti di implementazione, consultare Implementa funzioni Lambda per Python con gli archivi di file .zip nella Guida per gli sviluppatori di AWS Lambda e the section called “Creazione il pacchetto di implementazione Lambda” in questa guida.

Per creare la tua funzione utilizzando la console Lambda

1. Accedi alla console Lambda all'indirizzo https://console.aws.amazon.com/lambda/home. Nel riquadro di navigazione a sinistra, scegli Funzioni.
2. Seleziona Crea funzione.
3. Configura i campi seguenti:

   - Nome della funzione: opensearch-function
   - Runtime: Python 3.9
   - Architettura: x86_64

   Mantieni tutte le altre opzioni predefinite e scegli Crea funzione.
4. Nella sezione Codice sorgente della pagina di riepilogo della funzione, scegli il menu a discesa Carica da e seleziona il file.zip. Individua il **`my-deployment-package.zip`** file che hai creato e scegli Salva.
5. Il gestore è il metodo nel codice della funzione che elabora gli eventi. In Impostazioni di runtime, scegli Modifica e modifica il nome del gestore in base al nome del file nel pacchetto di distribuzione in cui si trova la funzione Lambda. Poiché il file ha un nome`opensearch-lambda.py`, rinomina il gestore in. *`opensearch-lambda`*`.lambda_handler` Per ulteriori informazioni, consulta Gestore della funzione Lambda in Python.

Fase 3: Creare l'API in API Gateway

L'utilizzo di API Gateway consente di creare un'API più limitata e semplifica il processo di interazione con l' OpenSearch `_search`API. API Gateway consente inoltre di abilitare caratteristiche di sicurezza

come l'autenticazione di Amazon Cognito e la limitazione delle richieste. Completare la procedura seguente per creare e implementare un'API:

Creazione e configurazione dell'API

Come creare l'API utilizzando la console API Gateway

1. Accedi alla console API Gateway all'indirizzo https://console.aws.amazon.com/apigateway/home. Nel riquadro di navigazione a sinistra, scegli API.
2. Individuare REST API (non privato) e scegliere Crea.
3. Nella pagina seguente, individua la sezione Crea nuova API e assicurati che sia selezionata Nuova API.
4. Configura i campi seguenti:
   - Nome API: opensearch-api
   - Descrizione: API pubblica per la ricerca di un dominio Amazon OpenSearch Service
   - Tipo di endpoint: regionale
5. Seleziona Create API (Crea API).
6. Scegliere Operazioni quindi Crea metodo.
7. Selezionare GET nel menu a discesa e fare clic sul segno di spunta per confermare.
8. Configurare le impostazioni seguenti, quindi scegliere Salva:

Impostazione	Valore
Tipo di integrazione	Funzione Lambda
Utilizzo dellintegrazione proxy Lambda	Sì
Regione Lambda	*us-west-1*
Funzione Lambda	`opensearch-lambda`
Utilizzo del timeout di default	Sì

Configurazione della richiesta del metodo

Scegliere Richiesta metodo e configurare le impostazioni seguenti:

Impostazione	Valore
Autorizzazione	NONE
Convalidatore di richieste	Convalida dei parametri e delle intestazioni delle stringhe di query
Chiave API richiesta	false

In Parametri della stringa di query URL, scegli Aggiungi stringa di query e configura il seguente parametro:

Impostazione	Valore
Nome	q
Richiesto	Sì

Implementazione dell'API e configurazione di una fase

La console API Gateway consente di distribuire un'API creando una distribuzione e associandola a una fase nuova o esistente.

1. Scegliere Operazioni e Implementa API.
2. Per Fase di implementazione, scegliere Nuova fase e nominare la fase `opensearch-api-test`.
3. Seleziona Deploy (Implementa).
4. Configurare le seguenti impostazioni nell'editor della fase, quindi scegliere Salva modifiche:

Impostazione	Valore
Abilitazione della limitazione	Sì

Impostazione	Valore
Tariffa	1000
Burst	500

Queste impostazioni configurano un'API che dispone di un solo metodo: una richiesta `GET` alla root dell'endpoint (`https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/search-es-api-test`). La richiesta richiede un singolo parametro (`q`), la stringa di query da ricercare. Quando viene chiamato, il metodo passa la richiesta a Lambda, che esegue la funzione `opensearch-lambda`. Per ulteriori informazioni, consultare Creazione di un'API in Amazon API Gateway e Implementazione di una REST API in Amazon API Gateway.

Fase 4: (facoltativa) Modifica della policy di accesso al dominio

Il dominio del OpenSearch servizio deve consentire alla funzione Lambda di effettuare `GET` richieste all'`movies`indice. Se il dominio ha una policy di accesso aperto con il controllo granulare degli accessi abilitato, è possibile lasciarlo così com'è:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/*"
    }
  ]
}
```

In alternativa, è possibile scegliere di rendere la policy di accesso al dominio più granulare. Per esempio, la policy minima seguente consente a `opensearch-lambda-role` (creato tramite Lambda) l'accesso in lettura all'indice `movies`: Per ottenere il nome esatto del ruolo creato automaticamente da Lambda, passare alla console AWS Identity and Access Management(IAM), scegliere Ruoli e cercare "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**
>
> Se hai abilitato il controllo granulare degli accessi per il dominio, devi anche mappare il ruolo a un utente nelle OpenSearch dashboard, altrimenti vedrai errori di autorizzazione.

Per ulteriori informazioni sulle policy di accesso a , consulta the section called “Configurazione delle policy di accesso”.

Mappatura del ruolo Lambda (se si utilizza il controllo granulare degli accessi)

Il controllo granulare degli accessi introduce un passaggio aggiuntivo prima che sia possibile testare l'applicazione. Anche se si utilizza l'autenticazione di base HTTP per tutti gli altri scopi, è necessario mappare il ruolo Lambda all'utente, altrimenti si riceveranno errori di autorizzazione.

1. Vai all'URL delle OpenSearch dashboard per il dominio.
2. Dal menu principale, scegli Sicurezza, Ruoli e seleziona il link al `all_access` ruolo a cui devi mappare il ruolo Lambda.
3. Scegliere Utenti mappati, Gestisci mappatura.
4. In Backend roles (Ruoli di backend), aggiungi il nome della risorsa Amazon (ARN) del ruolo Lambda. L'ARN dovrebbe assumere la forma di. `arn:aws:iam::123456789123:role/service-role/opensearch-lambda-role-1abcdefg`

5. Selezionare Mappa e confermare che l'utente o il ruolo venga visualizzato in Utenti mappati.

Fase 5: Test dell'applicazione Web

Per testare l'applicazione Web

1. Scaricare sample-site.zip, decomprimerlo e aprire `scripts/search.js` nell'editor di testo preferito.
2. Aggiorna la `apigatewayendpoint` variabile in modo che punti all'endpoint API Gateway e aggiungi una barra rovesciata alla fine del percorso specificato. Puoi trovare rapidamente l'endpoint in API Gateway scegliendo Stages (Fasi) e selezionando il nome dell'API. La `apigatewayendpoint` variabile deve assumere la forma di /. `https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/opensearch-api-test`
3. Aprire `index.html` e provare a eseguire la ricerca di thor, house e qualche altro termine.

Movie Search

thor

Found 7 results.

Thor

2011 — 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.

Thor: The Dark World

2013 — Faced with an enemy that even Odin and Asgard cannot withstand, Thor must embark on his most perilous and personal journey yet, one that will reunite him with Jane Foster and force him to sacrifice everything to save us all.

Vikingdom

2013 — A forgotten king, Eirick, is tasked with the impossible odds to defeat Thor, the God of Thunder.

Risoluzione degli errori CORS

Anche se la funzione Lambda include contenuti nella risposta per il supporto di CORS, è comunque possibile che venga visualizzato il seguente errore:

```
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.
```

In tal caso, prova quanto seguente:

1. Abilita CORS sulla risorsa GET. In Advanced (Avanzati), imposta Access-Control-Allow-Credentials a `'true'`.
2. Ridistribuisci la tua API in API Gateway (Actions (Operazioni),Deploy API (Distribuzione dell'API)).
3. Elimina e aggiungi nuovamente la tua attivazione della funzione Lambda. Aggiungila nuovamente, scegli Aggiungi trigger e crea l'endpoint HTTP che richiama la tua funzione. Il trigger deve avere la seguente configurazione:

Trigger	API	Fase della distribuzione	Sicurezza
API Gateway	opensearch-api	opensearch-api-test	Aperta

Passaggi successivi

Questo capitolo è solo un punto di partenza per dimostrare un concetto. Potresti valutare se apportare le seguenti modifiche:

- Aggiungi i tuoi dati al dominio del servizio. OpenSearch
- Aggiungere metodi all'API.
- Nella funzione Lambda, modificare la query di ricerca o potenziare campi diversi.
- Utilizzare uno stile diverso per i risultati o modificare `search.js` per visualizzare campi diversi all'utente.

Tutorial: Visualizzazione delle chiamate all'assistenza clienti con OpenSearch Service e Dashboards OpenSearch

Questo capitolo è un'analisi completa della seguente situazione: un'azienda riceve un numero di chiamate al servizio di assistenza clienti e desidera analizzarle. Qual è l'argomento di ogni chiamata? Quante sono state positive? Quante sono state negative? In che modo i responsabili possono cercare o analizzare le trascrizioni di queste chiamate?

Un flusso di lavoro manuale potrebbe coinvolgere dipendenti che ascoltano le registrazioni, annotano l'oggetto di ciascuna chiamata e decidono se l'interazione con il cliente è stata positiva.

Tale processo sarebbe estremamente impegnativo. Considerando un tempo medio di 10 minuti per chiamata, ogni dipendente potrebbe ascoltare solo 48 chiamate al giorno. Ad eccezione di eventuali distorsioni umane, i dati generati sarebbero altamente accurati, ma la quantità di dati sarebbe minima: solo l'oggetto della chiamata e un Boolean se il cliente è soddisfatto oppure no. Qualcosa di più complesso, come una trascrizione completa, potrebbe richiedere una grande quantità di tempo.

Grazie a Amazon S3, Amazon Transcribe, Amazon Comprehend e Amazon OpenSearch Service, è possibile automatizzare un processo analogo con pochissimo codice e ottenere molti più dati. Ad esempio, è possibile ottenere una trascrizione completa della chiamata, le parole chiave dalla trascrizione e un "sentiment" della chiamata (positivo, negativo, neutro o misto). Quindi è possibile utilizzare OpenSearch e OpenSearch Dashboards per cercare e visualizzare i dati.

Sebbene sia possibile utilizzare questa spiegazione passo per passo così com'è, l'intento è dare vita a nuove idee su come arricchire i documenti JSON prima di indicizzarli in Service. OpenSearch

Costi stimati

In generale, l'esecuzione della procedura indicata in questo scenario avrebbe un costo inferiore a $2. La procedura guidata utilizza le risorse seguenti:

- Bucket S3 con meno di 100 MB trasferiti e memorizzati

  Per ulteriori informazioni, consultare Amazon S3 Pricing.
- OpenSearchDominio di servizio con un'`t2.medium`istanza e 10 GiB di spazio di archiviazione per diverse ore

  Per ulteriori informazioni, consultare Prezzi di Amazon OpenSearch Service Pricing.
- Chiamate multiple ad Amazon Transcribe

Per ulteriori informazioni, consultare Prezzi di Amazon Transcribe.

- Diverse chiamate di elaborazione del linguaggio naturale ad Amazon Comprehend

  Per ulteriori informazioni, consultare Prezzi di Amazon Comprehend.

Argomenti

Fase 1: Configurazione dei prerequisiti

Prima di procedere, devi disporre delle risorse indicate di seguito.

Prerequisito	Descrizione
Bucket Amazon S3	Per ulteriori informazioni, consulta Creazione di un bucket nella Guida per l'utente di Amazon Simple Storage Service.
OpenSearchDominio del servizio	Destinazione per i dati. Per ulteriori informazioni, consulta Creazione di domini OpenSearch di servizio.

Se non si dispone già di queste risorse, è possibile crearle utilizzando i comandi AWS CLI seguenti:

```
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**
>
> Questi comandi utilizzano la regione `us-west-2`, ma è possibile usare qualsiasi regione supportata da Amazon Comprehend. Per ulteriori informazioni consulta Riferimenti generali di AWS.

Fase 2: Copia del codice di esempio

1. Copiare e incollare il seguente codice di esempio Python 3 in un nuovo file denominato `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. Aggiornare le prime sei variabili.
3. Installare i pacchetti necessari utilizzando i comandi seguenti:

```
pip install boto3
pip install requests
pip install requests_aws4auth
```

4. Posizionare MP3 nella stessa directory di `call-center.py` ed eseguire lo script. Di seguito è riportato un output di esempio:

```
$ 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` esegue una serie di operazioni:

1. Lo script carica un file audio (in questo caso, un MP3, ma Amazon Transcribe supporta diversi formati) nel bucket S3.
2. Invia l'URL del file audio ad Amazon Transcribe e attende il completamento del processo di trascrizione.

   Il tempo necessario per completare il processo di trascrizione dipende dalla durata del file audio. Supponiamo siano minuti, non secondi.

   > **Tip**
   >
   > Per migliorare la qualità della trascrizione, è possibile configurare un vocabolario personalizzato per Amazon Transcribe.

3. Una volta completato il processo di trascrizione, lo script estrae la trascrizione, la riduce a 5.000 caratteri e la invia ad Amazon Comprehend per l'analisi del sentiment e delle parole chiave.
4. Infine, lo script aggiunge la trascrizione completa, le parole chiave, il sentiment e l'attuale timestamp a un documento JSON e lo indicizza in Service. OpenSearch

> **Tip**
>
> LibriVoxdispone di audiolibri di pubblico dominio che puoi usare per i test.

(Facoltativo) Fase 3: Indicizzazione dei dati di esempio

Se non si dispone di un gruppo di registrazioni di chiamate (chi le ha, effettivamente?) è possibile indicizzare i documenti campione in sample-calls.zip, con un risultato simile a quello prodotto da `call-center.py`.

1. Creare un file denominato `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. Aggiornare le prime due variabili per `host` e `region`.
3. Installare il pacchetto necessario utilizzando il seguente comando:

```
pip install opensearch-py
```

4. Scaricare e decomprimere sample-calls.zip.
5. Posizionare `sample-calls.bulk` nella stessa directory di `bulk-helper.py` ed eseguire lo script helper. Di seguito è riportato un output di esempio:

```
$ 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
```

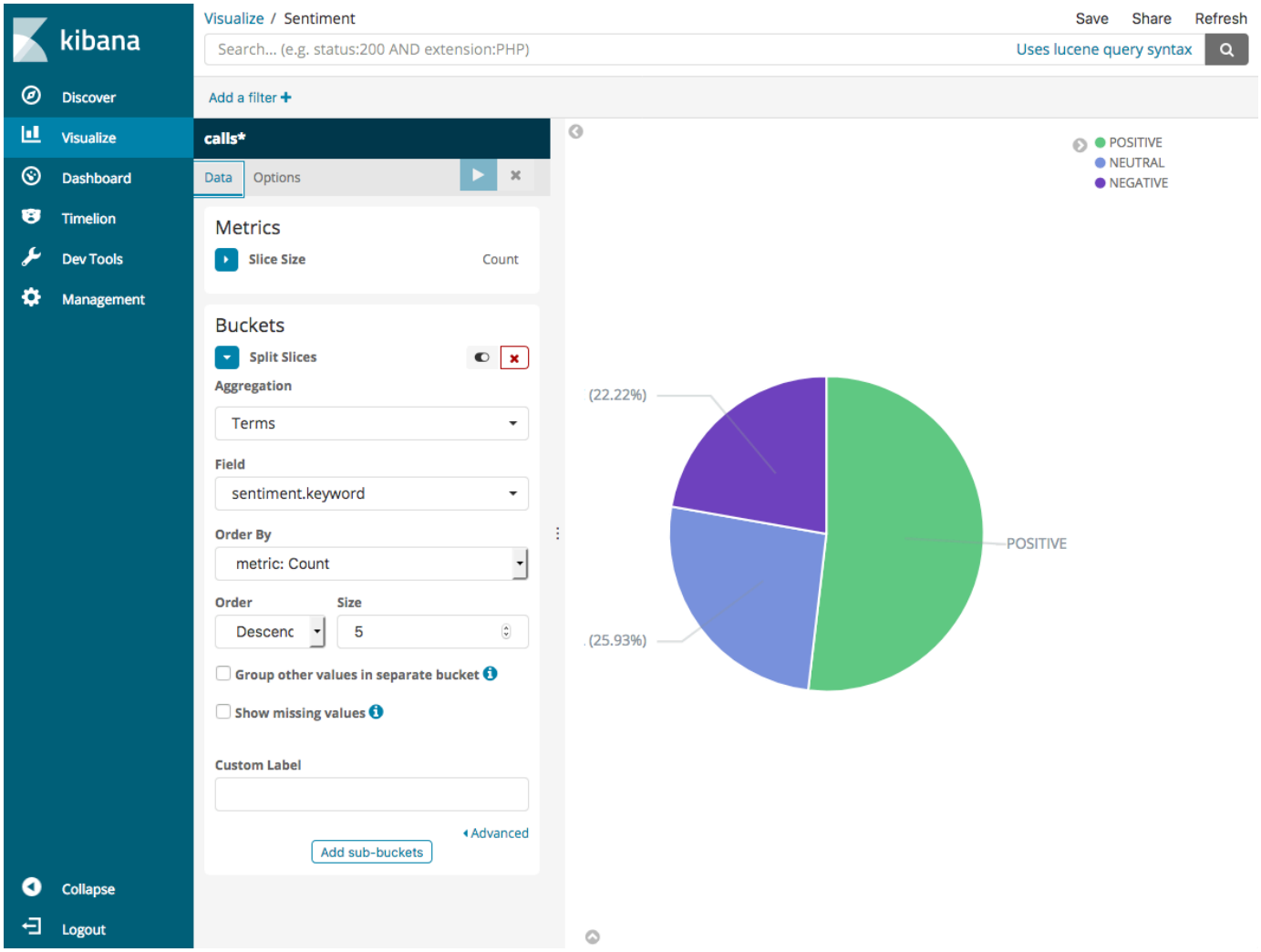
```
        },
        "_type": "_doc",
        "_version": 9,
        "result": "updated",
        "status": 200
      }
    },
    ...
  ],
  "took": 27
}
```

Fase 4: Analisi e visualizzazione dei dati

Ora che si dispone dei dati in OpenSearch Service, è possibile visualizzarli usando OpenSearch Dashboards.

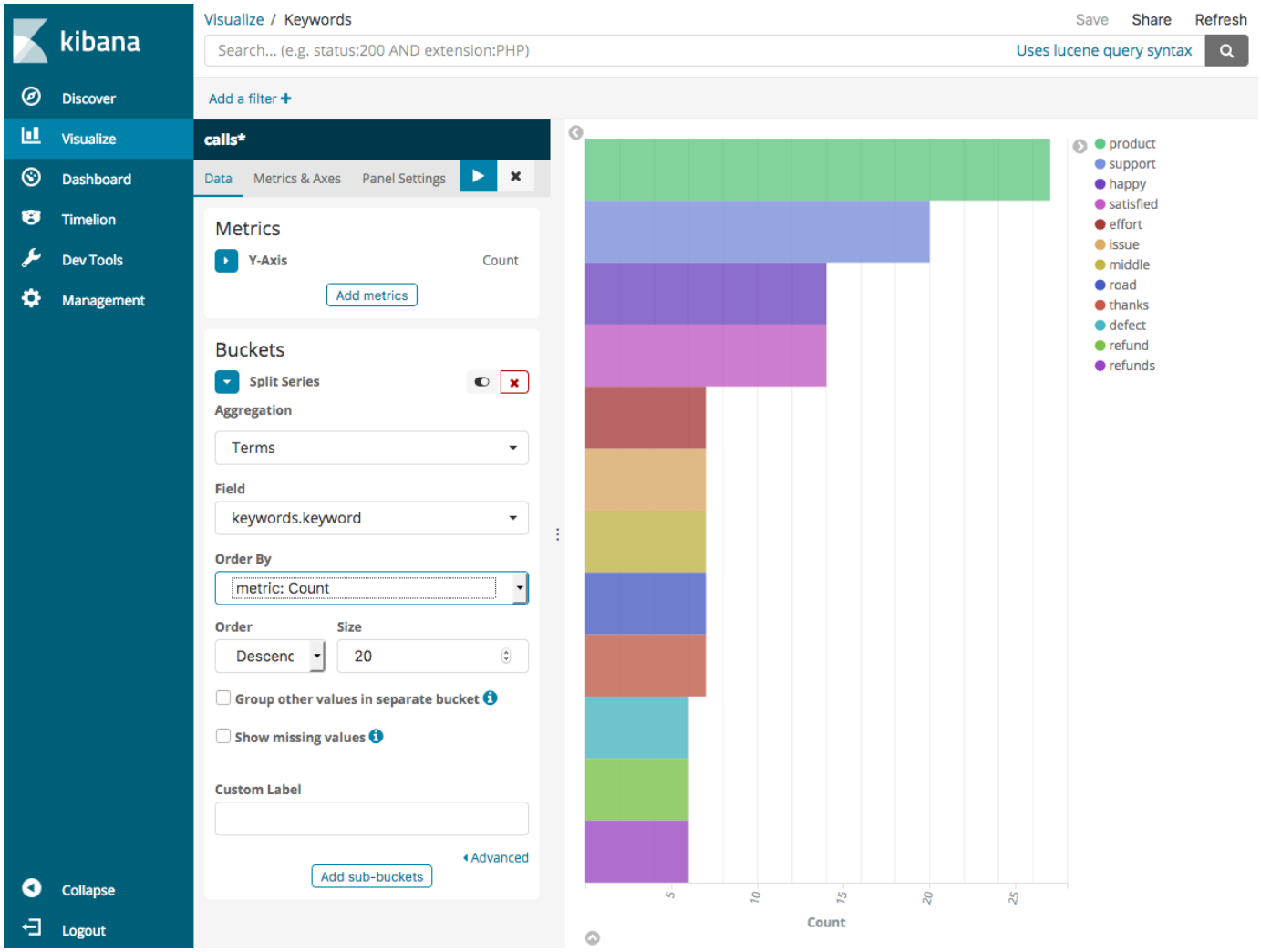
1. Accedere a `https://search-`*`domain`*`.`*`region`*`.es.amazonaws.com/_dashboards`.
2. Prima di utilizzare OpenSearch Dashboards, è però necessario un modello di indice. Dashboards usa modelli di indice per limitare l'analisi a uno o più indici. Per abbinare l'indice `support-calls` creato da `call-center.py`, passare a Gestione degli stack, Modelli di indice e definire un modello di indice di `support*`, quindi scegliere Approfondimenti.
3. In Time Filter field name (Nome campo Filtro tempo), scegliere timestamp.
4. Ora è possibile iniziare a creare le visualizzazioni. Scegliere Visualize (Visualizza), quindi aggiungere una nuova visualizzazione.
5. Scegliere il grafico a torta e il modello dell'indice `support*`.
6. La visualizzazione predefinita è di base, quindi scegliere Split Slices (Dividi sezioni) per creare una visualizzazione più interessante.

   Per Aggregation (Aggregazione) scegliere Terms (Termini). In Field (Campo), scegliere sentiment.keyword. Quindi selezionare Apply changes (Applica modifiche) e poi Save (Salva).

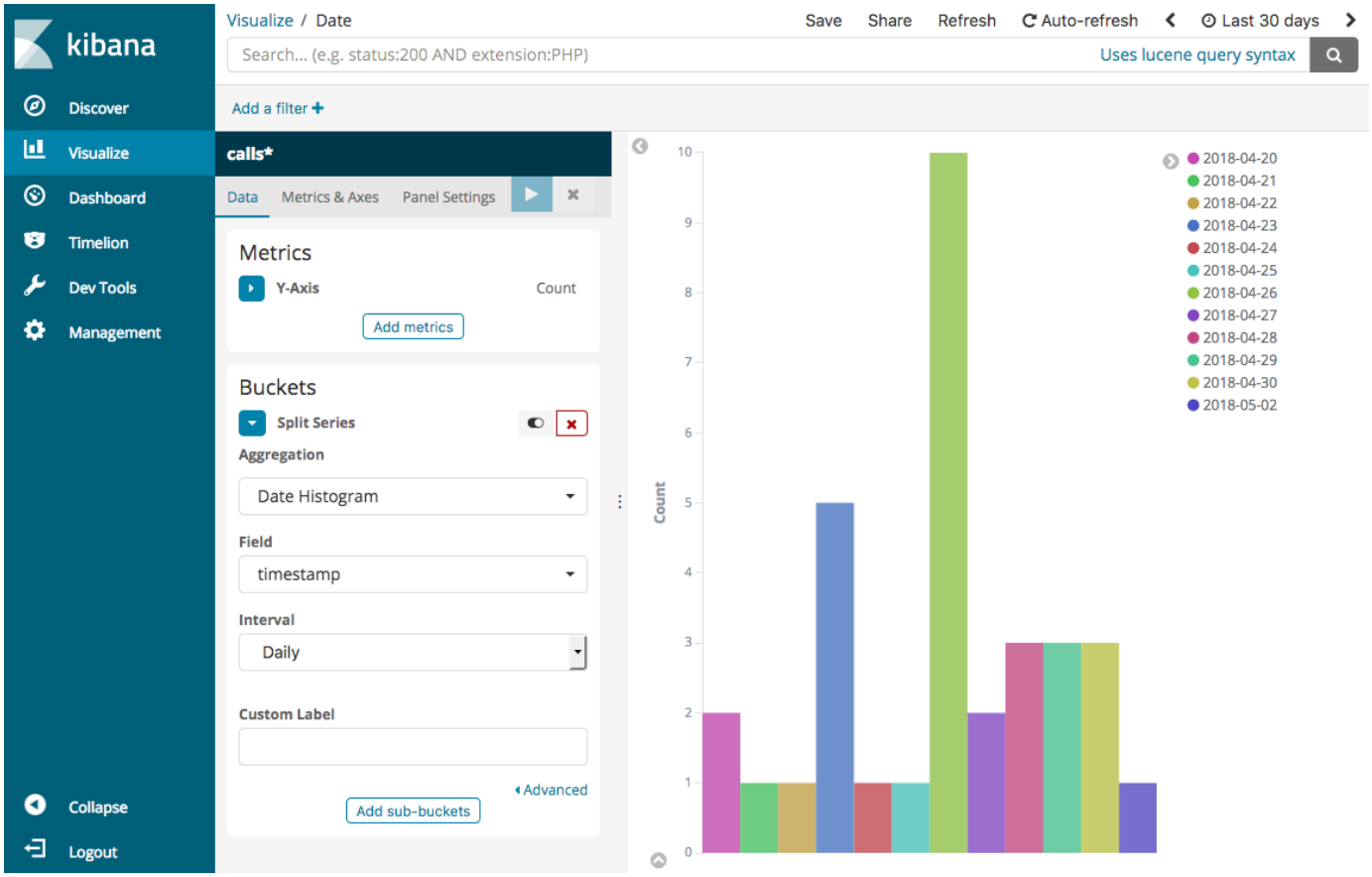


7. Tornare alla pagina Visualize (Visualizza) e aggiungere un'altra visualizzazione. Questa volta, scegliere il grafico a barre orizzontali.
8. Scegliere Split Series (Dividi serie).

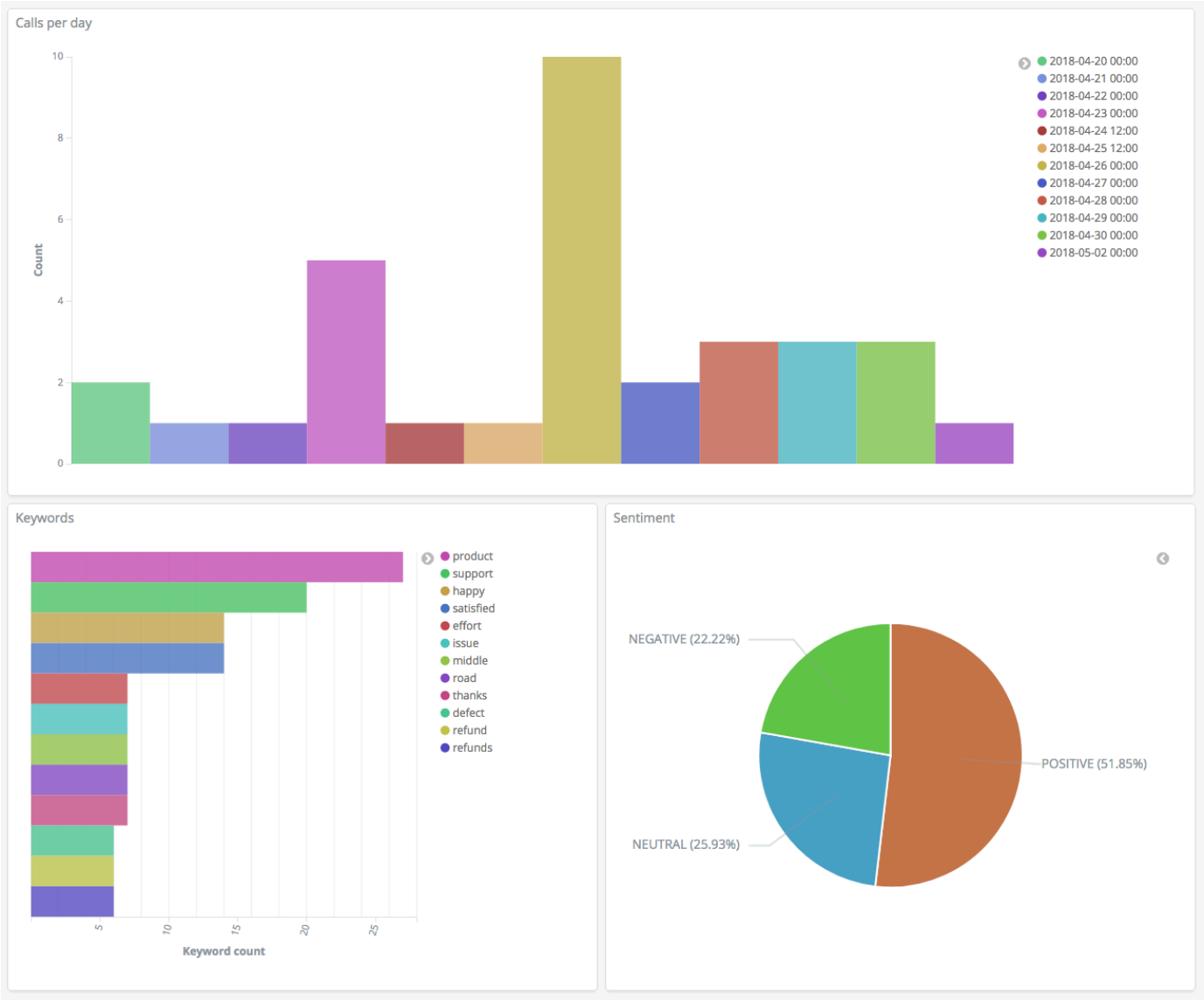
   Per Aggregation (Aggregazione) scegliere Terms (Termini). In Field (Campo), scegliere keywords.keyword e modificare Size (Dimensioni) in 20. Quindi selezionare Apply Changes (Applica modifiche) e poi Save (Salva).



9. Tornare alla pagina Visualize (Visualizza) e aggiungere una visualizzazione finale, un grafico a barre verticali.
10. Scegliere Split Series (Dividi serie). In Aggregation (Aggregazione), scegliere Date Histogram (Istogramma date). In Field (Campo), scegliere timestamp e modificare Interval (Intervallo) in Daily (Giornaliero).
11. Scegliere Metrics & Axes (Parametri e assi) e cambiare Mode (Modalità) in normal (normale).
12. Selezionare Apply Changes (Applica modifiche) e poi Save (Salva).



13. Ora che si dispone di tre visualizzazioni, è possibile aggiungerle a una visualizzazione di Dashboards. Scegliere Dashboard (Pannello di controllo), creare un pannello di controllo e aggiungere le visualizzazioni.



Fase 5: Pulizia delle risorse e fasi successive

Per evitare addebiti non necessari, eliminare il bucket S3 e il dominio di archiviazioneOpenSearch. Per ulteriori informazioni, consulta Eliminazione di un bucket nella Guida per l'utente di Amazon Simple Storage e Eliminazione di un dominio di OpenSearch servizio in questa guida.

Le trascrizioni richiedono molto meno spazio su disco rispetto ai file MP3. È possibile ridurre il periodo di conservazione degli MP3 ad esempio, da tre mesi di registrazioni di chiamate a un mese, conservare anni di trascrizioni e comunque risparmiare sui costi di archiviazione.

È inoltre possibile automatizzare il processo di trascrizione utilizzando AWS Step Functions e Lambda, aggiungere altri metadati prima dell'indicizzazione o progettare visualizzazioni più complesse per casi d'uso specifici.

Rinominazione del servizio OpenSearch di Amazon - Riepilogo delle modifiche

L'8 settembre 2021 la nostra suite di Amazon è stata rinominata servizio OpenSearch di Amazon. OpenSearch Service supporta OpenSearch così come Elasticsearch OSS legacy. Nelle sezioni seguenti vengono descritte le diverse parti del servizio modificate con la rinomina del servizio e le operazioni da eseguire per garantire che i domini continuino a funzionare correttamente.

Alcune di queste modifiche si applicano solo quando si aggiornano i domini da Elasticsearch a OpenSearch. In altri casi, ad esempio nella console di gestione fatturazione e costi, l'esperienza cambia immediatamente.

Questo elenco non è completo. Mentre anche altre parti del prodotto sono cambiate, questi aggiornamenti sono i più rilevanti.

Argomenti

Nuova versione dell'API

La nuova versione dell'API di configurazione del servizio OpenSearch (2021-01-01) funziona con OpenSearch e con Elasticsearch OSS legacy. 21 operazioni API sono state sostituite con nomi più concisi e indipendenti dal motore (ad esempio `CreateElasticsearchDomain`modificato in `CreateDomain`), ma OpenSearch Service continua a supportare entrambe le versioni delle API.

Per creare e gestire domini da questo punto in poi, consigliamo di utilizzare le nuove operazioni API. Notare che quando si utilizzano le nuove operazioni API per creare un dominio, è necessario specificare il parametro `EngineVersion` nel formato `Elasticsearch_X.Y` o `OpenSearch_X.Y`, piuttosto che solo il numero di versione. Se non su specifica una versione, il valore predefinito sarà l'ultima versione di OpenSearch.

Aggiornare la AWS CLI alla versione 1.20.40 o successiva per poter usare `aws opensearch ...` per creare e gestire i domini. Per il nuovo formato della CLI, consultare Documentazione di riferimento della CLI di OpenSearch.

Tipi di istanza rinominati

I tipi di istanza nel servizio OpenSearch di Amazon sono ora nel formato `<type>.<size>.search`, ad esempio `m6g.large.search` piuttosto che `m6g.large.elasticsearch`. Non è necessario eseguire nessuna operazione. I domini esistenti inizieranno automaticamente con riferimento ai nuovi tipi di istanza all'interno dell'API e nella console di gestione fatturazione e costi.

Se sono disponibili istanze riservate (IR), il contratto non sarà influenzato dalla modifica. La versione precedente dell'API di configurazione è ancora compatibile con il vecchio formato di denominazione, ma se si desidera utilizzare la nuova versione dell'API, sarà necessario utilizzare il nuovo formato.

Modifiche delle policy di accesso

Nelle sezioni seguenti vengono descritte le azioni da intraprendere per aggiornare le policy di accesso.

Policy IAM

Consigliamo di aggiornare le policy IAM in modo da utilizzare le operazioni API rinominate. Tuttavia, OpenSearch Service continuerà a rispettare le policy esistenti replicando internamente le vecchie autorizzazioni API. Ad esempio, se al momento si dispone dell'autorizzazione per eseguire l'operazione `CreateElasticsearchDomain`, è ora possibile effettuare sia chiamate a `CreateElasticsearchDomain` (vecchia operazione API) che a `CreateDomain` (nuova operazione API). Lo stesso vale per i rifiuti espliciti. Per un elenco delle operazioni API aggiornate, consultare il riferimento all'elemento policy.

Policy SCP

Le policy di controllo dei servizi (SCP) introducono un ulteriore livello di complessità rispetto allo standard IAM. Per evitare che le policy SCP non vengano rispettate, è necessario aggiungere sia le vecchie operazioni che le nuove per ogni policy SCP. Ad esempio, se un utente dispone attualmente delle autorizzazioni per `CreateElasticsearchDomain`, è necessario concedere loro anche le autorizzazioni per `CreateDomain` in modo che possano mantenere la possibilità di creare domini. Lo stesso vale per i rifiuti espliciti.

Ad esempio:

```
"Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:CreateElasticsearchDomain",
        "es:CreateDomain"
         ...
      ],
    },
      "Effect": "Deny",
      "Action:" [
        "es:DeleteElasticsearchDomain",
        "es:DeleteDomain"
         ...
```

Nuovi tipi di risorsa

OpenSearch Service introduce i seguenti nuovi tipi di risorse:

Risorsa	Descrizione
`AWS::OpenSearchService::Domain`	Rappresenta un dominio del servizio OpenSearch di Amazon. Questa risorsa esiste a livello di servizio e non è specifica del software in esecuzione nel dominio. Si applica a servizi come AWS CloudFormation e AWS Resource Groups, in cui è possibile

Risorsa	Descrizione
	creare e gestire le risorse per il servizio nel suo complesso. Per istruzioni su come aggiornare i domini definiti in CloudFormation da Elasticsearch a OpenSearch, vedere Osservazioni nella guida per l'utente di CloudFormation.
`AWS::OpenSearch::Domain`	Rappresenta il software OpenSearch/Elastic search in esecuzione su un dominio. Questa risorsa si applica a servizi come AWS CloudTrail e AWS Config, che fanno riferimento al software in esecuzione sul dominio piuttosto che a OpenSearch Service nel suo complesso . Questi servizi ora contengono tipi di risorse separati per i domini che eseguono Elasticse arch (`AWS::Elasticsearch::Domain`) rispetto ai domini che eseguono OpenSearch (`AWS::OpenSearch::Domain`).

> **Note**
>
> In AWS Config, i dati saranno disponibili nel tipo di risorsa `AWS::Elasticsearch::Domain` per diverse settimane, anche se uno o più domini vengono aggiornati a OpenSearch.

Kibana rinominato in OpenSearch Dashboards

OpenSearch Dashboards, l'alternativa AWS a Kibana, è uno strumento di visualizzazione open source progettato per funzionare con OpenSearch. Dopo l'aggiornamento di un dominio da Elasticsearch a OpenSearch, l'endpoint `/_plugin/kibana` cambia in `/_dashboards`. Il servizio OpenSearch reindirizzerà tutte le richieste al nuovo endpoint, ma se si utilizza l'endpoint Kibana in una qualsiasi delle policy IAM, aggiornare tali policy per includere anche il nuovo endpoint `/_dashboards`.

Se si utilizza the section called “Autenticazione SAML per dashboard OpenSearch ”, prima di aggiornare il dominio a OpenSearch, è necessario modificare tutti gli URL Kibana configurati nel provider di identità (IdP) da `/_plugin/kibana` a `/_dashboards`. Gli URL più comuni sono gli URL del servizio consumer assertion (ACS) e gli URL dei destinatari.

Il ruolo `kibana_read_only` predefinito per OpenSearch Dashboards è stato rinominato come `opensearch_dashboards_read_only`, e il ruolo `kibana_user` è stato rinominato come `opensearch_dashboards_user`. La modifica si applica a tutti i domini OpenSearch 1.x appena creato che eseguono il software del servizio R20211203 o versioni successive. Se si aggiorna un dominio esistente al software del servizio R20211203, i nomi dei ruoli rimangono invariati.

Parametri CloudWatch rinominati

Per i domini che eseguono OpenSearch diversi parametri CloudWatch cambiano. Quando si aggiorna un dominio a OpenSearch, i parametri cambiano automaticamente e gli avvisi CloudWatch si interromperanno. Prima di aggiornare il cluster da una versione di Elasticsearch a una versione di OpenSearch, assicurarsi di aggiornare gli allarmi CloudWatch in modo che utilizzino i nuovi parametri.

Sono stati modificati i seguenti parametri:

Nome parametro originale	Nuovo nome
`KibanaHealthyNodes`	`OpenSearchDashboardsHealthyNodes`
`KibanaConcurrentConnections`	`OpenSearchDashboardsConcurrentConnections`
`KibanaHeapTotal`	`OpenSearchDashboardsHeapTotal`
`KibanaHeapUsed`	`OpenSearchDashboardsHeapUsed`
`KibanaHeapUtilization`	`OpenSearchDashboardsHeapUtilization`
`KibanaOS1MinuteLoad`	`OpenSearchDashboardsOS1MinuteLoad`
`KibanaRequestTotal`	`OpenSearchDashboardsRequestTotal`

Nome parametro originale	Nuovo nome
`KibanaResponseTimesMaxInMillis`	`OpenSearchDashboardsResponseTimesMaxInMillis`
`ESReportingFailedRequestSysErrCount`	`KibanaReportingFailedRequestSysErrCount`
`ESReportingRequestCount`	`KibanaReportingRequestCount`
`ESReportingFailedRequestUserErrCount`	`KibanaReportingFailedRequestUserErrCount`
`ESReportingSuccessCount`	`KibanaReportingSuccessCount`
`ElasticsearchRequests`	`OpenSearchRequests`

Per un elenco completo dei parametri inviati da OpenSearch Service ad Amazon CloudWatch, consultare the section called “Monitoraggio dei parametri del cluster”.

Modifiche della console Gestione fatturazione e costi

I dati della cronologia nella console Gestione fatturazione e costi e in Report di costi e utilizzo continueranno a utilizzare il vecchio nome del servizio, quindi è necessario iniziare a utilizzare i filtri sia per il servizio OpenSearch di Amazon sia per Elasticsearch precedente durante la ricerca di dati. Se sono presenti report salvati esistenti, aggiornare i filtri per assicurarsi che includano anche OpenSearch Service. Inizialmente è possibile che venga ricevuto un avviso quando l'utilizzo diminuisce per Elasticsearch e aumenta per OpenSearch, ma scompare in pochi giorni.

Oltre al nome del servizio, i campi seguenti verranno modificati per tutti i report, le fatture e le operazioni API del listino prezzi:

Campo	Vecchio formato	Nuovo formato
Tipo di istanza	`m5.large.elasticsearch`	`m5.large.search`

Campo	Vecchio formato	Nuovo formato
Famiglia di prodotti	Istanza Elasticsearch Volume Elasticsearch	Istanza del servizio OpenSearch di Amazon Volume del servizio OpenSearch di Amazon
Descrizione dei prezzi	5.098 USD per ora di istanza c5.18xlarge.elasticsearch (o ora parziale) - EU	5.098 USD per ora di istanza c5.18xlarge.search (o ora parziale) - EU
Famiglia di istanze	`ultrawarm.elasticsearch`	`ultrawarm.search`

Nuovo formato evento

Il formato degli eventi che OpenSearch Service invia ad Amazon EventBridge e Amazon CloudWatch è cambiato, in particolare il campo `detail-type`. Il campo di origine (`aws.es`) rimane lo stesso. Per il formato completo per ogni tipo di evento, consultare the section called “Monitoraggio degli eventi”. Se si dispone di regole di evento esistenti che dipendono dal formato precedente, assicurarsi di aggiornarle in modo che siano conformi al nuovo formato.

Cosa rimane lo stesso?

Le seguenti caratteristiche e funzionalità, tra le altre non elencate, rimarranno invariate:

- Principale del servizio (`es.amazonaws.com`)
- Codice fornitore
- ARN di dominio
- Endpoint di dominio

Guida introduttiva: Aggiornamento dei domini a OpenSearch 1.x

OpenSearch 1.x supporta gli aggiornamenti dalle versioni 6.8 e 7.x di Elasticsearch. Per istruzioni su come aggiornare il dominio, consultare the section called “Avvio di un aggiornamento (console)”.

Se si utilizza la AWS CLI o l'API di configurazione per aggiornare il dominio, è necessario specificare `TargetVersion` come `OpenSearch_1.x`.

OpenSearch 1.x introduce un'impostazione di dominio aggiuntiva denominata Abilita modalità di compatibilità. Poiché alcuni client e plug-in di Elasticsearch OSS controllano la versione del cluster prima della connessione, la modalità di compatibilità imposta OpenSearch per segnalare la versione 7.10 in modo che questi client continuino a funzionare.

È possibile attivare la modalità di compatibilità quando si creano domini OpenSearch per la prima volta o quando si esegue l'aggiornamento a OpenSearch da una versione di Elasticsearch. Se non è impostato, viene ripristinato il parametro predefinito, `false`, quando crei un dominio e `true` quando esegui l'aggiornamento di un dominio.

Per abilitare la modalità di compatibilità utilizzando l'API di configurazione, impostare `override_main_response_version` su `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"
   }
}
```

Per abilitare o disabilitare la modalità di compatibilità in domini OpenSearch esistenti, è necessario utilizzare l'operazione API _cluster/settings di OpenSearch:

```
PUT /_cluster/settings
{
  "persistent" : {
    "compatibility.override_main_response_version" : true
  }
}
```

Risoluzione dei problemi con Amazon OpenSearch Service

Questo argomento descrive come identificare e risolvere i problemi più comuni OpenSearch di Amazon Service. Consulta le informazioni contenute in questa sezione prima di contattare AWS Support.

Impossibile accedere alle OpenSearch dashboard

L'endpoint OpenSearch Dashboards non supporta le richieste firmate. Se la policy di controllo accessi per il dominio consente l'accesso solo a determinati ruoli IAM e non è stata configurata l'autenticazione Amazon Cognito, quando si prova ad accedere a Dashboards è possibile che venga ricevuto il seguente messaggio di errore:

```
"User: anonymous is not authorized to perform: es:ESHttpGet"
```

Se il tuo dominio di OpenSearch servizio utilizza l'accesso VPC, potresti non ricevere questo errore, ma la richiesta potrebbe scadere. Per ulteriori informazioni su come correggere questo problema e le varie opzioni di configurazione disponibili, consulta the section called “Controllo dell'accesso ai dashboard OpenSearch ”, the section called “Informazioni sulle policy d'accesso nei domini VPC” e the section called “Identity and Access Management”.

Impossibile accedere al dominio VPC

Consulta the section called “Informazioni sulle policy d'accesso nei domini VPC” e the section called “Test dei domini VPC”.

Cluster in stato di sola lettura

Rispetto alle versioni precedenti di Elasticsearch ed Elasticsearch 7 OpenSearch . x utilizza un sistema diverso per il coordinamento dei cluster. In questo nuovo sistema, quando il cluster perde il quorum, il cluster non è disponibile finché non si esegue un'azione. La perdita del quorum può assumere due forme:

- Se il cluster utilizza nodi master dedicati, la perdita del quorum si verifica quando metà o più nodi non sono disponibili.

- Se il cluster non utilizza nodi master dedicati, la perdita del quorum si verifica quando metà o più nodi di dati non sono disponibili.

Se si verifica una perdita del quorum e il cluster ha più di un nodo, OpenSearch Service ripristina il quorum e imposta il cluster in uno stato di sola lettura. Sono disponibili due opzioni:

- Rimuovi lo stato di sola lettura e utilizza il cluster così com'è.
- Ripristina il cluster o i singoli indici da uno snapshot.

Se preferisci utilizzare il cluster così com'è, verifica che lo stato del cluster sia verde utilizzando la seguente richiesta:

```
GET _cat/health?v
```

Se lo stato del cluster è rosso, ti consigliamo di ripristinare il cluster da uno snapshot. Puoi anche consultare the section called “Cluster in stato rosso” per la risoluzione dei problemi. Se l'integrità del cluster è verde, controlla che tutti gli indici previsti siano presenti utilizzando la seguente richiesta:

```
GET _cat/indices?v
```

Quindi esegui alcune ricerche per verificare che i dati previsti siano presenti. In caso affermativo, puoi rimuovere lo stato di sola lettura utilizzando la seguente richiesta:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.blocks.read_only": false
  }
}
```

Se si verifica una perdita del quorum e il cluster ha un solo nodo, OpenSearch Service sostituisce il nodo e non pone il cluster in uno stato di sola lettura. In caso contrario, le opzioni sono le stesse: utilizza il cluster così com'è o ripristina da uno snapshot.

In entrambe le situazioni, OpenSearch Service invia due eventi al tuo. AWS Health Dashboard Il primo segnala la perdita del quorum. Il secondo si verifica dopo che il OpenSearch Servizio ha ripristinato correttamente il quorum. Per ulteriori informazioni sull'utilizzo di AWS Health Dashboard, consulta la Guida per l'AWS Health utente.

Cluster in stato rosso

Lo stato rosso del cluster indica che almeno uno shard primario e le relative repliche non sono allocati a un nodo. OpenSearch Il servizio continua a cercare di scattare istantanee automatiche di tutti gli indici indipendentemente dal loro stato, ma le istantanee falliscono finché persiste lo stato rosso del cluster.

Le cause più comuni dello stato rosso del cluster sono l'errore dei nodi del cluster e l'arresto anomalo del OpenSearch processo a causa di un carico di elaborazione continuo e intenso.

> **Note**
>
> OpenSearch Il servizio archivia le istantanee automatizzate per 14 giorni indipendentemente dallo stato del cluster. Pertanto, se lo stato rosso del cluster persiste per più di due settimane, l'ultimo snapshot automatico integro verrà eliminato e i dati del cluster potrebbero essere persi definitivamente. Se il dominio del OpenSearch servizio assume lo stato di cluster rosso, AWS Support potresti contattarti per chiederti se desideri risolvere il problema da solo o se desideri ricevere assistenza dal team di supporto. Puoi impostare un CloudWatch allarme per avvisarti quando si verifica lo stato di un cluster rosso.

In definitiva, partizioni rosse causano cluster rossi e indici rossi causano partizioni rosse. Per identificare gli indici che causano lo stato rosso del cluster, OpenSearch dispone di alcune API utili.

- `GET /_cluster/allocation/explain` sceglie la prima partizione non assegnata che trova e spiega perché non può essere allocata 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` mostra lo stato di integrità, il numero di documenti e l'utilizzo del disco per ogni indice:

```
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
```

L'eliminazione degli indici rossi è il modo più rapido per risolvere uno stato rosso del cluster. A seconda del motivo dello stato del cluster rosso, è possibile ridimensionare il dominio di OpenSearch servizio in modo da utilizzare tipi di istanze più grandi, più istanze o più storage basato su EBS e provare a ricreare gli indici problematici.

Se non è possibile eliminare un indice problematico, puoi ripristinare una snapshot, eliminare documenti dall'indice, modificarne le impostazioni, ridurre il numero di repliche o eliminare altri indici per liberare spazio su disco. Il passaggio importante consiste nel risolvere lo stato rosso del cluster prima di riconfigurare il dominio di servizio. OpenSearch Riconfigurare un dominio con un cluster in stato rosso può peggiorare il problema e portare al blocco del dominio nello stato di configurazione Processing (Elaborazione) finché lo stato rosso non sarà risolto.

Correzione automatico di cluster rossi

Se lo stato del cluster è continuamente rosso per più di un'ora, il OpenSearch Servizio tenta di correggerlo automaticamente reindirizzando gli shard non allocati o ripristinando le istantanee precedenti.

Se non riesce a correggere uno o più indici rossi e lo stato del cluster rimane rosso per un totale di 14 giorni, il OpenSearch Servizio intraprende ulteriori azioni solo se il cluster soddisfa almeno uno dei seguenti criteri:

- Ha una sola zona di disponibilità
- Non ha nodi principali dedicati
- Contiene i tipi di istanze espandibili (T2 o T3)

Al momento, se il cluster soddisfa uno di questi criteri, il OpenSearch Servizio invia notifiche giornaliere nei prossimi 7 giorni per spiegare che se non correggi questi indici, tutti gli shard non assegnati verranno eliminati. Se lo stato del cluster è ancora rosso dopo 21 giorni, il OpenSearch Servizio elimina gli shard non assegnati (archiviazione e calcolo) su tutti gli indici rossi. Riceverai notifiche nel pannello Notifiche della console di OpenSearch servizio per ciascuno di questi eventi. Per ulteriori informazioni, consulta the section called “Eventi sull'integrità del cluster”.

Ripristino da un carico di elaborazione costantemente elevato

Per determinare se un cluster è in stato rosso a causa di un carico di elaborazione costantemente elevato su un nodo di dati, monitora i seguenti parametri del cluster.

Parametro pertinente	Descrizione	Ripristino
JVM MemoryPressure	Specifica la percentuale massima dell'heap di Java utilizzata per tutti i nodi di dati in un cluster. Visualizza la statistica Massimo per questo parametro e cerca drop sempre minori nella pressione della memoria mano aman mano che il garbage collector Java riesce a recuperare memoria sufficiente. Questo modello è probabilmente dovuto a query complesse o campi di dati di grandi dimensioni. I tipi di istanza x86 utilizzano il garbage collector (GC) Concurrent Mark Sweep (CMS), che viene eseguito insieme ai thread dell'applicazione per tenere le pause brevi. Se CMS non è in grado di recuperare memoria sufficiente durante le raccolte normali, attiva una garbage collection (GC) completa, che può portare a lunghe pause dell'appl	Imposta interruttori di memoria per JVM. Per ulteriori informazioni, consulta the section called “JVM OutOfMemoryError”. Se il problema persiste, elimina indici non necessari, riduci il numero o la complessità delle richieste per il dominio, aggiungi istanze oppure utilizza tipi di istanza di dimensioni maggiori.

Parametro pertinente	Descrizione	Ripristino
	icazione con un impatto sulla stabilità del cluster. I tipi di istanza Graviton basati su ARM utilizzano il garbage collector (GC) Garbage-First (G1), che è simile a CMS, ma utilizza ulteriori brevi pause e deframmentazione heap per ridurre ulteriormente la necessità di garbage collection complete. In entrambi i casi, se l'utilizzo della memoria continua a crescere oltre i limiti che il Garbage Collector può recuperare durante le Garbage Collection complete, OpenSearch si blocca con un errore di memoria esaurita. Su tutti i tipi di istanza, è preferibile mantenere l'utilizzo al di sotto dell'80%. L'API `_nodes/stats/jvm` offre un riepilogo delle statistiche JVM, dell'utilizzo dei pool di memoria e della garbage collection: `GET domain-endpoint /_nodes/stats/jvm?pretty`	
CPUUtilization	Specifica la percentuale di risorse della CPU utilizzate per i nodi di dati in un cluster. Visualizza la statistica Maximum (Massimo) per questo parametro e cerca un modello continuo di utilizzo elevato.	Aggiungi nodi di dati o passa a tipi di istanza più grandi per i nodi di dati esistenti.

Parametro pertinente	Descrizione	Ripristino
Nodi	Specifica il numero di nodi in un cluster. Visualizza la statistica Minimum (Minimo) per questo parametro. Questo valore fluttua quando il servizio distribuisce un nuovo parco di istanze per un cluster.	Aggiungi nodi di dati.

Stato giallo del cluster

Un cluster in stato giallo indica che le partizioni principali per tutti gli indici sono allocate sui nodi in un cluster, ma che le partizioni di replica per almeno un indice non lo sono. I cluster a nodo singolo si inizializzano sempre con uno stato di cluster giallo perché non esiste nessun altro nodo a cui Service può assegnare una replica. OpenSearch Per portare il cluster in stato verde, aumenta il numero di nodi. Per ulteriori informazioni, consultare the section called “Dimensionamento dei domini”.

I cluster a più nodi potrebbero avere brevemente uno stato di cluster giallo dopo la creazione di un nuovo indice o dopo un errore di nodo. Questo stato si risolve automaticamente durante la replica dei dati nel cluster. OpenSearch Anche la mancanza di spazio su disco può provocare uno stato del cluster giallo; il cluster può distribuire partizioni di replica solo se i nodi dispongono dello spazio su disco per ospitarle.

ClusterBlockException

L'errore `ClusterBlockException` può presentarsi per i motivi indicati di seguito.

Mancanza di spazio di archiviazione disponibile

Se uno o più nodi del cluster hanno uno spazio di archiviazione inferiore al valore minimo di 1) 20% dello spazio di archiviazione disponibile o 2) 20 GiB di spazio di archiviazione, le operazioni di scrittura di base come l'aggiunta di documenti e la creazione di indici possono iniziare a fallire. the section called “Calcolo dei requisiti di archiviazione”fornisce un riepilogo di come il OpenSearch Servizio utilizza lo spazio su disco.

Per evitare problemi, monitora la `FreeStorageSpace` metrica nella console di OpenSearch servizio e crea CloudWatch allarmi da attivare quando `FreeStorageSpace` scende al di sotto di una certa soglia. `GET /_cat/allocation?v`fornisce anche un utile riepilogo dell'allocazione degli shard e dell'utilizzo del disco. Per risolvere i problemi associati alla mancanza di spazio di archiviazione, ridimensiona il dominio del OpenSearch servizio per utilizzare tipi di istanze più grandi, più istanze o più storage basato su EBS.

Pressione di memoria JVM elevata

Quando la MemoryPressure metrica JVM supera il 92% per 30 minuti, OpenSearch Service attiva un meccanismo di protezione e blocca tutte le operazioni di scrittura per evitare che il cluster raggiunga lo stato rosso. Quando la protezione è attiva, le operazioni di scrittura hanno esito negativo con errore `ClusterBlockException`, non è possibile creare nuovi indici e viene generato l'errore `IndexCreateBlockException`.

Quando la MemoryPressure metrica JVM torna all'88% o meno per cinque minuti, la protezione viene disabilitata e le operazioni di scrittura sul cluster vengono sbloccate.

Una pressione della memoria JVM elevata può essere causata da picchi nel numero di richieste al cluster, allocazioni di partizioni sbilanciate tra i nodi, troppe partizioni in un cluster, esplosioni di dati di campo o di mappatura degli indici o tipi di istanze che non sono in grado di gestire i carichi in ingresso. Può essere causata anche dall'utilizzo di aggregazioni, caratteri jolly o ampi intervalli temporali nelle query.

Per ridurre il traffico verso il cluster e risolvere problemi di pressione della memoria JVM elevata, prova una o più delle seguenti operazioni:

- Scala il dominio in modo che la dimensione massima dell'heap per nodo sia di 32 GB.
- Riduci il numero di partizioni eliminando gli indici vecchi o inutilizzati.
- Cancella la cache dei dati con l'operazione API `POST` *`index-name`*`/_cache/clear?fielddata=true`. Tieni presente che la cancellazione della cache può interrompere le query in corso.

In generale, per evitare una pressione della memoria JVM elevata in futuro, segui queste best practice:

- Evita l'aggregazione su campi di testo o modifica il tipo mappatura per i tuoi indici in `keyword`.
- Ottimizza le richieste di ricerca e indicizzazione scegliendo il numero corretto di partizioni.

- Imposta le policy ISM (Index State Management) per rimuovere gli indici inutilizzati con regolarità.

Errore durante la migrazione a Multi-AZ con Standby

I seguenti problemi potrebbero verificarsi quando si migra un dominio esistente su Multi-AZ in modalità standby.

Creazione di un indice, di un modello di indice o di una politica ISM durante la migrazione da domini senza standby a domini con standby

Se si crea un indice durante la migrazione di un dominio da Multi-AZ senza Standby a con Standby e il modello di indice o la politica ISM non seguono le linee guida consigliate sulla copia dei dati, ciò può causare un'incoerenza dei dati e la migrazione potrebbe non riuscire. Per evitare questa situazione, crea il nuovo indice con un numero di copie dei dati (compresi i nodi primari e le repliche) multiplo di tre. Puoi controllare l'avanzamento della migrazione utilizzando l'API. `DescribeDomainChangeProgress` Se si verifica un errore di conteggio delle repliche, correggilo e contatta l'AWS assistenza per riprovare la migrazione.

Numero errato di copie dei dati

Se non disponi del numero corretto di copie dei dati nel tuo dominio, la migrazione a Multi-AZ con Standby avrà esito negativo.

JVM OutOfMemoryError

Un errore `OutOfMemoryError` JVM in genere significa che è stato raggiunto uno dei seguenti interruttori JVM.

Interruttore	Descrizione	Proprietà impostazione cluster
Interruttore padre	Percentuale totale di memoria heap JVM consentita per tutti gli interruttori. Il valore di default è 95%.	`indices.breaker.total.limit`
Interruttore campo dati	Percentuale di memoria heap JVM consentita per	`indices.breaker.fielddata.limit`

Interruttore	Descrizione	Proprietà impostazione cluster
	caricare in memoria un singolo campo di dati. Il valore predefinito è 40%. Se vengono caricati dati con campi di grandi dimensioni, è possibile che sia necessario aumentare tale limite.	
Interruttore richieste	Percentuale di memoria heap JVM consentita per le strutture di dati utilizzat e nelle risposte a una richiesta di servizio. Il valore predefinito è 60%. Se le richieste di servizio prevedono il calcolo di aggregazioni, è consiglia bile aumentare tale limite.	`indices.breaker.request.limit`

Nodi cluster con errori

Le istanze Amazon EC2 potrebbero andare incontro a terminazioni e riavvii imprevisti. In genere, OpenSearch Service riavvia i nodi automaticamente. Tuttavia, è possibile che uno o più nodi di un OpenSearch cluster rimangano in una condizione di errore.

Per verificare questa condizione, apri la dashboard del dominio nella console OpenSearch di servizio. Passa alla scheda Integrità del cluster e scegli il parametro Numero totale di nodi. Verifica se il numero di nodi indicati è inferiore al numero che hai configurato per il tuo cluster. Se dal parametro emerge che uno o più nodi restano non disponibili per più di un giorno, contatta AWS Support.

Puoi anche impostare un CloudWatch allarme per avvisarti quando si verifica questo problema.

> **Note**
>
> Il parametro Numero totale di nodi non è preciso durante le modifiche della configurazione del cluster e durante la manutenzione di routine per il servizio. Si tratta di un comportamento normale. Il parametro tornerà a indicare il numero corretto di nodi del cluster a breve. Per ulteriori informazioni, consulta the section called “Modifiche di configurazione”.

Per proteggere i cluster da terminazioni e riavvii imprevisti dei nodi, crea almeno una replica per ogni indice del dominio di servizio. OpenSearch

Limite massimo di partizioni superato

OpenSearch oltre a 7. le versioni x di Elasticsearch hanno un'impostazione predefinita di non più di 1.000 shard per nodo. OpenSearch/Elasticsearch genera un errore se una richiesta, ad esempio la creazione di un nuovo indice, comporta il superamento di questo limite. Se si verifica questo errore, sono disponibili diverse opzioni:

- Aggiungere più nodi di dati al cluster.
- Aumentare l'impostazione `_cluster/settings/cluster.max_shards_per_node`.
- Utilizzare l'API _shrink per ridurre il numero di partizioni sul nodo.

Dominio bloccato nello stato di elaborazione

Il dominio del OpenSearch servizio entra nello stato «Elaborazione» quando è nel bel mezzo di una modifica della configurazione. Quando si avvia una modifica alla configurazione, lo stato del dominio passa a «Elaborazione» mentre il OpenSearch Servizio crea un nuovo ambiente. Nel nuovo ambiente, OpenSearch Service lancia un nuovo set di nodi applicabili (come data, master o UltraWarm). Al termine della migrazione, i nodi più vecchi vengono terminati.

Il cluster può rimanere bloccato nello stato "Elaborazione" se si verifica una di queste situazioni:

- Un nuovo set di nodi di dati non può essere avviato.

- La migrazione della partizione al nuovo set di nodi di dati non riesce.
- Il controllo di convalida non è riuscito con errori.

Per i passaggi di risoluzione dettagliati in ciascuna di queste situazioni, consulta Perché il mio dominio Amazon OpenSearch Service è bloccato nello stato «Elaborazione»? .

Saldo di burst EBS basso

OpenSearch Il servizio ti invia una notifica sulla console quando il saldo di burst EBS su uno dei tuoi volumi General Purpose (SSD) è inferiore al 70% e una notifica di follow-up se il saldo scende al di sotto del 20%. Per risolvere questo problema, puoi aumentare le dimensioni del cluster o ridurre gli IOPS di lettura e scrittura in modo da poter accreditare il saldo di burst. Il saldo di espansione rimane a 0 per i domini con tipi di volumi gp3 e i domini con volumi gp2 con una dimensione del volume superiore a 1.000 GiB. Per ulteriori informazioni, consulta General Purpose SSD volumes (gp2) (Volumi SSD a scopo generico [gp2]). Puoi monitorare il burst balance di EBS con la metrica. `BurstBalance` CloudWatch

Impossibile abilitare i log di verifica

Potresti riscontrare il seguente errore quando tenti di abilitare la pubblicazione dei registri di controllo utilizzando la OpenSearch console di servizio:

La politica di accesso alle risorse specificata per il gruppo di log CloudWatch Logs non concede autorizzazioni sufficienti ad Amazon OpenSearch Service per creare un flusso di log. Controllare la policy di accesso alle risorse.

Se si verifica questo errore, verificare che l'elemento `resource` della policy includa l'ARN del gruppo di log corretto. Se lo fa, procedere come indicato di seguito:

1. Attendere qualche minuto.
2. Aggiornare la pagina nel browser Web.
3. Scegli Seleziona gruppo esistente.
4. Per Gruppo di log esistente, scegliere il gruppo di log creato prima di ricevere il messaggio di errore.
5. Nella sezione Policy di accesso, scegli Seleziona policy esistente.
6. Per Policy esistente, scegliere la policy creata prima di ricevere il messaggio di errore.
7. Scegli Enable (Abilita).

Se l'errore persiste anche dopo aver ripetuto il processo più volte, contattare AWS Support.

Impossibile chiudere l'indice

OpenSearch Il servizio supporta l'`_close`API solo per le versioni 7.4 OpenSearch e successive di Elasticsearch. Se si utilizza una versione più vecchia e si sta ripristinando un indice da uno snapshot, è possibile eliminare l'indice esistente (prima o dopo la reindicizzazione).

Controlli delle licenze client

Le distribuzioni predefinite di Logstash e Beats includono un controllo della licenza proprietaria e non riescono a connettersi alla versione open source di. OpenSearch Assicurati di utilizzare le distribuzioni Apache 2.0 (OSS) di questi client con Service. OpenSearch

Limitazione delle richieste

Se si ricevono errori `403 Request throttled due to too many requests` o `429 Too Many Requests` persistenti, considerare il dimensionamento verticale. Amazon OpenSearch Service limita le richieste se il payload fa sì che l'utilizzo della memoria superi la dimensione massima dell'heap Java.

Impossibile eseguire SSH nel nodo

Non puoi usare SSH per accedere a nessuno dei nodi del tuo OpenSearch cluster e non puoi modificarlo direttamente. `opensearch.yml` Utilizza invece la console o gli AWS CLI SDK per configurare il tuo dominio. Puoi specificare alcune impostazioni a livello di cluster anche utilizzando le API OpenSearch REST. Per ulteriori informazioni, consulta Amazon OpenSearch Service API Reference ethe section called “Operazioni supportate”.

Se hai bisogno di maggiori informazioni sulle prestazioni del cluster, puoi pubblicare i log degli errori e gli slow log su. CloudWatch

Errore snapshot "Non valido per la classe di archiviazione dell'oggetto"

OpenSearch Le istantanee del servizio non supportano la classe di storage S3 Glacier. È possibile che si verifichi questo errore quando si prova a elencare gli snapshot se il bucket S3 include una regola del ciclo di vita che trasferisce gli oggetti alla classe di archiviazione S3 Glacier.

Se è necessario ripristinare uno snapshot dal bucket, ripristinare gli oggetti da S3 Glacier, copiare gli oggetti su un nuovo bucket e registrare il nuovo bucket come archivio di snapshot.

Intestazione dell'host non valida

OpenSearch Il servizio richiede che i client lo specifichino `Host` nelle intestazioni della richiesta. A valore `Host` valido è l'endpoint del dominio senza `https://`, come:

```
Host: search-my-sample-domain-ih2lhn2ew2scurji.us-west-2.es.amazonaws.com
```

Se ricevi un `Invalid Host Header` errore durante la richiesta, verifica che il client o il proxy includa l'endpoint del dominio OpenSearch Service (e non, ad esempio, il relativo indirizzo IP) nell'`Host`intestazione.

Tipo di istanza M3 non valido

OpenSearch Il servizio non supporta l'aggiunta o la modifica di istanze M3 a domini esistenti che eseguono OpenSearch o eseguono versioni di Elasticsearch 6.7 e successive. È possibile continuare a utilizzare le istanze M3 con Elasticsearch 6.5 e versioni precedenti.

Si consiglia di scegliere un tipo di istanza più recente. Per i domini che eseguono Elasticsearch 6.7 OpenSearch o versioni successive, si applicano le seguenti restrizioni:

- Se il dominio esistente non utilizza istanze M3, non è più possibile passare a tali istanze.
- Se si modifica un dominio esistente da un tipo di istanza M3 a un altro tipo di istanza, non è possibile tornare indietro.

Le hot query smettono di funzionare dopo l'attivazione UltraWarm

Quando si abilita UltraWarm su un dominio, se non sono presenti sostituzioni preesistenti all'`search.max_buckets`impostazione, OpenSearch Service imposta automaticamente il valore per evitare che le query che richiedono molta memoria `10000` saturino i nodi caldi. Se le tue hot query utilizzano più di 10.000 bucket, potrebbero smettere di funzionare quando abiliti. UltraWarm

Poiché non puoi modificare questa impostazione a causa della natura gestita di Amazon OpenSearch Service, devi aprire una richiesta di assistenza per aumentare il limite. Gli aumenti di limite non richiedono un abbonamento Premium Support.

Impossibile eseguire il downgrade dopo l'aggiornamento

Gli aggiornamenti locali sono irreversibili, ma se si contatta il AWS Supporto, è possibile ripristinare lo snapshot automatico pre-aggiornamento in un nuovo dominio. Ad esempio, se aggiorni un dominio da Elasticsearch 5.6 a 6.4, AWS Support può aiutarti a ripristinare lo snapshot precedente all'aggiornamento su un nuovo dominio Elasticsearch 5.6. Se dal dominio originale è stato preso uno snapshot manuale, è possibile eseguire questa fase da soli.

È necessario il riepilogo dei domini di tutte le Regioni AWS

Lo script seguente utilizza il AWS CLI comando Amazon EC2 describe-regions per creare un elenco di tutte le regioni in cui OpenSearch il servizio potrebbe essere disponibile. Quindi chiama per ogni regione list-domain-names:

```
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
```

Per ogni regione si riceve il seguente output:

```
Listing domains in region:'us-west-2'...
[
  {
    "DomainName": "sample-domain"
  }
]
```

Le regioni in cui il OpenSearch servizio non è disponibile restituiscono «Impossibile connettersi all'URL dell'endpoint».

Errore del browser durante l'utilizzo OpenSearch delle dashboard

Il browser inserisce i messaggi di errore del servizio negli oggetti di risposta HTTP quando si utilizzano le dashboard per visualizzare i dati nel dominio del servizio. OpenSearch Puoi usare gli strumenti di sviluppo comunemente disponibili nei Web browser, ad esempio la modalità di sviluppo in Chrome, per visualizzare gli errori del servizio sottostanti e semplificare le attività di debug.

Per visualizzare gli errori del servizio in Chrome

1. Dalla barra dei menu principale di Chrome, scegliere Visualizza, Sviluppatore, Strumenti per gli sviluppatori.
2. Scegliere la scheda Network (Rete).
3. Nella colonna Status (Stato) scegliere qualsiasi sessione HTTP con stato 500.

Per visualizzare gli errori del servizio in Firefox

1. Dal menu scegliere Tools (Strumenti), Web Developer (Sviluppatore Web), Network (Rete).
2. Scegliere qualsiasi sessione HTTP con stato 500.
3. Scegliere la scheda Response (Risposta) per visualizzare la risposta del servizio.

Asimmetria di partizioni e storage di nodi

L'asimmetria di partizioni di nodi si verifica quando uno o più nodi all'interno di un cluster presentano un numero significativamente maggiore di partizioni rispetto agli altri nodi. L'asimmetria di storage di nodi si verifica quando uno o più nodi all'interno di un cluster presentano una quantità di storage significativamente maggiore (`disk.indices`) rispetto agli altri nodi. Sebbene entrambe queste condizioni possano verificarsi temporaneamente, ad esempio quando un dominio ha sostituito un nodo e sta ancora allocando partizioni su quel nodo, se persistono, devono essere risolte.

Per identificare entrambi i tipi di asimmetria, esegui l'operazione API _cat/allocation e confronta le voci `shards` e `disk.indices` nella risposta:

```
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
```

Sebbene alcune asimmetrie di storage siano normali, qualsiasi valore superiore al 10% rispetto alla media è significativo. Quando la distribuzione delle partizioni è asimmetrica, anche l'utilizzo della CPU, della rete e della larghezza di banda del disco può essere asimmetrico. Poiché un maggior numero di dati significa in genere un maggior numero di operazioni di indicizzazione e ricerca, i nodi più pesanti tendono ad essere anche quelli con maggiori risorse, mentre i nodi più leggeri rappresentano una capacità sottoutilizzata.

Correzione: utilizza conteggi di partizioni che siano multipli del numero di nodi di dati per garantire che ogni indice sia distribuito uniformemente tra i nodi di dati.

Asimmetria di partizioni e storage di indici

L'asimmetria di partizioni di indici si verifica quando uno o più nodi contengono più partizioni di un indice rispetto agli altri nodi. L'asimmetria di storage di indici si verifica quando uno o più nodi contengono una quantità sproporzionatamente elevata di storage totale di un indice.

L'asimmetria di indici è più difficile da identificare rispetto all'asimmetria di nodi perché richiede una certa manipolazione dell'output dell'API _cat/shards. Esamina l'asimmetria di indici per verificare se esiste qualche indicazione di asimmetria nei parametri del cluster o del nodo. Di seguito sono riportate le indicazioni comuni dell'asimmetria di indici:

- Errori HTTP 429 che si verificano su un sottoinsieme di nodi di dati
- Accodamento non uniforme delle operazioni di indicizzazione o di ricerca tra i nodi di dati
- Utilizzo non uniforme dell'heap della JVM e/o della CPU tra i nodi di dati

Correzione: utilizza conteggi di partizioni che siano multipli del numero di nodi di dati per garantire che ogni indice sia distribuito uniformemente tra i nodi di dati. Se la memorizzazione dell'indice o lo shard skew persistono, potrebbe essere necessario forzare la riallocazione degli shard, operazione che si verifica con ogni distribuzione blu/verde del dominio di servizio. OpenSearch

Operazione non autorizzata dopo la selezione dell'accesso VPC

Quando crei un nuovo dominio utilizzando la console di OpenSearch servizio, hai la possibilità di selezionare VPC o accesso pubblico. Se si seleziona Accesso VPC, il OpenSearch servizio richiede informazioni sul VPC e fallisce se non si dispone delle autorizzazioni appropriate:

```
You are not authorized to perform this operation. (Service: AmazonEC2; Status Code:
 403; Error Code: UnauthorizedOperation
```

Per permettere questa query, è necessario disporre di accesso alle operazioni `ec2:DescribeVpcs`, `ec2:DescribeSubnets` ed `ec2:DescribeSecurityGroups`. Questo requisito riguarda solo la console. Se utilizzi la AWS CLI per creare e configurare un dominio con un endpoint VPC, non è necessario accedere a tali operazioni.

Caricamento bloccato dopo la creazione di un dominio VPC

Dopo aver creato un nuovo dominio che usa l'accesso VPC, il valore di Configuration state (Stato di configurazione) del dominio potrebbe non andare mai oltre Loading (Caricamento). Se si verifica questo problema, probabilmente hai disabilitato AWS Security Token Service (AWS STS) per la tua regione.

Per aggiungere endpoint VPC al tuo VPC, OpenSearch Service deve assumere il ruolo. `AWSServiceRoleForAmazonOpenSearchService` Pertanto, AWS STS deve essere abilitato a creare nuovi domini che utilizzano l'accesso VPC in una determinata regione. Per ulteriori informazioni sull'attivazione e la disabilitazione AWS STS, consulta la IAM User Guide.

Richieste rifiutate all'API OpenSearch

Con l'introduzione del controllo degli accessi basato su tag per l' OpenSearch API, potresti iniziare a vedere errori di accesso negato dove prima non si verificavano. Ciò potrebbe essere dovuto al fatto che una o più policy di accesso contiene `Deny` che usa la condizione `ResourceTag` e tali condizioni ora sono soddisfatte.

Ad esempio, la policy seguente utilizzata per negare l'accesso solo all'azione `CreateDomain` dall'API di configurazione, se il dominio aveva il tag `environment=production`. Anche se l'elenco delle azioni include anche `ESHttpPut`, la dichiarazione di negazione non si applicava a tale o ad altre azioni `ESHttp*`.

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

```
      "es:ESHttpPut"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Con il supporto aggiunto dei tag per i metodi OpenSearch HTTP, una policy basata sull'identità IAM come quella sopra riportata comporterà il rifiuto dell'accesso all'azione all'utente collegato. `ESHttpPut` In precedenza, in assenza di convalida di tag, l'utente collegato poteva comunque inviare richieste PUT.

Se inizi a scoprire errori di accesso negato dopo aver aggiornato i domini al software di servizio R20220323 o versioni successive, controlla le policy di accesso basate sull'identità per verificare se il problema è questo e aggiornali, se necessario, per consentire l'accesso.

Impossibile connettersi da Alpine Linux

Alpine Linux limita la dimensione della risposta DNS a 512 byte. Se tenti di connetterti al tuo dominio di OpenSearch servizio da Alpine Linux versione 3.18.0 o precedente, la risoluzione DNS può fallire se il dominio si trova in un VPC e ha più di 20 nodi. Se utilizzi una versione di Alpine Linux successiva alla 3.18.0, dovresti essere in grado di risolvere più di 20 host. Per ulteriori informazioni, consulta le note di rilascio di Alpine Linux 3.18.0.

Se il proprio dominio è in un VPC, si consiglia di usare altre distribuzioni Linux, come Debian, Ubuntu, CentOS, Red Hat Enterprise Linux o Amazon Linux 2, per connettersi a esso.

Troppe richieste per Search Backpressure

Il controllo degli accessi basato sulla CPU è un meccanismo di controllo che limita in modo proattivo il numero di richieste a un nodo in base alla sua capacità attuale, sia in caso di aumenti organici che di picchi di traffico. Un numero eccessivo di richieste restituisce un codice di stato HTTP 429 «Troppe

richieste» in caso di rifiuto. Questi errori indicano risorse di cluster insufficienti, richieste di ricerca che richiedono molte risorse o un picco involontario del carico di lavoro.

Search Backpressure fornisce il motivo del rifiuto, che può aiutare a ottimizzare le richieste di ricerca che richiedono molte risorse. In caso di picchi di traffico, consigliamo di ripetere i tentativi sul lato client con backoff e jitter esponenziali.

Errore di certificato quando si utilizza un SDK

Poiché AWS gli SDK utilizzano i certificati CA del tuo computer, le modifiche ai certificati sui AWS server possono causare errori di connessione quando tenti di utilizzare un SDK. I messaggi di errore variano, ma in genere contengono il testo seguente:

```
Failed to query OpenSearch
...
SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

Puoi prevenire questi errori conservando i certificati CA e il sistema operativo del tuo computer. up-to-date Se si riscontra questo problema in un ambiente aziendale e non si gestisce il computer in uso, potrebbe essere necessario richiedere all'amministratore assistenza con il processo di aggiornamento.

Nell'elenco seguente vengono riportati i requisiti minimi del sistema operativo e delle versioni di Java:

- Le versioni di Microsoft Windows con aggiornamenti installati da gennaio 2005 in poi contengono nell'elenco di certificati attendibili almeno uno dei CA richiesti.
- Mac OS X 10.4 con Java per Mac OS X 10.4 release 5 (febbraio 2007), Mac OS X 10.5 (ottobre 2007) e versioni successive contengono nell'elenco di certificati attendibili almeno uno dei CA richiesti.
- Red Hat Enterprise Linux 5 (marzo 2007), 6 e 7 e CentOS 5, 6 e 7 contengono nell'elenco di certificati attendibili almeno uno dei CA richiesti.
- Java 1.4.2_12 (maggio 2006), 5 aggiornamento 2 (marzo 2005) e tutte le versioni successive, incluso Java 6 (dicembre 2006), 7 e 8, contengono nell'elenco di certificati attendibili almeno uno dei CA richiesti.

Le tre autorità di certificazione sono:

- Autorità di certificazione root Amazon 1

- Autorità di certificazione root dei servizi Starfield - G2
- Autorità di certificazione Starfield classe 2

I certificati root delle prime due autorità sono disponibili presso Amazon Trust Services, ma mantenere il computer up-to-date è la soluzione più semplice. Per ulteriori informazioni sui certificati forniti da ACM, consulta le Domande frequenti su AWS Certificate Manager.

> **Note**
>
> Attualmente, i domini di OpenSearch servizio nella regione us-east-1 utilizzano certificati di un'autorità diversa. Prevediamo di aggiornare la regione per l'uso di queste nuove autorità di certificazione in futuro.

Cronologia dei documenti per Amazon OpenSearch Service

Questo argomento descrive importanti modifiche ad Amazon OpenSearch Service. Gli aggiornamenti software del servizio aggiungono il supporto per nuove funzionalità, patch di sicurezza, correzioni di bug e altri miglioramenti. Per utilizzare nuove funzionalità, potrebbe essere necessario aggiornare il software del servizio nel dominio. Per ulteriori informazioni, consulta the section called “Aggiornamenti del software del servizio”.

Le funzionalità del servizio vengono implementate in modo incrementale a seconda del Regioni AWS luogo in cui il servizio è disponibile. Aggiorniamo questa documentazione solo per la prima versione. Non forniamo informazioni sulla disponibilità delle regioni e non annunciamo implementazioni successive delle regioni. Per informazioni sulla disponibilità regionale delle funzionalità del servizio e per iscriverti alle notifiche sugli aggiornamenti, vedi Cosa c'è di AWS nuovo?

Date rilevanti per questa cronologia:

- Versione corrente del prodotto: 2021-01-01
- Ultima versione del prodotto: 12 giugno 2024
- Ultimo aggiornamento della documentazione: 12 giugno 2024

Per ricevere le notifiche sugli aggiornamenti, è possibile sottoscrivere il feed RSS.

> **Note**
>
> Rilascio patch: le versioni del software di servizio che terminano con "-P" e un numero, ad esempio R20211203-P4, sono versioni di patch. È probabile che le patch includano miglioramenti delle prestazioni, correzioni di bug lievi e correzioni di sicurezza o miglioramenti della posizione. Poiché le patch non includono nuove funzionalità o modifiche importanti, generalmente non hanno un impatto diretto sull'utente o sulla documentazione, per cui le specifiche di ogni patch non sono incluse nella cronologia del documento.

Modifica	Descrizione	Data
Nuovi ruoli collegati al servizio	Amazon OpenSearch Service aggiunge un ruolo collegato al	12 giugno 2024

	servizio chiamato`AWSServiceRoleForOpensearchIngestionSelfManagedVpce` , che consente ad Amazon OpenSearch Ingestion di inviare dati metrici a Amazon CloudWatch pipeline con endpoint VPC autogestiti.	
Integrazione Zero-ETL di Amazon OpenSearch Service con Amazon S3	Amazon OpenSearch Service ora supporta le query dirette per interrogare i dati in Amazon S3.	22 maggio 2024
OpenSearch Supporto 2.13	Amazon OpenSearch Service ora supporta la OpenSearch versione 2.13. Questa versione include tutte le funzionalità che facevano parte delle versioni 2.12 e 2.13. Per ulteriori informazioni, consulta le note di rilascio 2.12 e 2.13.	21 maggio 2024
Supporto Amazon OpenSearch Ingestion per Data Prepper versione 2.7	Amazon OpenSearch Ingestion aggiunge il supporto per Data Prepper versione 2.7. Per ulteriori informazioni, consulta le note di rilascio 2.7.	4 aprile 2024
Servizio AWS accesso privato per le collezioni OpenSearch Serverless	Ora puoi concedere l'accesso specifico Servizi AWS, come Amazon Bedrock, alle tue raccolte OpenSearch Serverless all'interno di una politica di accesso alla rete.	28 marzo 2024

Aggiornamenti EBS in loco	Ora puoi apportare alcune modifiche EBS ai tuoi domini senza una distribuzione blu/verde in Amazon Service. OpenSearch	14 febbraio 2024
Visibilità delle modifiche alla configurazione	Ora puoi tenere traccia delle modifiche alla configurazione del dominio nella console OpenSearch di Amazon Service e utilizzando l'API di configurazione.	6 febbraio 2024
Disponibilità generale delle raccolte di ricerca vettoriale	Le raccolte di ricerca vettoriale e Amazon OpenSearch Serverless sono ora disponibili a livello generale. I seguenti miglioramenti importanti sono stati apportati durante la fase di anteprima: • Le raccolte di ricerca vettoriale ora supportano carichi di lavoro con miliardi di vettori, ciascuno con un massimo di 128 dimensioni. • OpenSearch Le dashboard ora supportano le raccolte di ricerca vettoriale.	29 novembre 2023
Istanze OR1	Amazon OpenSearch Service ora supporta i tipi di istanze OR1.	29 novembre 2023

Interrogazioni dirette con Amazon S3 (anteprima)	Le query dirette forniscono una soluzione completamente gestita per rendere disponibili i dati transazionali in Amazon OpenSearch Service entro pochi secondi dalla loro scrittura su un bucket Amazon S3.	29 novembre 2023
Capacità di 10 TiB per le raccolte di serie temporali	Amazon OpenSearch Serverless aggiunge il supporto per un massimo di 10 TiB di dati indicizzati per le raccolte di serie temporali. Questa versione supporta anche una capacità massima consentita di 200 OCU per tutti i tipi di raccolte e la possibilità di disabilitare le repliche in standby quando si crea una raccolta.	29 novembre 2023
OpenSearch Supporto 2.11	Amazon OpenSearch Service ora supporta la OpenSearch versione 2.11. Questa versione include tutte le funzionalità che facevano parte delle versioni 2.10 e 2.11. Per ulteriori informazioni, consulta le note di rilascio 2.10 e 2.11.	17 novembre 2023

Supporto Amazon OpenSearch Ingestion per Data Prepper versione 2.6	Amazon OpenSearch Ingestion aggiunge il supporto per Data Prepper versione 2.6. Per ulteriori informazioni, consulta le note di rilascio 2.6. Inoltre, puoi specificare Amazon DynamoDB come origine della pipeline. Per ulteriori informazioni, consulta Usare una pipeline di OpenSearch ingestione con Amazon DynamoDB.	17 novembre 2023
Supporto Amazon OpenSearch Ingestion per Data Prepper versione 2.5	Amazon OpenSearch Ingestion aggiunge il supporto per Data Prepper versione 2.5. Per ulteriori informazioni, consulta le note di rilascio 2.5. Inoltre, ora puoi specificare un dominio di OpenSearch servizio o una raccolta OpenSearch Serverless come origine della pipeline. Per ulteriori informazioni, consulta il plug-in di OpenSearch origine nella documentazione di Data Prepper.	17 novembre 2023

CloudFormation modello per l'inferenza remota	Per facilitare la configurazione dell'inferenza remota per la ricerca semantica, Amazon OpenSearch Service fornisce un AWS CloudFormation modello nella console che automatizza il processo di provisioning del modello per te.	7 novembre 2023
Aggiornamento della politica relativa ai ruoli collegati ai servizi	Aggiunge le autorizzazioni necessarie alla politica dei ruoli collegati al servizio per assegnare e annullare l'assegnazione degli indirizzi `AmazonOpenSearchServiceRolePolicy` IPv6. Anche la politica obsoleta di Elasticsearch è stata aggiornata per garantire la compatibilità con le versioni precedenti. `AmazonElasticsearchServiceRolePolicy`	26 ottobre 2023

Policy del ciclo di vita OpenSearch di Amazon Serverless	Amazon OpenSearch Serverless introduce le policy del ciclo di vita degli indici per semplificare la gestione della conservazione e dell'eliminazione dei dati. Ora puoi utilizzare le API o un'interfaccia di configurazione nella console per impostare politiche di conservazione dei dati per le raccolte di serie temporali, eliminando la necessità di creare indici o script giornalieri per eliminare i vecchi dati.	25 ottobre 2023
Supporto per istanze Im4gn	Amazon OpenSearch Service ora supporta i tipi di istanze Im4gn. Le istanze Im4gn sono ottimizzate per carichi di lavoro che gestiscono set di dati di grandi dimensioni e richiedono un'elevata densità di storage per vCPU.	20 ottobre 2023
Opzioni amministrative	Amazon OpenSearch Service offre ora diverse opzioni amministrative che forniscono un controllo granulare se devi risolvere problemi con il tuo dominio. Queste opzioni includono la possibilità di riavviare il OpenSearch processo su un nodo di dati e la possibilità di riavviare un nodo di dati.	17 ottobre 2023

Plugin opzionali	Amazon OpenSearch Service aggiunge il supporto per quattro nuovi plugin di analisi linguistica: Nori (coreano) , Sudachi (giapponese), Pinyin (cinese) e StConvert Analysis (cinese), oltre al plug-in Amazon Personalize Search Ranking.	16 ottobre 2023
OpenSearch Supporto 2.9	Amazon OpenSearch Service ora supporta la OpenSearch versione 2.9. Questa versione include tutte le funzionalità che facevano parte delle versioni 2.8 e 2.9. Per ulteriori informazioni, consultate le note di rilascio 2.8 e 2.9.	2 ottobre 2023
Connettori ML	Amazon OpenSearch Service aggiunge il supporto per i connettori di machine learning (ML). I connettori facilitano l'accesso ai modelli ML ospitati su altre Servizi AWS piattaforme di machine learning (ML) o su piattaforme di apprendimento automatico (ML) di terze parti.	6 settembre 2023

Amazon OpenSearch Ingestion aggiunge il supporto per Data Prepper versione 2.4	Amazon OpenSearch Ingestion aggiunge il supporto per Data Prepper versione 2.4. Per ulteriori informazioni, consulta le note di rilascio 2.4. Inoltre, ora puoi specificare Amazon Managed Streaming for Apache Kafka (Amazon MSK) come origine della pipeline.	31 agosto 2023
Capacità di 6 TiB per le raccolte di serie temporali	Amazon OpenSearch Serverless aggiunge il supporto per un massimo di 6 TiB di dati indicizzati per le raccolte di serie temporali . Questa versione supporta anche una capacità massima consentita di 100 OCU per le raccolte di ricerche e di serie temporali.	15 agosto 2023
Raccolte di ricerca vettoriale	Amazon OpenSearch Serverless aggiunge la possibilità di creare una raccolta di ricerche vettorial i, che puoi utilizzare per archiviare incorporamenti vettoriali per potenziare ricerche semantiche e di similarità.	26 luglio 2023

OpenSearch 2.7 supporto	Amazon OpenSearch Service ora supporta OpenSearch la versione 2.7. Questa versione include tutte le funzionalità che facevano parte delle versioni 2.6 e 2.7. Per ulteriori informazioni, consultate le note di rilascio 2.6 e 2.7.	10 luglio 2023
Supporto per Data Prepper 2.3	Amazon OpenSearch Ingestion aggiunge il supporto Data Prepper versione 2.3. Per ulteriori informazioni, consulta le note di rilascio 2.3. Inoltre, ora puoi specificare Amazon Security Lake come origine della pipeline.	26 giugno 2023
Multi-AZ con Standby	Amazon OpenSearch Service aggiunge la possibilità di distribuire un dominio in tre zone di disponibilità (AZ), con ciascuna zona di disponibilità contenente una copia completa dei dati e con i nodi in una di queste zone che fungono da standby. L'opzione di implementazione Multi-AZ with Standby offre una disponibilità del 99,99% e prestazioni costanti in caso di guasto dell'infrastruttura.	3 maggio 2023

Nuovi ruoli collegati al servizio	Amazon OpenSearch Service aggiunge un ruolo collegato al servizio chiamato`AWSServiceRoleForAmazonOpenSearchIngestionService` , che consente ad Amazon OpenSearch Ingestion di inviare dati metrici a. Amazon CloudWatch	26 aprile 2023
OpenSearch Ingestione di Amazon	Amazon OpenSearch Ingestion è un raccoglitore di dati completamente gestito che fornisce dati di log and trace in tempo reale a domini di OpenSearch servizio e raccolte Serverless. OpenSearch OpenSearch Ingestion elimina la necessità di utilizzare soluzioni di terze parti come Logstash o Jaeger per inserire dati nei tuoi domini e nelle tue raccolte.	26 aprile 2023
OpenSearch 2.5 supporto	Amazon OpenSearch Service ora supporta OpenSearch la versione 2.5. Questa versione include tutte le funzionalità che facevano parte delle versioni 2.4 e 2.5. Per ulteriori informazioni, consultate le note di rilascio 2.4 e 2.5.	13 marzo 2023

Finestre di manutenzione non di punta	Amazon OpenSearch Service aggiunge finestre non di punta, ovvero blocchi di tempo giornalieri di 10 ore a basso traffico durante i quali può pianificare gli aggiornamenti del software di servizio e le ottimizzazioni Auto-Tune che richiedono una distribuzione blu/verde. Gli aggiornamenti non di punta aiutano a ridurre al minimo il carico sui nodi master dedicati di un cluster durante i periodi di traffico più intenso. Per i nuovi domini creati dopo il 16 febbraio, la finestra non di punta viene configurata automaticamente tra le 22:00 e le 8:00 ora locale. Per i domini esistenti, devi abilitare esplicitamente la finestra.	16 febbraio 2023
Configurazione dell'autenticazione SAML durante la creazione del dominio	Amazon OpenSearch Service ora supporta la configurazione dell'autenticazione SAML durante la creazione del dominio. In precedenza, era necessario configurare le opzioni SAML dopo che il dominio era già stato creato.	1 febbraio 2023

Reindicizzazione remota per i domini VPC	Amazon OpenSearch Service aggiunge l'opzione per una connessione endpoint VPC tra due domini. È ora possibile utilizzare la reindicizzazione remota per copiare gli indici da un dominio VPC a un altro senza un proxy inverso. Per utilizzare questa funzionalità, i domini VPC devono eseguire il software di servizio R20221114 o versione successiva.	31 gennaio 2023

Disponibilità generale di Amazon OpenSearch Serverless	Amazon OpenSearch Serverless è ora disponibile a livello generale. I seguenti miglioramenti importanti sono stati apportati durante la fase di anteprima: • La capacità può ora essere ridotta fino al minimo delle OCU configurati quando si verifica una diminuzione del traffico sull'endpoint di raccolta. • Il numero massimo di OCU consentite sia per l'indiciz zazione che per la ricerca è stato aumentato da 20 a 50. Ogni OCU include una memoria temporanea a caldo sufficiente per 120 GiB di dati di indice. • È ora possibile configurare le impostazioni di accesso ai dati durante la creazione delle raccolte anziché in un flusso di lavoro separato.	25 gennaio 2023
Esecuzione asincrona	Amazon OpenSearch Service ora supporta l'async dry run, che ti consente di eseguire un controllo di convalida prima di apportare una modifica alla configurazione e ti avvisa se le modifiche causeranno una distribuzione blu/verde.	19 gennaio 2023

Nuovi ruoli collegati al servizio	Amazon OpenSearch Service aggiunge un ruolo collegato al servizio chiamato`AWSServiceRoleForAmazonOpenSearchServerless` , che consente a OpenSearch Serverless di inviare dati metrici a. Amazon CloudWatch	29 novembre 2022
Anteprima di Amazon OpenSearch Serverless	Amazon OpenSearch Serverless è una configurazione serverless su richiesta, con scalabilità automatica per Amazon Service. OpenSearch Serverless rimuove le complessità operative legate al provisioning, alla configurazione e all'ottimizzazione dei cluster. OpenSearch	29 novembre 2022
OpenSearch 2.3 supporto	Amazon OpenSearch Service ora supporta OpenSearch la versione 2.3. Questa versione include tutte le funzionalità che facevano parte delle versioni 2.0, 2.1 e 2.2. Per ulteriori informazioni, consulta le note di rilascio 2.0, 2.1, 2.2 e 2.3. La versione 2.3 contiene una modifica importante. Per ulteriori informazioni, consulta la sezione Percorsi di upgrade supportati.	15 novembre 2022

Supporto per il plug-in Notifications	Amazon OpenSearch Service ora supporta il plug-in Notifications, che offre una posizione centrale per tutte le notifiche provenienti dai OpenSearch plug-in. A partire dalla versione 2.0, le destinazioni degli avvisi sono diventate obsolete e sono state sostituite con canali di notifica.	15 novembre 2022
Supporto per Kibana 7.1.1	I domini Amazon OpenSearch Service che eseguono Elasticsearch 7.1 ora supportano l'ultima versione di patch per Kibana 7.1.1, che aggiunge correzioni di bug e migliora la sicurezza. Quando aggiorni i domini 7.1 al software di servizio R20221114, Service li aggiornerà automaticamente a questa versione di patch. OpenSearch	15 novembre 2022

Supporto per Kibana 6.8.13	I domini Amazon OpenSearch Service che eseguono Elasticsearch 6.8 ora supportano l'ultima versione di patch per Kibana 6.8.13, che aggiunge correzioni di bug e migliora la sicurezza. Quando aggiorni i domini 6.8 al software di servizio R20221114, Service li aggiornerà automaticamente a questa versione di patch. OpenSearch	15 novembre 2022
Supporto per Kibana 6.3.2	I domini Amazon OpenSearch Service che eseguono Elasticsearch 6.3 ora supportano l'ultima versione di patch per Kibana 6.3.2, che aggiunge correzioni di bug e migliora la sicurezza. Quando aggiorni i domini 6.3 al software di servizio R20221114, Service li aggiornerà automaticamente a questa versione di patch. OpenSearch	15 novembre 2022

AWS PrivateLink	Con gli endpoint OpenSearch VPC gestiti da Amazon Service, puoi connetterti direttamente ai domini Service OpenSearch VPC utilizzando un endpoint VPC di interfaccia anziché collegarti tramite Internet. Un endpoint OpenSearch VPC gestito dai servizi è accessibile solo all'interno del VPC in cui viene fornito l'endpoint o da qualsiasi VPC collegato al VPC in cui viene fornito l'endpoint, come consentito dalle tabelle di routing e dai gruppi di sicurezza. Il dominio VPC deve eseguire il software di servizio R20220928 o versione successiva per connettersi a un endpoint VPC di interfaccia.	7 novembre 2022
Correzioni di bug e miglioramenti delle prestazioni	Il software del servizio R20220928 include correzioni di bug e miglioramenti delle prestazioni, tra cui una migliore registrazione SAML. L'aggiornamento modifica anche il tenant predefinito in `Global` anziché `Private`.	3 ottobre 2022

Riferimento alle API migliorato	Amazon OpenSearch Service offre un riferimento API di configurazione migliorato e completo. Questo nuovo riferimento contiene tutte le operazioni e i tipi di dati disponibili, esempi di sintassi di richieste e risposte e collegamenti ai riferimenti SDK corrispondenti per tutti i linguaggi supportati.	13 settembre 2022
Convalida blu/verde	Amazon OpenSearch Service ora esegue un controllo di convalida prima delle distribuzioni blu/green e rileva errori di convalida se il tuo dominio non è idoneo per un aggiornamento.	16 agosto 2022
OpenSearch 1.3 supporto	Amazon OpenSearch Service ora supporta OpenSearch la versione 1.3. Per ulteriori informazioni, consulta le Note di rilascio 1.3.	27 luglio 2022
Supporto per il plugin ML Commons	Amazon OpenSearch Service aggiunge il supporto per il plug-in ML Commons, che fornisce una serie di algoritmi di apprendimento automatico comuni tramite trasporto e chiamate API REST. Puoi anche interagire con il plugin ML Commons tramite i comandi PPL.	27 luglio 2022

Supporto del volume gp3	Amazon OpenSearch Service aggiunge il supporto per il tipo di volume SSD gp3 EBS General Purpose. Puoi specificare capacità di IOPS allocata e velocità di trasmissione effettiva aggiuntive quando crei o modifichi il dominio.	26 luglio 2022
Documentazione delle best practice avanzate	La documentazione OpenSearch di Amazon Service fornisce best practice operative migliorate e consigli generali per la creazione e la gestione dei domini OpenSearch di servizio.	6 luglio 2022
Integrazione con Service Quotas	Ora puoi visualizzare le quote per Amazon OpenSearch Service e richiedere aumenti delle quote dalla console Service Quotas.	29 giugno 2022
Controllo degli accessi basato su tag per l'API OpenSearch	Ora puoi usare i tag per controllare l'accesso alle OpenSearch API. In precedenza, i tag potevano essere utilizzati solo per controllare l'accesso all'API di configurazione.	16 giugno 2022

Ricerca tra cluster tra regioni	La ricerca tra cluster è ora supportata Regioni AWS purché entrambi i domini eseguano Elasticsearch versione 7.10 o successiva o qualsiasi versione di. OpenSearch	14 giugno 2022
Supporto per Kibana 5.6 singolo	Amazon OpenSearch Service aggiunge il supporto per Kibana 5.6.16 singolo. Con Kibana 5.6.16 singolo, puoi utilizzare Kibana 5.6 come front-end durante la connessione alle versioni di Elasticsearch 5.1, 5.3, 5.5 e 5.6. Per utilizzare Kibana 5.6 singolo, è necessario utilizzare il software di servizio R20220323 o versioni successive.	4 aprile 2022
R20220323-P1	Amazon OpenSearch Service ha recentemente rilasciato l'aggiornamento del software di servizio R20220323, ma l'aggiornamento è stato successivamente annullato a causa di un problema. Si consiglia di aggiornare i domini alla versione di patch R20220323-P1 o versione successiva, il che risolve il problema.	4 aprile 2022

OpenSearch 1.2 supporto	Amazon OpenSearch Service ora supporta OpenSearch la versione 1.2. Per ulteriori informazioni, consultare le Note di rilascio 1.2.	4 aprile 2022
Osservabilità	L'installazione predefinita di OpenSearch Dashboards for Amazon OpenSearch Service include il plug-in Observability, che puoi utilizzare per visualizzare eventi basati sui dati utilizzando Piped Processing Language (PPL) per esplorare e interrogare i tuoi dati. Il plug-in richiede OpenSearch 1.2 o versione successiva e il software di servizio R20220323 o successivo.	4 aprile 2022
Supporto per Kibana 7.7.1	I domini Amazon OpenSearch Service che eseguono Elasticsearch 7.7 ora supportano l'ultima versione di patch per Kibana 7.7, che aggiunge correzioni di bug e migliora la sicurezza. Quando aggiorni i domini 7.7 al software di servizio R20220323 o versione successiva, Service li aggiornerà automaticamente a questa versione di patch. OpenSearch	4 aprile 2022

Modifica dei parametri della pressione della memoria JVM	Amazon OpenSearch Service ha modificato la logica delle `JVMMemoryPressure` CloudWatch metriche per riflettere in modo più accurato l'utilizzo della memoria. In precedenza i parametri consideravano solo il pool di memoria di vecchia generazione dell'heap della JVM. Con questa modifica il parametro considera anche il pool di memoria di nuova generazione. Dopo l'aggiornamento del dominio al software di servizio R20220323, è possibile che si verifichi un aumento della `JVMMemoryPressure` , `MasterJVMMemoryPressure` , e/o parametri `WarmJVMMemoryPressure` .	4 aprile 2022
Dizionari personalizzati con il plug-in IK (Chinese) Analysis	Amazon OpenSearch Service ora supporta l'utilizzo di dizionari personalizzati con il plug-in IK (cinese) Analysis.	4 aprile 2022

Replica tra cluster su domini esistenti	Amazon OpenSearch Service ha rimosso la limitazione secondo cui è possibile implementare la ricerca e la replica tra cluster solo su domini creati a partire dal 3 giugno 2020. Ora puoi abilitare queste caratteristiche su tutti i domini indipendentemente dal momento in cui sono state create. Per entrambi i domini è necessario il software di servizio R20220323 o versioni successive.	4 aprile 2022
Visibilità blue/verde dell'implementazione	Amazon OpenSearch Service ora offre una maggiore visibilità sullo stato di avanzamento delle implementazioni blu/green. Puoi monitorare questi dettagli nella console o utilizzando l'API di configurazione.	27 gennaio 2022

Controllo granulare degli accessi sui domini esistenti	Ora puoi abilitare il controllo granulare degli accessi sui domini esistenti. Puoi abilitare un periodo di migrazione temporaneo per le policy di accesso open/basate su per garantire che gli utenti possano continuar e ad accedere al dominio durante la creazione e la mappatura dei ruoli. L'abilita zione del controllo granulare degli accessi sui domini esistenti richiede il software di servizio R20211203 o versioni successive.	6 gennaio 2022
OpenSearch Ruoli Dashboard s rinominati	Con il software di servizio R20211203, il ruolo `kibana_user` è stato rinominato `opensearc h_dashboards_user` , e `kibana_read_only` è stato rinominato `opensearc h_dashboards_read_ only` . Questa modifica si applica a tutti i 1 appena OpenSearch creati. x domini. Per i OpenSearch domini esistenti che vengono aggiornati al software di servizio R20211203, i ruoli rimangono gli stessi.	4 gennaio 2022

OpenSearch 1.1 supporto	Amazon OpenSearch Service ora supporta OpenSearch la versione 1.1. Per ulteriori informazioni, consultare le Note di rilascio 1.1.	4 gennaio 2022
Editor visivo ISM	L'installazione predefinita di OpenSearch Dashboard s for Amazon OpenSearch Service ora supporta l'editor visivo per le politiche ISM. Questa funzionalità richiede la OpenSearch versione 1.1 o successiva.	4 gennaio 2022
Aggiornamento della prevenzione del "confused deputy" tra servizi	Amazon OpenSearch Service supporta l'utilizzo delle chiavi di contesto `aws:SourceArn` e delle condizioni `aws:SourceAccount` globali nelle politiche delle risorse IAM per prevenire il confuso problema del vice. Per utilizzare queste chiavi di condizione, è necessario utilizzare il software di servizio R20211203 o versioni successive.	4 gennaio 2022

Patch Log4j	Il software di servizio R20211203-P2 aggiorna la versione di Log4j utilizzata in OpenSearch Service come consigliato dagli avvisi contenuti in CVE-2021-44228 e CVE-2021-45046. La patch si applica ai domini che eseguono tutte le versioni di Elasticsearch. OpenSearch OpenSearch Il servizio continuerà ad aggiornare internamente varie versioni di Log4j e non saranno necessariamente limitate all'ultima versione di Log4j. La versione di Log4j sul tuo dominio dipende dalla versione del software su cui il dominio è in esecuzione. Tuttavia, indipendentemente dalla versione di Log4j, se utilizzi R20211203-P2 o versioni successive, i domini contengono l'aggiornamento di Log4j necessario per risolvere i problemi di CVE-2021-44228 e CVE-2021-45046.	15 dicembre 2021

Replica tra cluster	La replica tra cluster consente di replicare indici, mappature e metadati da un dominio di servizio a un altro. OpenSearch La replica tra cluster richiede un dominio che esegue Elasticsearch 7.10 o 1.1 o versione successiva. OpenSearch	5 ottobre 2021
AWS Nuove politiche gestite	Il lancio di Amazon OpenSearch Service include nuove politiche AWS gestite e l'eliminazione delle vecchie politiche.	8 settembre 2021
Supporto per Kibana 6.4.3	I domini Amazon OpenSearch Service che eseguono la versione precedente di Elasticsearch 6.4 ora supportano l'ultima versione di patch per Kibana 6.4, che aggiunge correzioni di bug e migliora la sicurezza . OpenSearch Il servizio aggiornerà automaticamente i domini a questa versione di patch.	8 settembre 2021

Flussi di dati	Amazon OpenSearch Service aggiunge il supporto per i flussi di dati, che semplific ano il processo di gestione dei dati delle serie temporali . Il tuo dominio deve avere la OpenSearch versione 1.0 o successiva per utilizzare i flussi di dati.	8 settembre 2021
OpenSearch Servizio Amazon	AWS rinomina Amazon OpenSearch Service per rimuovere il marchio precedent e «Elasticsearch». Amazon OpenSearch Service supporta un sistema operativo OpenSearch Elasticsearch legacy. Quando crei un cluster, puoi scegliere quale motore di ricerca utilizzar e. OpenSearch Il servizio offre un'ampia compatibilità con Elasticsearch OSS 7.10, l'ultima versione open source del software.	8 settembre 2021

Archiviazione a freddo	L'archiviazione a freddo è un nuovo livello di archiviazione per i dati storici o a cui si accede raramente. Gli indici a freddo occupano solo l'archiviazione S3 e non hanno alcun calcolo collegato. L'archiviazione a freddo richiede un dominio che esegue Elasticsearch 7.9 o versione successiva e il software di servizio R20210426 o versione successiva.	13 maggio 2021
Istanze Graviton basate su ARM	Amazon OpenSearch Service ora supporta i tipi di istanze Graviton basati su ARM (M6G, C6G, R6G e R6GD). I tipi di istanza Graviton sono disponibili su domini nuovi ed esistenti che eseguono Elasticsearch 7.9 o versioni successive e software di servizio R20210331 o versioni successive.	4 maggio 2021

Modelli ISM	Amazon OpenSearch Service aggiunge il supporto per i modelli ISM, che consenton o di allegare automatic amente una policy ISM a un indice se l'indice corrispon de a uno schema definito nella policy. I modelli ISM richiedono il software di servizio R20210426 o versioni successive. Questo aggiornam ento rende obsoleta anche l'impostazione `policy_id` , il che significa che non è più possibile utilizzare modelli di indice per applicare policy ISM agli indici appena creati. L'aggiornamento introduce una modifica sostanziale per i CloudFormation modelli esistenti che utilizzano questa impostazione.	27 aprile 2021
Supporto per Elasticsearch 7.10	Amazon OpenSearch Service ora supporta la versione 7.10 di Elasticsearch. Per ulteriori informazioni, consultare Note di rilascio 7.10.	21 aprile 2021

Ricerca asincrona	Amazon OpenSearch Service ora supporta la ricerca asincrona, che consente di eseguire richieste di ricerca in background. La ricerca asincrona richiede un dominio che esegue Elasticsearch 7.10 o versione successiva e il software di servizio R20210331 o versione successiva.	21 aprile 2021
Controllo degli accessi basato su tag per API di configurazione	Ora puoi utilizzare i AWS tag per controllare l'accesso all'API di configurazione di Amazon ES.	2 marzo 2021
Regolazione automatica	Amazon OpenSearch Service aggiunge Auto-Tune, che utilizza i parametri di prestazioni e utilizzo del cluster per suggerire modifiche alle impostazioni JVM sui nodi. La regolazione automatica richiede un dominio che esegue Elasticsearch 6.7 o versione successiva e il software di servizio R20201117 o versione successiva.	24 febbraio 2021

Trace Analytics	L'installazione predefinita di Kibana per Amazon OpenSearch Service ora include il plug-in di analisi delle tracce, che consente di monitorare i dati di traccia dalle applicazioni distribuite. Il plug-in richiede un dominio che esegue Elasticsearch 7.9 o versione successiva e il software di servizio R20210201 o versione successiva.	17 febbraio 2021
Parametri delle partizioni	Amazon OpenSearch Service aggiunge le seguenti CloudWatch metriche per tracciare lo stato degli shard:`Shards.active` ,,, `Shards.unassigned` `Shards.delayedUnassigned` `Shards.activePrimary` ,`Shards.initializing` . `Shards.relocating` I parametri sono disponibili nei domini con software di servizio R20210201 o versioni successive.	17 febbraio 2021

Report di Kibana	L'installazione predefinita di Kibana per Amazon OpenSearch Service ora supporta report su richiesta per le pagine Discover, Visualize e Dashboard. Questa funzionalità richiede Elasticsearch 7.9 o versione successiva e il software di servizio R20210201 o versione successiva.	17 febbraio 2021
Supporto per Kibana 5.6.16	I domini Amazon OpenSearch Service che eseguono Elasticsearch 5.6 ora supportano l'ultima versione di patch per Kibana 5.6, che aggiunge correzioni di bug e migliora la sicurezza. Amazon ES aggiornerà automaticamente i domini a questa versione di patch.	17 febbraio 2021
Crittografia per domini esistenti	Amazon OpenSearch Service ora supporta l'abilitazione della crittografia dei dati inattivi e della node-to-node crittografia su domini esistenti che eseguono Elasticsearch 6.7 o versione successiva. Dopo aver abilitato queste impostazioni, non è possibile disabilitarle.	27 gennaio 2021

Reindicizzazione remota	Amazon OpenSearch Service ora supporta la reindiciz zazione remota, che consente di migrare gli indici da domini remoti. Questa funzional ità richiede il software del servizio R20201117 o versioni successive.	24 novembre 2020
Piped Processing Language (PPL)	Amazon OpenSearch Service ora supporta Piped Processing Language (PPL), un linguaggi o di query che consente di utilizzare la sintassi pipe (|) per interrogare i dati archiviat i in Elasticsearch. Questa funzionalità richiede il software del servizio R20201117 o versioni successive. Per ulteriori informazioni, consultar e.	24 novembre 2020
Notebook Kibana	Amazon OpenSearch Service aggiunge il supporto per i notebook Kibana, che consente di combinare visualizzazioni dal vivo e testo narrativo in un'unica interfaccia. Questa funzional ità richiede il software del servizio R20201117 o versioni successive.	24 novembre 2020

Grafici Gantt	L'installazione predefinita di Kibana per Amazon OpenSearch Service ora supporta un nuovo tipo di visualizzazione, i diagrammi di Gantt. Questa funzionalità richiede il software del servizio R20201117 o versioni successive.	24 novembre 2020
Supporto per Elasticsearch 7.9	Amazon OpenSearch Service ora supporta la versione 7.9 di Elasticsearch. Per ulteriori informazioni, consultare Note di rilascio 7.9.	24 novembre 2020
Aggiornamenti al rilevamento delle anomalie	Il rilevamento delle anomalie per Amazon OpenSearch Service aggiunge il supporto per la cardinalità elevata, che consente di classificare le anomalie con una dimensione come indirizzo IP, ID prodotto, codice paese e così via. Questa funzionalità richiede il software del servizio R20201117 o versioni successive.	24 novembre 2020

Aggiornamenti del dizionario dinamico	Amazon OpenSearch Service ora ti consente di aggiornar e i tuoi analizzatori di ricerca senza reindicizzarli. È possibile aggiornare i file del dizionario su alcuni o tutti i tuoi domini e Amazon ES tiene traccia delle versioni dei pacchetti nel tempo, in modo da avere una cronologi a di ciò che è cambiato e quando. Questa funzional ità richiede il software del servizio R20201019 o versioni successive.	17 novembre 2020
Endpoint personalizzati	Amazon OpenSearc h Service ora supporta endpoint personalizzati, che ti consentono di assegnare al tuo dominio Amazon ES un nuovo URL. Se si scambiano domini, è possibile mantenere lo stesso URL. Questa funzionalità richiede il software del servizio R20201019 o versioni successive.	5 novembre 2020

Nuovi plug-in del linguaggio	Amazon OpenSearch Service ora supporta i plug-in IK (Chinese) Analysis, Vietnames e Analysis e Thai Analysis su domini che eseguono Elasticsearch 7.7 o versione successiva con il software di servizio R20201019 o successivo.	28 ottobre 2020
Supporto per Elasticsearch 7.8	Amazon OpenSearch Service ora supporta la versione 7.8 di Elasticsearch. Per ulteriori informazioni, consultare Note di rilascio 7.8.	28 ottobre 2020
Autenticazione SAML per Kibana	Amazon OpenSearch Service ora supporta l'autenticazione SAML per Kibana, che consente di utilizzare provider di identità di terze parti per accedere a Kibana, gestire il controllo granulare degli accessi, cercare dati e creare visualizzazioni. Questa funzionalità richiede il software del servizio R20201019 o versioni successive.	27 ottobre 2020
Istanze T3	Amazon OpenSearch Service ora supporta i tipi di `t3.medium` istanze `t3.small` e.	23 settembre 2020

Log di verifica	Amazon OpenSearch Service ora supporta i log di controllo per i tuoi dati, che ti consenton o di tenere traccia dei tentativi di accesso falliti, dell'accesso degli utenti a indici, documenti e campi e molto altro. Questa funzionalità richiede il software del servizio R20200910 o versioni successive.	16 settembre 2020
UltraWarm aggiornamenti	UltraWarm per Amazon OpenSearch Service aggiunge nuove metriche, nuove impostazioni, una coda di migrazione più ampia e un'API di cancellazione. Questi aggiornamenti richiedon o il software di servizio R20200910 o versione successiva. Per ulteriori informazioni, consultare .	14 settembre 2020
Learning to Rank	Amazon OpenSearch Service ora supporta il plug-in open source Learning to Rank, che consente di utilizzare tecnologi e di apprendimento automatic o per migliorare la pertinenz a delle ricerche. Questa funzionalità richiede il software del servizio R20200721 o versioni successive.	27 luglio 2020

Similitudine del coseno k-NN	k-Nearest Neighbor (k-NN) ora ti permette di cercare i "vicini più vicini" per similitudine del coseno oltre alla distanza euclidea. Questa funzionalità richiede il software del servizio R20200721 o versioni successive.	23 luglio 2020
Compressione gzip	Amazon OpenSearch Service ora supporta la compressione gzip per la maggior parte delle richieste e risposte HTTP, che può ridurre la latenza e conservare la larghezza di banda. Questa funzionalità richiede il software del servizio R20200721 o versioni successive.	23 luglio 2020
Supporto per Elasticsearch 7.7	Amazon OpenSearch Service ora supporta la versione 7.7 di Elasticsearch. Per ulteriori informazioni, consultare Note di rilascio 7.7.	23 luglio 2020
Servizio di mappa di Kibana	L'installazione predefinita di Kibana per Amazon OpenSearch Service ora include un server di mappe WMS, ad eccezione dei domini nelle regioni di India e Cina.	18 giugno 2020

Miglioramenti per SQL	Il supporto SQL per Amazon OpenSearch Service ora supporta molte nuove operazioni, un'interfaccia utente Kibana dedicata per l'esplorazione dei dati e una CLI interattiva. Per ulteriori informazioni, consulta .	3 giugno 2020
Funzionalità di ricerca tra cluster	Amazon OpenSearch Service ti consente di eseguire query e aggregazioni tra cluster su più domini connessi.	3 giugno 2020
Rilevamento di anomalie	Amazon OpenSearch Service ti consente di rilevare automaticamente le anomalie quasi in tempo reale.	3 giugno 2020
UltraWarm	UltraWarm lo storage per Amazon OpenSearch Service non è più disponibile in anteprima pubblica ed è ora disponibile a livello generale. La funzionalità ora supporta una gamma più ampia di versioni e Regioni AWS. Per ulteriori informazioni, consulta .	5 maggio 2020

Dizionari personalizzati	Amazon OpenSearch Service ti consente di caricare file di dizionario personalizzati da utilizzare con il tuo cluster. Questi file migliorano i risultati della ricerca dicendo a Elasticsearch di ignorare determinate parole ad alta frequenza o di trattare termini come equivalenti.	21 aprile 2020
Supporto per Elasticsearch 7.4	Amazon OpenSearch Service ora supporta la versione 7.4 di Elasticsearch. Per ulteriori informazioni, consultare Versioni supportate.	12 marzo 2020
k-NN	Amazon OpenSearch Service aggiunge il supporto per la ricerca K-Nearest Neighbor (k-NN). k-NN richiede il software di servizio R20200302 o successivo.	3 marzo 2020
Index State Management	Amazon OpenSearch Service aggiunge Index State Management (ISM), che consente di automatizzare le attività di routine, come l'eliminazione degli indici quando raggiungono una certa età. Questa funzionalità richiede il software del servizio R20200302 o versioni successive.	3 marzo 2020

Supporto per Elasticsearch 5.6.16	Amazon OpenSearch Service ora supporta l'ultima versione di patch per la versione 5.6, che aggiunge correzioni di bug e migliora la sicurezza . Amazon ES aggiornerà automaticamente i domini versione 5.6 esistenti a questa versione. Questa versione di Elasticsearch riporta erroneamente la versione come 5.6.17.	2 marzo 2020
Controllo granulare degli accessi	Amazon OpenSearch Service ora supporta il controllo granulare degli accessi, che offre sicurezza a livello di indice, documento e campo, la multi-tenancy Kibana e l'autenticazione di base HTTP opzionale per il cluster.	11 febbraio 2020
UltraWarm archiviazione (anteprima)	Amazon OpenSearch Service aggiunge UltraWarm un nuovo livello di storage caldo che utilizza Amazon S3 e una sofisticata soluzione di caching per migliorare le prestazio ni. Per gli indici su cui non si scrive attivamente e che vengono interrogati con minore frequenza, UltraWarm lo storage offre costi per GiB notevolmente inferiori.	3 dicembre 2019

Funzionalità di crittografia per le regioni Cina	La crittografia dei dati archiviati e node-to-node la crittografia sono ora disponibili nella regione `cn-north-1` Cina (Pechino) e nella regione `cn-northwest-1` Cina (Ningxia).	20 novembre 2019
Richiedi HTTPS	Adesso è possibile richiedere che tutto il traffico verso i domini Amazon ES arrivi tramite HTTPS. Durante la configurazione del dominio, seleziona la casella Require HTTPS (Richiedi HTTPS). Questa funzionalità richiede il software del servizio R20190808 o versioni successive.	3 ottobre 2019
Supporto per Elasticsearch 7.1 e 6.8	Amazon OpenSearch Service ora supporta le versioni 7.1 e 6.8 di Elasticsearch. Per ulteriori informazioni, consultare Versioni supportate.	13 agosto 2019
Snapshot orari	Invece di istantanee giornaliere, Amazon OpenSearch Service ora acquisisce istantanee orarie dei domini che eseguono Elasticsearch 5.3 e versioni successive, in modo da avere backup più frequenti da cui ripristinare i dati.	8 luglio 2019

Supporto per Elasticsearch 6.7	Amazon OpenSearch Service ora supporta la versione 6.7 di Elasticsearch. Per ulteriori informazioni, consultare Versioni supportate.	29 maggio 2019
Supporto per SQL	Amazon OpenSearch Service ora ti consente di interroga re i tuoi dati utilizzando SQL. Il supporto SQL richiede il software del servizio R20190418 o versioni successive.	15 maggio 2019
Tipi di istanza 5-series	Amazon OpenSearch Service ora supporta i tipi di istanze M5, C5 e R5. Rispetto ai tipi di istanze di vecchia generazio ne, questi nuovi tipi offrono prestazioni migliori a prezzi inferiori. Per ulteriori informazi oni, consulta Limiti.	24 aprile 2019
Supporto per Elasticsearch 6.5	Amazon OpenSearch Service ora supporta la versione 6.5 di Elasticsearch.	8 Aprile 2019
Avviso	Gli avvisi per Amazon OpenSearch Service ti avvisano quando i dati di uno o più indici Amazon ES soddisfano determinate condizioni. La funzionalità di avviso richiede il software del servizio R20190221 o versioni successive.	25 marzo 2019

Supporto per tre zone di disponibilità	Amazon OpenSearch Service ora supporta tre zone di disponibilità in molte regioni. Questa versione include anche un'esperienza della console ottimizzata. Questo multi-AZ richiede il software del servizio R20181023 o versioni successive.	7 febbraio 2019
Supporto per Elasticsearch 6.4	Amazon OpenSearch Service ora supporta la versione 6.4 di Elasticsearch.	23 gennaio 2019
Cluster di 200 nodi	Amazon ES ora consente di creare cluster con fino a 200 nodi di dati per un totale di 3 PB di archiviazione.	22 gennaio 2019
Aggiornamenti del software del servizio	Amazon ES ora consente di aggiornare manualmente il software di servizio per il dominio al fine di trarre vantaggio dalle nuove funzionalità più rapidamente o aggiornarlo in un momento con poco traffico. Per ulteriori informazioni, consultare.	20 novembre 2018
CloudWatch Nuove metriche	Amazon ES ora offre i parametri a livello di nodo e le nuove schede Integrità del cluster e Integrità dell'istanza nella console Amazon ES.	20 novembre 2018

Supporto per Cina (Pechino)	Amazon OpenSearch Service è ora disponibile nella regione cn-north-1, dove supporta i tipi di istanze M4, C4 e R4.	17 ottobre 2018
Nessuna crittografia ode-to-node	Amazon OpenSearch Service ora supporta node-to-node la crittografia, che mantiene i dati crittografati mentre Amazon ES li distribuisce in tutto il cluster.	18 settembre 2018
Aggiornamenti locali della versione	Amazon OpenSearch Service ora supporta gli upgrade di versione in loco.	14 agosto 2018
Supporto per Elasticsearch 6.3 e 5.6	Amazon OpenSearch Service ora supporta le versioni 6.3 e 5.6 di Elasticsearch.	14 agosto 2018
Log di errore	Amazon ES ora consente di pubblicare i log degli errori di Elasticsearch su Amazon. CloudWatch	31 luglio 2018
Istanze riservate della regione Cina (Ningxia)	Amazon ES ora offre istanze riservate nella regione Cina (Ningxia).	29 maggio 2018
Istanze riservate	Amazon ES ora offre il supporto per le istanze riservate.	7 maggio 2018

Aggiornamenti precedenti

Nella tabella seguente sono riportate le modifiche importanti apportate ad Amazon ES prima di maggio 2018.

Modifica	Descrizione	Data
Autenticazione di Amazon Cognito per Kibana	Amazon ES offre ora protezione della pagina di accesso per Kibana. Per ulteriori informazioni, consultare the section called “Autenticazione Amazon Cognito per dashboard OpenSearch ”.	2 aprile 2018
Supporto per Elasticsearch 6.2	Amazon OpenSearch Service ora supporta la versione 6.2 di Elasticsearch.	14 marzo 2018
Plug-in di analisi coreano	Amazon ES supporta ora una versione ottimizzata per la memoria del plug-in di analisi coreano Seunjeon.	13 marzo 2018
Aggiornamenti istantanei per il controllo degli accessi	Le modifiche apportate alle policy di controllo degli accessi nei domini Amazon ES ora hanno effetto immediatamente.	7 marzo 2018
Scala in petabyte	Amazon ES supporta ora i tipi di istanza I3 e dimension i di archiviazione totali del dominio fino a 1,5 PB. Per ulteriori informazioni, consultare the section called “Scala in petabyte”.	19 dicembre 2017
Crittografia dei dati a riposo	Amazon ES supporta ora la crittografia dei dati a riposo. Per ulteriori informazioni, consultare the section called “Crittografia a riposo”.	7 dicembre 2017
Supporto per Elasticsearch 6.0	Amazon ES ora supporta Elasticsearch versione 6.0. Per le considerazioni e le istruzioni relative alla migrazione, consulta the section called “Aggiornamento dei domini”.	6 dicembre 2017
Supporto per VPC	Amazon ES consente ora di avviare domini all'interno di Amazon Virtual Private Cloud. il supporto per VPC offre un ulteriore livello di sicurezza e semplifica le comunicaz ioni tra Amazon ES e altri servizi all'interno di un VPC. Per ulteriori informazioni, consultare the section called “Supporto per VPC”.	17 ottobre 2017

Modifica	Descrizione	Data
Pubblicazione di log di query lente	Amazon ES ora supporta la pubblicazione di slow log su Logs. CloudWatch Per ulteriori informazioni, consultare the section called “Monitoraggio dei log”.	16 ottobre 2017
Supporto per Elasticsearch 5.5	Amazon ES ora supporta Elasticsearch versione 5.5. Adesso è possibile ripristinare snapshot automatici senza contattare AWS Support e archiviare gli script tramite l'API `_scripts`.	7 settembre 2017
Supporto per Elasticsearch 5.3	Amazon ES ha aggiunto il supporto per Elasticsearch versione 5.3.	1 giugno 2017
Più istanze e capacità di EBS per ogni cluster	Amazon ES supporta ora fino a 100 nodi e 150 TB di capacità di EBS per ogni cluster.	5 Aprile 2017
Supporto per le regioni Canada (Centrale) e UE (Londra)	Amazon ES ha aggiunto il supporto per le seguenti regioni: Canada (Centrale), ca-central-1, ed Europa (Londra), eu-west-2.	20 marzo 2017
Più istanze e volumi EBS di dimensioni maggiori	Amazon ES ha aggiunto il supporto per più istanze e volumi EBS di dimensioni maggiori.	21 febbraio 2017
Supporto per Elasticsearch 5.1	Amazon ES ha aggiunto il supporto per Elasticsearch versione 5.1.	30 gennaio 2017
Supporto per il plug-in di analisi fonetica	Amazon ES fornisce ora l'integrazione predefinita con il plug-in di analisi fonetica, che permette di eseguire query basate sulla fonetica sui dati.	22 dicembre 2016
Supporto per la regione Stati Uniti orientali (Ohio)	Amazon ES ha aggiunto il supporto per la regione Stati Uniti orientali (Ohio), us-east-2.	17 ottobre 2016

Modifica	Descrizione	Data
Nuovo parametro per le prestazioni	Amazon ES ha aggiunto un parametro per le prestazioni, `ClusterUsedSpace` .	29 luglio 2016
Supporto per Elasticsearch 2.3	Amazon ES ha aggiunto il supporto per Elasticsearch versione 2.3.	27 luglio 2016
Supporto per la regione Asia Pacifico (Mumbai)	Amazon ES ha aggiunto il supporto per la seguente regione: Asia Pacifico (Mumbai), ap-south-1.	27 giugno 2016
Più istanze per cluster	Amazon ES ha aumentato il numero massimo di istanze (numero di istanze) per cluster da 10 a 20.	18 maggio 2016
Supporto per la regione Asia Pacifico (Seoul)	Amazon ES ha aggiunto il supporto per la seguente regione: Asia Pacifico (Seoul), ap-northeast-2.	28 gennaio 2016
Amazon ES	Versione iniziale.	1 Ottobre 2015

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.