Gestire i servizi della piattaforma S3

StorageGRID 11.9

NetApp
November 08, 2024

Sommario

Gestire i servizi della piattaforma S3

Servizi della piattaforma S3

Panoramica e considerazioni sui servizi di piattaforma

Prima di implementare i servizi della piattaforma, esaminare la panoramica e le considerazioni relative all'utilizzo di tali servizi.

Per informazioni su S3, vedere "UTILIZZARE L'API REST S3".

Panoramica dei servizi della piattaforma

I servizi della piattaforma StorageGRID possono aiutarti a implementare una strategia di cloud ibrido consentendo di inviare notifiche di eventi e copie di oggetti S3 e metadati di oggetti a destinazioni esterne.

Poiché la posizione di destinazione dei servizi della piattaforma è generalmente esterna all'implementazione di StorageGRID, i servizi della piattaforma offrono la potenza e la flessibilità derivanti dall'utilizzo di risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi per i dati.

È possibile configurare qualsiasi combinazione di servizi di piattaforma per un singolo bucket S3. Ad esempio, è possibile configurare sia il "Servizio CloudMirror" che "notifiche" in un bucket StorageGRID S3 in modo da poter mirrorare oggetti specifici ad Amazon Simple Storage Service (S3), inviando una notifica a un'applicazione di monitoring di terze parti per tenere traccia delle spese AWS.

> L'utilizzo dei servizi della piattaforma deve essere abilitato per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione del grid.

Modalità di configurazione dei servizi della piattaforma

I servizi della piattaforma comunicano con gli endpoint esterni configurati tramite "Manager tenant"o "API di gestione del tenant". Ogni endpoint rappresenta una destinazione esterna, come un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento di Amazon SNS o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

Dopo aver creato un endpoint esterno, è possibile attivare un servizio di piattaforma per un bucket aggiungendo la configurazione XML al bucket. La configurazione XML identifica gli oggetti su cui il bucket deve agire, l'azione che il bucket deve intraprendere e l'endpoint che il bucket deve utilizzare per il servizio.

È necessario aggiungere configurazioni XML separate per ogni servizio di piattaforma che si desidera configurare. Ad esempio:

- Se si desidera che tutti gli oggetti le cui chiavi iniziano con `/images` vengano replicati in un bucket Amazon S3, è necessario aggiungere una configurazione di replica al bucket di origine.
- Se si desidera anche inviare notifiche quando questi oggetti vengono memorizzati nel bucket, è necessario aggiungere una configurazione di notifica.
- Se si desidera indicizzare i metadati per questi oggetti, è necessario aggiungere la configurazione di notifica dei metadati utilizzata per implementare l'integrazione della ricerca.

Il formato per l'XML di configurazione è regolato dalle API REST S3 utilizzate per implementare i servizi della piattaforma StorageGRID:

Servizio di piattaforma	API REST S3	Fare riferimento a.
Replica di CloudMirror	• GetBucketReplication • PutBucketReplication	• "Replica di CloudMirror" • "Operazioni sui bucket"
Notifiche	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notifiche" • "Operazioni sui bucket"
Integrazione della ricerca	• OTTIENI la configurazione della notifica dei metadati del bucket • INSERIRE la configurazione della notifica dei metadati del bucket	• "Integrazione della ricerca" • "Operazioni personalizzate di StorageGRID"

Considerazioni sull'utilizzo dei servizi della piattaforma

Considerazione	Dettagli
Monitoraggio degli endpoint di destinazione	È necessario monitorare la disponibilità di ciascun endpoint di destinazione. Se la connettività all'endpoint di destinazione viene persa per un periodo di tempo prolungato ed esiste un grande backlog di richieste, le richieste client aggiuntive (come LE richieste PUT) a StorageGRID non avranno esito positivo. È necessario riprovare queste richieste non riuscite quando l'endpoint diventa raggiungibile.
Rallentamento dell'endpoint di destinazione	Il software StorageGRID potrebbe ridurre le richieste S3 in entrata per un bucket se la velocità con cui le richieste vengono inviate supera la velocità con cui l'endpoint di destinazione può ricevere le richieste. La limitazione si verifica solo quando è presente un backlog di richieste in attesa di essere inviate all'endpoint di destinazione. L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, le operazioni del client S3 (come LE richieste PUT) finiranno per fallire. È più probabile che le richieste CloudMirror siano influenzate dalle performance dell'endpoint di destinazione, perché queste richieste comportano in genere un maggior numero di trasferimenti di dati rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Considerazione	Dettagli
Garanzie di ordinazione	StorageGRID garantisce l'ordine delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni relative a un oggetto si trovano all'interno dello stesso sito, lo stato finale dell'oggetto (per la replica) sarà sempre uguale allo stato in StorageGRID. StorageGRID tenta al meglio di ordinare le richieste quando le operazioni vengono eseguite nei siti StorageGRID. Ad esempio, se si scrive inizialmente un oggetto nel sito A e successivamente si sovrascrive lo stesso oggetto nel sito B, l'oggetto finale replicato da CloudMirror nel bucket di destinazione non è garantito come l'oggetto più recente.
Eliminazioni di oggetti basate su ILM	Per far fronte al comportamento di eliminazione del CRR AWS e del servizio di notifica Amazon Simple, CloudMirror e le richieste di notifica degli eventi non vengono inviate quando un oggetto nel bucket di origine viene eliminato a causa delle regole ILM di StorageGRID. Ad esempio, se una regola ILM elimina un oggetto dopo 14 giorni, non viene inviata alcuna richiesta di notifica di CloudMirror o di evento. Al contrario, le richieste di integrazione della ricerca vengono inviate quando gli oggetti vengono eliminati a causa di ILM.
Utilizzo degli endpoint Kafka	Per gli endpoint Kafka, il TLS reciproco non è supportato. Di conseguenza, se si è `ssl.client.auth` impostato su `required` nella configurazione del broker Kafka, potrebbero verificarsi problemi di configurazione degli endpoint Kafka. L'autenticazione degli endpoint Kafka utilizza i seguenti tipi di autenticazione. Questi tipi sono diversi da quelli utilizzati per l'autenticazione di altri endpoint, come Amazon SNS, e richiedono credenziali per nome utente e password. • SASL/SEMPLICE • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Nota:** le impostazioni proxy di archiviazione configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Considerazioni sull'utilizzo del servizio di replica CloudMirror

Considerazione	Dettagli
Stato della replica	StorageGRID non supporta la `x-amz-replication-status` testata.

Considerazione	Dettagli
Dimensione dell'oggetto	La dimensione massima per gli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è 5 TIB, che corrisponde alla dimensione massima dell'oggetto *supportata*. **Nota**: La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.
Versioni e ID della versione del bucket	Se il bucket S3 di origine in StorageGRID ha attivato la versione, è necessario attivare anche la versione per il bucket di destinazione. Quando si utilizza la versione, tenere presente che l'ordinamento delle versioni degli oggetti nel bucket di destinazione è il massimo sforzo e non garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3. **Nota**: Gli ID della versione per il bucket di origine in StorageGRID non sono correlati agli ID della versione per il bucket di destinazione.
Tagging per le versioni degli oggetti	Il servizio CloudMirror non replica le richieste PutObjectTagging o DeleteObjectTagging che forniscono un ID di versione, a causa delle limitazioni del protocollo S3. Poiché gli ID di versione per l'origine e la destinazione non sono correlati, non esiste alcun modo per garantire che venga replicato un aggiornamento del tag a un ID di versione specifico. Al contrario, il servizio CloudMirror replica le richieste PutObjectTagging o DeleteObjectTagging che non specificano un ID di versione. Queste richieste aggiornano i tag per la chiave più recente (o la versione più recente se il bucket è in versione). Vengono replicati anche i normali ingest con tag (senza tagging degli aggiornamenti).
Caricamenti e valori multiparte `ETag`	Quando si esegue il mirroring degli oggetti caricati utilizzando un caricamento multiparte, il servizio CloudMirror non conserva le parti. Di conseguenza, il `ETag` valore per l'oggetto speculare sarà diverso dal `ETag` valore dell'oggetto originale.
Oggetti crittografati con SSE-C (crittografia lato server con chiavi fornite dal cliente)	Il servizio CloudMirror non supporta oggetti crittografati con SSE-C. se si tenta di acquisire un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione non riesce.
Bucket con blocco oggetti S3 attivato	La replica non è supportata per i bucket di origine o di destinazione con blocco oggetti S3 attivato.

Comprendere il servizio di replica CloudMirror

È possibile abilitare la replica CloudMirror per un bucket S3 se si desidera che StorageGRID replichi oggetti specificati aggiunti al bucket in uno o più bucket di destinazione esterni.

Ad esempio, è possibile utilizzare la replica di CloudMirror per eseguire il mirroring di record specifici dei clienti

in Amazon S3 e sfruttare i servizi AWS per eseguire analisi dei dati.

> La replica di CloudMirror non è supportata se il bucket di origine ha attivato il blocco oggetti S3.

CloudMirror e ILM

La replica CloudMirror funziona indipendentemente dalle policy ILM attive del grid. Il servizio CloudMirror replica gli oggetti memorizzati nel bucket di origine e li consegna al bucket di destinazione il prima possibile. La consegna degli oggetti replicati viene attivata quando l'acquisizione degli oggetti ha esito positivo.

CloudMirror e replica cross-grid

La replica di CloudMirror presenta importanti analogie e differenze con la funzionalità di replica cross-grid. Fare riferimento alla "Confronta la replica cross-grid e la replica CloudMirror".

Bucket Cloud Mirror e S3

La replica di CloudMirror è generalmente configurata per utilizzare un bucket S3 esterno come destinazione. Tuttavia, è anche possibile configurare la replica in modo che utilizzi un'altra implementazione StorageGRID o qualsiasi servizio compatibile con S3.

Bucket esistenti

Quando si attiva la replica CloudMirror per un bucket esistente, vengono replicati solo i nuovi oggetti aggiunti a tale bucket. Gli oggetti esistenti nel bucket non vengono replicati. Per forzare la replica degli oggetti esistenti, è possibile aggiornare i metadati dell'oggetto esistente eseguendo una copia dell'oggetto.

> Se si utilizza la replica CloudMirror per copiare oggetti in una destinazione Amazon S3, tenere presente che Amazon S3 limita la dimensione dei metadati definiti dall'utente all'interno di ogni intestazione della richiesta PUT a 2 KB. Se un oggetto ha metadati definiti dall'utente superiori a 2 KB, tale oggetto non verrà replicato.

Bucket multipli di destinazione

Per replicare gli oggetti in un singolo bucket in più bucket di destinazione, specificare la destinazione per ogni regola nell'XML di configurazione della replica. Non è possibile replicare un oggetto in più bucket contemporaneamente.

Benne in versione o non in versione

È possibile configurare la replica di CloudMirror nei bucket con versione o senza versione. I bucket di destinazione possono essere aggiornati o non aggiornati. È possibile utilizzare qualsiasi combinazione di bucket con versione e senza versione. Ad esempio, è possibile specificare un bucket con versione come destinazione per un bucket di origine senza versione o viceversa. È inoltre possibile eseguire la replica tra bucket senza versione.

Eliminazione, loop di replica ed eventi

Comportamento di eliminazione

È uguale al comportamento di eliminazione del servizio Amazon S3, Cross-Region Replication (CRR). L'eliminazione di un oggetto in un bucket di origine non elimina mai un oggetto replicato nella destinazione. Se sia il bucket di origine che quello di destinazione sono entrambi con versione, il marker di eliminazione viene replicato. Se il bucket di destinazione non è dotato di versione, l'eliminazione di un oggetto nel bucket di origine non replica il contrassegno di eliminazione nel bucket di destinazione o elimina l'oggetto di destinazione.

Protezione dai loop di replica

Quando gli oggetti vengono replicati nel bucket di destinazione, StorageGRID li contrassegna come "repliche". Un bucket StorageGRID di destinazione non replicerà gli oggetti contrassegnati come repliche, proteggendoti da loop di replica accidentali. Questo contrassegno di replica è interno a StorageGRID e non ti impedisce di sfruttare il CRR AWS quando utilizzi un bucket Amazon S3 come destinazione.

> L'intestazione personalizzata utilizzata per contrassegnare una replica è `x-ntap-sg-replica`. Questo contrassegno impedisce un mirror a cascata. StorageGRID supporta un CloudMirror bidirezionale tra due griglie.

Eventi nel bucket di destinazione

L'unicità e l'ordinamento degli eventi nel bucket di destinazione non sono garantiti. Più di una copia identica di un oggetto di origine potrebbe essere consegnata alla destinazione in seguito alle operazioni eseguite per garantire il successo della consegna. In rari casi, quando lo stesso oggetto viene aggiornato simultaneamente da due o più siti StorageGRID diversi, l'ordine delle operazioni sul bucket di destinazione potrebbe non corrispondere all'ordine degli eventi sul bucket di origine.

Comprendere le notifiche per i bucket

È possibile attivare la notifica degli eventi per un bucket S3 se si desidera che StorageGRID invii notifiche relative agli eventi specificati a un cluster Kafka di destinazione o a un servizio di notifica Amazon Simple.

Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.

Le notifiche degli eventi vengono create nel bucket di origine come specificato nella configurazione della notifica e vengono inviate alla destinazione. Se un evento associato a un oggetto ha esito positivo, viene creata una notifica relativa a tale evento e messa in coda per il recapito.

L'unicità e l'ordine delle notifiche non sono garantiti. È possibile che più di una notifica di un evento venga inviata alla destinazione a seguito delle operazioni eseguite per garantire il successo della consegna. Inoltre, poiché la consegna è asincrona, non è garantito che l'ordine temporale delle notifiche alla destinazione corrisponda all'ordine degli eventi nel bucket di origine, in particolare per le operazioni provenienti da diversi siti StorageGRID. È possibile utilizzare il `sequencer` tasto nel messaggio dell'evento per determinare l'ordine degli eventi per un particolare oggetto, come descritto nella documentazione di Amazon S3.

Le notifiche degli eventi StorageGRID seguono l'API Amazon S3 con alcune limitazioni.

- Sono supportati i seguenti tipi di evento:
  - S3:ObjectCreated:
  - s3:ObjectCreated:put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copy
  - s3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved:
  - s3:ObjectRemoved:Elimina
  - s3:ObjectRemoved:DeleteMarkerCreated

    - s3:ObjectRestore:Post
- Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ma non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nella tabella:

Nome della chiave	Valore StorageGRID
EventSource	`sgws:s3`
AwsRegion	*non incluso*
x-amz-id-2	*non incluso*
arn	`urn:sgws:s3:::bucket_name`

Comprendere il servizio di integrazione della ricerca

È possibile attivare l'integrazione della ricerca per un bucket S3 se si desidera utilizzare un servizio di ricerca e analisi dei dati esterno per i metadati degli oggetti.

Il servizio di integrazione della ricerca è un servizio StorageGRID personalizzato che invia in modo automatico e asincrono i metadati degli oggetti S3 a un endpoint di destinazione ogni volta che un oggetto viene creato o eliminato o quando i relativi metadati o tag vengono aggiornati. Potrai quindi utilizzare sofisticati strumenti di ricerca, analisi dei dati, visualizzazione o apprendimento automatico forniti dal servizio di destinazione per cercare, analizzare e ottenere informazioni dai dati degli oggetti.

Ad esempio, è possibile configurare i bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. È quindi possibile utilizzare Elasticsearch per eseguire ricerche tra bucket ed eseguire analisi sofisticate dei modelli presenti nei metadati degli oggetti.

Sebbene l'integrazione di Elasticsearch possa essere configurata in un bucket con blocco oggetto S3 abilitato, i metadati S3 Object Lock (incluso lo stato Retain until Date e Legal Hold) degli oggetti non verranno inclusi nei metadati inviati a Elasticsearch.

> Poiché il servizio di integrazione della ricerca fa sì che i metadati degli oggetti vengano inviati a una destinazione, il relativo XML di configurazione viene definito "*metadata* Notification Configuration XML". Questo XML di configurazione è diverso dal "XML di configurazione delle notifiche" utilizzato per attivare le notifiche *event*.

Integrazione di ricerca e bucket S3

È possibile attivare il servizio di integrazione della ricerca per qualsiasi bucket con versione o senza versione. L'integrazione della ricerca viene configurata associando XML di configurazione della notifica dei metadati al bucket che specifica gli oggetti su cui agire e la destinazione dei metadati dell'oggetto.

Le notifiche dei metadati vengono generate sotto forma di un documento JSON denominato con il nome del bucket, il nome dell'oggetto e l'ID versione, se presente. Ogni notifica di metadati contiene un set standard di metadati di sistema per l'oggetto, oltre a tutti i tag dell'oggetto e ai metadati dell'utente.

Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Cerca notifiche

Le notifiche sui metadati vengono generate e messe in coda per essere inviate quando:

- Viene creato un oggetto.
- Un oggetto viene eliminato, anche quando gli oggetti vengono eliminati in seguito all'operazione della policy ILM della griglia.
- I tag o i metadati degli oggetti vengono aggiunti, aggiornati o cancellati. L'insieme completo di metadati e tag viene sempre inviato in seguito all'aggiornamento, non solo i valori modificati.

Dopo aver aggiunto XML per la configurazione delle notifiche dei metadati a un bucket, vengono inviate notifiche per i nuovi oggetti creati e per gli oggetti modificati aggiornando i dati, i metadati dell'utente o i tag. Tuttavia, non vengono inviate notifiche per oggetti già presenti nel bucket. Per garantire che i metadati degli oggetti per tutti gli oggetti nel bucket vengano inviati alla destinazione, eseguire una delle seguenti operazioni:

- Configurare il servizio di integrazione della ricerca subito dopo la creazione del bucket e prima di aggiungere oggetti.
- Eseguire un'azione su tutti gli oggetti già presenti nel bucket che attiverà l'invio di un messaggio di notifica dei metadati alla destinazione.

Servizio di integrazione della ricerca ed Elasticsearch

Il servizio di integrazione della ricerca di StorageGRID supporta un cluster Elasticsearch come destinazione. Come per gli altri servizi della piattaforma, la destinazione viene specificata nell'endpoint il cui URN viene utilizzato nel XML di configurazione per il servizio. Utilizzare "Tool di matrice di interoperabilità NetApp" per determinare le versioni supportate di Elasticsearch.

Gestire gli endpoint dei servizi della piattaforma

Configurare gli endpoint dei servizi della piattaforma

Prima di poter configurare un servizio di piattaforma per un bucket, è necessario configurare almeno un endpoint in modo che sia la destinazione del servizio di piattaforma.

L'accesso ai servizi della piattaforma viene attivato per tenant da un amministratore di StorageGRID. Per creare o utilizzare un endpoint di servizi di piattaforma, è necessario essere un utente tenant con autorizzazione di accesso Gestisci endpoint o root, in una griglia la cui rete è stata configurata per consentire ai nodi di storage di accedere alle risorse esterne degli endpoint. Per un singolo tenant, è possibile configurare un massimo di 500 endpoint di servizi della piattaforma. Per ulteriori informazioni, contattare l'amministratore di StorageGRID.

Che cos'è un endpoint di servizi di piattaforma?

Un endpoint dei servizi di piattaforma specifica le informazioni necessarie a StorageGRID per accedere alla destinazione esterna.

Ad esempio, se si desidera replicare gli oggetti da un bucket StorageGRID a un bucket Amazon S3, si crea un endpoint dei servizi della piattaforma che include le informazioni e le credenziali necessarie a StorageGRID per accedere al bucket di destinazione su Amazon.

Ogni tipo di servizio di piattaforma richiede un proprio endpoint, pertanto è necessario configurare almeno un endpoint per ogni servizio di piattaforma che si intende utilizzare. Dopo aver definito un endpoint di servizi di piattaforma, si utilizza l'URN dell'endpoint come destinazione nel XML di configurazione utilizzato per attivare il servizio.

È possibile utilizzare lo stesso endpoint della destinazione per più bucket di origine. Ad esempio, è possibile configurare diversi bucket di origine per inviare metadati di oggetto allo stesso endpoint di integrazione della ricerca, in modo da poter eseguire ricerche in più bucket. È inoltre possibile configurare un bucket di origine per utilizzare più endpoint come destinazione, che consente di eseguire operazioni quali l'invio di notifiche sulla creazione di oggetti a un argomento Amazon Simple Notification Service (Amazon SNS) e notifiche sull'eliminazione di oggetti a un secondo argomento Amazon SNS.

Endpoint per la replica di CloudMirror

StorageGRID supporta endpoint di replica che rappresentano i bucket S3. Questi bucket potrebbero essere ospitati su Amazon Web Services, sullo stesso o in un'implementazione remota di StorageGRID o su un altro servizio.

Endpoint per le notifiche

StorageGRID supporta gli endpoint Amazon SNS e Kafka. Gli endpoint SQS (Simple Queue Service) o AWS Lambda non sono supportati.

Per gli endpoint Kafka, il TLS reciproco non è supportato. Di conseguenza, se si è `ssl.client.auth` impostato su `required` nella configurazione del broker Kafka, potrebbero verificarsi problemi di configurazione degli endpoint Kafka.

Endpoint per il servizio di integrazione della ricerca

StorageGRID supporta endpoint di integrazione della ricerca che rappresentano cluster Elasticsearch. Questi cluster di Elasticsearch possono trovarsi in un data center locale o in un cloud AWS o altrove.

L'endpoint di integrazione della ricerca si riferisce a un tipo e un indice Elasticsearch specifici. È necessario creare l'indice in Elasticsearch prima di creare l'endpoint in StorageGRID, altrimenti la creazione dell'endpoint non avrà esito positivo. Non è necessario creare il tipo prima di creare l'endpoint. StorageGRID crea il tipo, se necessario, quando invia i metadati dell'oggetto all'endpoint.

Informazioni correlate

"Amministrare StorageGRID"

Specificare URN per l'endpoint dei servizi della piattaforma

Quando si crea un endpoint dei servizi della piattaforma, è necessario specificare un nome di risorsa (URN) univoco. Verrà utilizzato l'URN per fare riferimento all'endpoint quando si crea un XML di configurazione per il servizio di piattaforma. L'URN per ciascun

endpoint deve essere univoco.

StorageGRID convalida gli endpoint dei servizi della piattaforma durante la loro creazione. Prima di creare un endpoint di servizi di piattaforma, verificare che la risorsa specificata nell'endpoint esista e che sia possibile raggiungerla.

Elementi DI URNA

L'URN per un endpoint dei servizi di piattaforma deve iniziare con `arn:aws` o `urn:mysite`, come segue:

- Se il servizio è ospitato su Amazon Web Services (AWS), utilizzare `arn:aws`
- Se il servizio è ospitato su Google Cloud Platform (GCP), utilizza `arn:aws`
- Se il servizio è ospitato localmente, utilizzare `urn:mysite`

Ad esempio, se si specifica l'URN per un endpoint CloudMirror ospitato su StorageGRID, l'URN potrebbe iniziare con `urn:sgws`.

L'elemento successivo dell'URN specifica il tipo di servizio della piattaforma, come segue:

Servizio	Tipo
Replica di CloudMirror	`s3`
Notifiche	`sns` o. `kafka`
Integrazione della ricerca	`es`

Ad esempio, per continuare a specificare l'URN per un endpoint CloudMirror ospitato su StorageGRID, aggiungere `s3` a get `urn:sgws:s3`.

L'elemento finale dell'URN identifica la risorsa di destinazione specifica nell'URI di destinazione.

Servizio	Risorsa specifica
Replica di CloudMirror	`bucket-name`
Notifiche	`sns-topic-name` o. `kafka-topic-name`
Integrazione della ricerca	`domain-name/index-name/type-name` **Nota:** se il cluster Elasticsearch è **non** configurato per creare gli indici automaticamente, è necessario creare l'indice manualmente prima di creare l'endpoint.

Urns per i servizi ospitati su AWS e GCP

Per le entità AWS e GCP, l'URN completo è un ARN AWS valido. Ad esempio:

- Replica di CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notifiche:

```
arn:aws:sns:region:account-id:topic-name
```

- Integrazione della ricerca:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> Per un endpoint di integrazione della ricerca AWS, `domain-name` deve includere la stringa letterale `domain/` , come mostrato qui.

Urns per servizi in hosting locale

Quando si utilizzano servizi ospitati in locale invece di servizi cloud, è possibile specificare l'URN in qualsiasi modo che crei un URN valido e univoco, purché l'URN includa gli elementi richiesti nella terza e ultima posizione. È possibile lasciare vuoti gli elementi indicati da opzionale oppure specificarli in qualsiasi modo che consenta di identificare la risorsa e rendere l'URN unico. Ad esempio:

- Replica di CloudMirror:

```
urn:mysite:s3:optional:optional:bucket-name
```

  Per un endpoint CloudMirror ospitato su StorageGRID, è possibile specificare un URN valido che inizia con `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notifiche:

  Specificare un endpoint di Amazon Simple Notification Service:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

  Specificare un endpoint Kafka:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- Integrazione della ricerca:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

> Per gli endpoint di integrazione della ricerca ospitati localmente, l'elemento può essere qualsiasi stringa, `domain-name` purché l'URN dell'endpoint sia univoco.

Creare endpoint di servizi di piattaforma

È necessario creare almeno un endpoint del tipo corretto prima di poter attivare un servizio di piattaforma.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire gli endpoint o l'autorizzazione di accesso root".
- La risorsa a cui fa riferimento l'endpoint dei servizi della piattaforma è stata creata:
  - Replica di CloudMirror: Bucket S3
  - Notifica dell'evento: Argomento Kafka o Amazon Simple Notification Service (Amazon SNS)
  - Notifica di ricerca: Indice Elasticsearch, se il cluster di destinazione non è configurato per creare automaticamente gli indici.
- Si dispone delle informazioni relative alla risorsa di destinazione:
  - Host e porta per l'Uniform Resource Identifier (URI)

    > Se si prevede di utilizzare un bucket ospitato su un sistema StorageGRID come endpoint per la replica di CloudMirror, contattare l'amministratore del grid per determinare i valori da inserire.

  - Nome risorsa univoco (URN)

    "Specificare URN per l'endpoint dei servizi della piattaforma"

  - Credenziali di autenticazione (se richieste):

Endpoint di integrazione della ricerca

Per gli endpoint di integrazione della ricerca, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key
- HTTP di base: Nome utente e password

Endpoint di replica CloudMirror

Per gli endpoint di replica di CloudMirror, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key
- CAP (C2S Access Portal): URL con credenziali temporanee, certificati server e client, chiavi client e passphrase opzionale con chiave privata del client.

Endpoint Amazon SNS

Per gli endpoint Amazon SNS, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key

Endpoint Kafka

Per gli endpoint Kafka, è possibile utilizzare le seguenti credenziali:

- SASL/PLAIN: Nome utente e password
- SASL/SCRAM-SHA-256: Nome utente e password
- SASL/SCRAM-SHA-512: Nome utente e password

  - Certificato di protezione (se si utilizza un certificato CA personalizzato)

- Se le funzioni di protezione di Elasticsearch sono attivate, si dispone del privilegio del cluster di monitoraggio per il test di connettività e del privilegio di scrittura dell'indice o di entrambi i privilegi di indice e di eliminazione per gli aggiornamenti dei documenti.

Fasi

1. Selezionare **STORAGE (S3)** > **Platform Services Endpoint**. Viene visualizzata la pagina Platform Services Endpoint.
2. Selezionare **Crea endpoint**.
3. Inserire un nome visualizzato per descrivere brevemente l'endpoint e il suo scopo.

   Il tipo di servizio della piattaforma supportato dall'endpoint viene visualizzato accanto al nome dell'endpoint quando viene elencato nella pagina degli endpoint, quindi non è necessario includere tali informazioni nel nome.

4. Nel campo **URI**, specificare l'URI (Unique Resource Identifier) dell'endpoint.

   Utilizzare uno dei seguenti formati:

```
https://host:port
http://host:port
```

Se non si specifica una porta, vengono utilizzate le seguenti porte predefinite:

- Porta 443 per URI HTTPS e porta 80 per URI HTTP (la maggior parte degli endpoint)
- Porta 9092 per URI HTTPS e HTTP (solo endpoint Kafka)

Ad esempio, l'URI per un bucket ospitato su StorageGRID potrebbe essere:

```
https://s3.example.com:10443
```

In questo esempio, `s3.example.com` rappresenta la voce DNS per l'IP virtuale (VIP) del gruppo ha (StorageGRID High Availability) e `10443` rappresenta la porta definita nell'endpoint del bilanciamento del carico.

> Quando possibile, è necessario connettersi a un gruppo ha di nodi per il bilanciamento del carico per evitare un singolo punto di errore.

Analogamente, l'URI per un bucket ospitato su AWS potrebbe essere:

```
https://s3-aws-region.amazonaws.com
```

> Se l'endpoint viene utilizzato per il servizio di replica CloudMirror, non includere il nome del bucket nell'URI. Il nome del bucket viene incluso nel campo **URN**.

5. Immettere il nome di risorsa (URN) univoco per l'endpoint.

> Non è possibile modificare l'URN di un endpoint dopo la creazione dell'endpoint.

6. Selezionare **continua**.
7. Selezionare un valore per **tipo di autenticazione**.

Endpoint di integrazione della ricerca

Immettere o caricare le credenziali per un endpoint di integrazione della ricerca.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta
HTTP di base	Utilizza un nome utente e una password per autenticare le connessioni alla destinazione.	• Nome utente • Password

Endpoint di replica CloudMirror

Immettere o caricare le credenziali per un endpoint di replica CloudMirror.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta
CAP (portale di accesso C2S)	Utilizza certificati e chiavi per autenticare le connessioni alla destinazione.	• URL temporaneo delle credenziali • Certificato CA del server (caricamento file PEM) • Certificato client (caricamento file PEM) • Chiave privata del client (caricamento file PEM, formato crittografato OpenSSL o formato chiave privata non crittografato) • Passphrase della chiave privata del client (opzionale)

Endpoint Amazon SNS

Immettere o caricare le credenziali per un endpoint Amazon SNS.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta

Endpoint Kafka

Immettere o caricare le credenziali per un endpoint Kafka.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
SASL/SEMPLICE	Utilizza un nome utente e una password con testo normale per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-256	Utilizza un nome utente e una password utilizzando un protocollo di risposta alla verifica e l'hash SHA-256 per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-512	Utilizza un nome utente e una password utilizzando un protocollo di risposta alla verifica e l'hash SHA-512 per autenticare le connessioni alla destinazione.	• Nome utente • Password

Selezionare **Usa autenticazione con delega** se il nome utente e la password sono derivati da un token di delega ottenuto da un cluster Kafka.

8. Selezionare **continua**.

9. Selezionare un pulsante di opzione per **verify server** (verifica server) per scegliere la modalità di verifica della connessione TLS all'endpoint.

Tipo di verifica del certificato	Descrizione
USA certificato CA personalizzato	Utilizzare un certificato di protezione personalizzato. Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo **certificato CA**.
Utilizzare il certificato CA del sistema operativo	Utilizzare il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato. Questa opzione non è sicura.

10. Selezionare **Test e creare endpoint**.
    - Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene convalidata da un nodo in ogni sito.
    - Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Se è necessario modificare l'endpoint per correggere l'errore, selezionare **Torna ai dettagli dell'endpoint** e aggiornare le informazioni. Quindi, selezionare **Test e creare endpoint**.

> La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant. Contattare l'amministratore di StorageGRID.

Dopo aver configurato un endpoint, è possibile utilizzare il relativo URN per configurare un servizio di piattaforma.

Informazioni correlate

- "Specificare URN per l'endpoint dei servizi della piattaforma"
- "Configurare la replica di CloudMirror"
- "Configurare le notifiche degli eventi"
- "Configurare il servizio di integrazione della ricerca"

Verifica della connessione per l'endpoint dei servizi della piattaforma

Se la connessione a un servizio della piattaforma è stata modificata, è possibile verificare la connessione per l'endpoint per verificare l'esistenza della risorsa di destinazione e che sia possibile raggiungerla utilizzando le credenziali specificate.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire gli endpoint o l'autorizzazione di accesso root".

A proposito di questa attività

StorageGRID non convalida che le credenziali dispongano delle autorizzazioni corrette.

Fasi

1. Selezionare **STORAGE (S3)** > **Platform Services Endpoint**.

   Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.

2. Selezionare l'endpoint di cui si desidera verificare la connessione.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Test di connessione**.
   - Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene convalidata da un nodo in ogni sito.
   - Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Se è necessario modificare l'endpoint per correggere l'errore, selezionare **Configuration** (Configurazione) e aggiornare le informazioni. Quindi, selezionare **Test e salvare le modifiche**.

Modifica dell'endpoint dei servizi della piattaforma

È possibile modificare la configurazione di un endpoint di servizi di piattaforma per modificarne il nome, l'URI o altri dettagli. Ad esempio, potrebbe essere necessario aggiornare le credenziali scadute o modificare l'URI in modo che punti a un indice Elasticsearch di backup per il failover. Non è possibile modificare l'URN per un endpoint di servizi di piattaforma.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire gli endpoint o l'autorizzazione di accesso root".

Fasi

1. Selezionare **STORAGE (S3)** > **Platform Services Endpoint**.

   Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.

2. Selezionare l'endpoint che si desidera modificare.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Configurazione**.
4. Se necessario, modificare la configurazione dell'endpoint.

   Non è possibile modificare l'URN di un endpoint dopo la creazione dell'endpoint.

   a. Per modificare il nome di visualizzazione per l'endpoint, selezionare l'icona di modifica .
   b. Se necessario, modificare l'URI.
   c. Se necessario, modificare il tipo di autenticazione.
      - Per l'autenticazione della chiave di accesso, modificare la chiave in base alle necessità

selezionando **Modifica chiave S3** e incollando un nuovo ID della chiave di accesso e una chiave di accesso segreta. Se si desidera annullare le modifiche, selezionare **Ripristina modifica tasto S3**.

- Per l'autenticazione CAP (C2S Access Portal), modificare l'URL delle credenziali temporanee o la passphrase della chiave privata del client opzionale e caricare nuovi file di certificato e chiavi in base alle necessità.

> La chiave privata del client deve essere in formato crittografato OpenSSL o non crittografato.

d. Se necessario, modificare il metodo di verifica del server.

5. Selezionare **Test e salvare le modifiche**.
   - Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene verificata da un nodo in ogni sito.
   - Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Modificare l'endpoint per correggere l'errore, quindi selezionare **Test e salvare le modifiche**.

Eliminare l'endpoint dei servizi della piattaforma

È possibile eliminare un endpoint se non si desidera più utilizzare il servizio di piattaforma associato.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire gli endpoint o l'autorizzazione di accesso root".

Fasi

1. Selezionare **STORAGE (S3)** > **Platform Services Endpoint**.

   Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.

2. Selezionare la casella di controllo per ciascun endpoint che si desidera eliminare.

> Se elimini un endpoint di servizi di piattaforma in uso, il servizio di piattaforma associato verrà disattivato per tutti i bucket che utilizzano l'endpoint. Tutte le richieste non ancora completate verranno interrotte. Le nuove richieste continueranno a essere generate fino a quando non si modifica la configurazione del bucket per non fare più riferimento all'URN cancellato. StorageGRID segnalerà queste richieste come errori irrecuperabili.

3. Selezionare **azioni** > **Elimina endpoint**.

   Viene visualizzato un messaggio di conferma.

4. Selezionare **Delete endpoint** (Elimina endpoint).

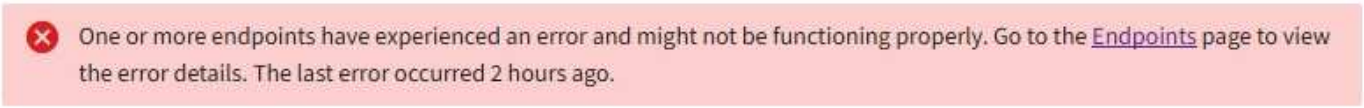
Risolvere gli errori degli endpoint dei servizi della piattaforma

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi della piattaforma, viene visualizzato un messaggio sul dashboard. Nella pagina

Platform Services Endpoint, la colonna Last error (ultimo errore) indica per quanto tempo si è verificato l'errore. Se le autorizzazioni associate alle credenziali di un endpoint non sono corrette, non viene visualizzato alcun errore.

Determinare se si è verificato un errore

Se si sono verificati errori degli endpoint dei servizi della piattaforma negli ultimi 7 giorni, la dashboard di Tenant Manager visualizza un messaggio di avviso. Per ulteriori informazioni sull'errore, visitare la pagina relativa agli endpoint dei servizi della piattaforma.



Lo stesso errore visualizzato nella dashboard viene visualizzato anche nella parte superiore della pagina Platform Services Endpoint. Per visualizzare un messaggio di errore più dettagliato:

Fasi

1. Dall'elenco degli endpoint, selezionare l'endpoint che presenta l'errore.
2. Nella pagina dei dettagli dell'endpoint, selezionare **connessione**. Questa scheda visualizza solo l'errore più recente per un endpoint e indica quanto tempo fa si è verificato l'errore. Negli ultimi 7 giorni si sono verificati errori che includono l'icona X rossa .

Controllare se l'errore è ancora aggiornato

Alcuni errori potrebbero continuare a essere visualizzati nella colonna **ultimo errore** anche dopo la risoluzione. Per verificare se un errore è corrente o per forzare la rimozione di un errore risolto dalla tabella:

Fasi

1. Selezionare l'endpoint.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Selezionare **connessione** > **verifica connessione**.

Selezionando **verifica connessione**, StorageGRID convalida l'esistenza dell'endpoint dei servizi della piattaforma e può essere raggiunto con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Risolvi gli errori degli endpoint

È possibile utilizzare il messaggio **Last error** (ultimo errore) nella pagina dei dettagli dell'endpoint per determinare la causa dell'errore. Alcuni errori potrebbero richiedere la modifica dell'endpoint per risolvere il problema. Ad esempio, se StorageGRID non riesce ad accedere al bucket S3 di destinazione perché non dispone delle autorizzazioni di accesso corrette o la chiave di accesso è scaduta, può verificarsi un errore di CloudMirroring. Il messaggio è "è necessario aggiornare le credenziali dell'endpoint o l'accesso alla destinazione" e i dettagli sono "AccessDenied" o "InvalidAccessKeyId".

Se è necessario modificare l'endpoint per risolvere un errore, selezionando **verifica e salva modifiche** StorageGRID convalida l'endpoint aggiornato e conferma che è possibile raggiungerlo con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Fasi

1. Selezionare l'endpoint.
2. Nella pagina dei dettagli dell'endpoint, selezionare **Configurazione**.
3. Modificare la configurazione dell'endpoint in base alle necessità.
4. Selezionare **connessione** > **verifica connessione**.

Credenziali endpoint con autorizzazioni insufficienti

Quando StorageGRID convalida un endpoint di servizi di piattaforma, conferma che le credenziali dell'endpoint possono essere utilizzate per contattare la risorsa di destinazione ed esegue un controllo delle autorizzazioni di base. Tuttavia, StorageGRID non convalida tutte le autorizzazioni richieste per determinate operazioni di servizi della piattaforma. Per questo motivo, se si riceve un errore quando si tenta di utilizzare un servizio di piattaforma (ad esempio "403 Proibito"), controllare le autorizzazioni associate alle credenziali dell'endpoint.

Informazioni correlate

- **Amministrare StorageGRID › risolvere i problemi relativi ai servizi della piattaforma**
- "Creare endpoint di servizi di piattaforma"
- "Verifica della connessione per l'endpoint dei servizi della piattaforma"
- "Modifica dell'endpoint dei servizi della piattaforma"

Configurare la replica di CloudMirror

Per attivare la replica CloudMirror per un bucket, è necessario creare e applicare un XML di configurazione di replica bucket valido.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- È già stato creato un bucket per fungere da origine della replica.
- L'endpoint che si intende utilizzare come destinazione per la replica CloudMirror esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

La replica di CloudMirror copia gli oggetti da un bucket di origine a un bucket di destinazione specificato in un endpoint.

Per informazioni generali sulla replica bucket e su come configurarla, vedere "Documentazione di Amazon Simple Storage Service (S3): Replica di oggetti". Per informazioni sull'implementazione di GetBucketReplication, DeleteBucketReplication e PutBucketReplication da parte di StorageGRID, vedere "Operazioni sui bucket".

> La replica di CloudMirror presenta importanti analogie e differenze con la funzionalità di replica cross-grid. Per ulteriori informazioni, vedere "Confronta la replica cross-grid e la replica CloudMirror".

Durante la configurazione della replica di CloudMirror, osservare i seguenti requisiti e caratteristiche:

- Quando si crea e si applica un XML di configurazione di replica bucket valido, è necessario utilizzare l'URN di un endpoint bucket S3 per ogni destinazione.
- La replica non è supportata per i bucket di origine o di destinazione con blocco oggetti S3 attivato.
- Se si attiva la replica CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket vengono replicati, ma gli oggetti esistenti nel bucket non vengono replicati. È necessario aggiornare gli oggetti esistenti per attivare la replica.
- Se si specifica una classe di storage nell'XML di configurazione della replica, StorageGRID utilizza tale classe quando esegue operazioni sull'endpoint S3 di destinazione. L'endpoint di destinazione deve supportare anche la classe di storage specificata. Assicurarsi di seguire le raccomandazioni fornite dal vendor del sistema di destinazione.

Fasi

1. Abilita la replica per il bucket di origine:
   - Utilizzare un editor di testo per creare l'XML di configurazione della replica richiesto per attivare la replica, come specificato nell'API di replica S3.
   - Durante la configurazione dell'XML:
     - Tenere presente che StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo dell' `Filter`elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, consultare la documentazione di Amazon sulla configurazione della replica.
     - Utilizzare l'URN di un endpoint del bucket S3 come destinazione.
     - Se lo si desidera, aggiungere l' `<StorageClass>`elemento e specificare una delle seguenti opzioni:
       - `STANDARD`: La classe di archiviazione predefinita. Se non si specifica una classe di archiviazione quando si carica un oggetto, viene utilizzata la `STANDARD` classe di archiviazione.
       - `STANDARD_IA`: (Accesso standard - non frequente) Utilizza questa classe di storage per i dati a cui si accede meno frequentemente, ma che richiedono comunque un accesso rapido quando necessario.
       - `REDUCED_REDUNDANCY`: Utilizzare questa classe di archiviazione per i dati non critici e riproducibili che possono essere memorizzati con una ridondanza minore rispetto alla `STANDARD` classe di archiviazione.
     - Se si specifica un nell'XML di configurazione, `Role` questo verrà ignorato. Questo valore non viene utilizzato da StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
3. Selezionare il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services** > **Replication**.
5. Selezionare la casella di controllo **Enable Replication** (attiva replica).
6. Incollare il file XML di configurazione della replica nella casella di testo e selezionare **Save changes** (Salva modifiche).

   > I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID utilizzando l'API di gestione griglia o di gestione griglia. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che la replica sia configurata correttamente:
   a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per la replica come specificato nella configurazione della replica.

      Nell'esempio illustrato in precedenza, gli oggetti che corrispondono al prefisso "2020" vengono replicati.

   b. Verificare che l'oggetto sia stato replicato nel bucket di destinazione.

      Per gli oggetti di piccole dimensioni, la replica avviene rapidamente.

Informazioni correlate

"Creare endpoint di servizi di piattaforma"

Configurare le notifiche degli eventi

È possibile attivare le notifiche per un bucket creando un XML di configurazione delle notifiche e utilizzando Gestione tenant per applicare il file XML a un bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- Hai già creato un bucket per fungere da origine delle notifiche.
- L'endpoint che si intende utilizzare come destinazione per le notifiche degli eventi esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

È possibile configurare le notifiche degli eventi associando l'XML di configurazione delle notifiche a un bucket di origine. La configurazione delle notifiche XML segue le convenzioni S3 per la configurazione delle notifiche bucket, con l'argomento Kafka o Amazon SNS di destinazione specificato come URN di un endpoint.

Per informazioni generali sulle notifiche degli eventi e su come configurarle, fare riferimento alla "Documentazione Amazon" . Per informazioni su come StorageGRID implementa l'API di configurazione delle notifiche bucket S3, fare riferimento alla "Istruzioni per l'implementazione delle applicazioni client S3".

Durante la configurazione delle notifiche degli eventi per un bucket, osservare i seguenti requisiti e caratteristiche:

- Quando si crea e si applica un XML di configurazione di notifica valido, è necessario utilizzare l'URN di un endpoint di notifica degli eventi per ciascuna destinazione.
- Sebbene la notifica degli eventi possa essere configurata in un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (incluso lo stato Mantieni fino alla data e conservazione legale) degli oggetti non verranno inclusi nei messaggi di notifica.
- Dopo aver configurato le notifiche degli eventi, ogni volta che si verifica un evento specifico per un oggetto nel bucket di origine, viene generata una notifica e inviata all'argomento Amazon SNS o Kafka utilizzato come endpoint di destinazione.
- Se si abilitano le notifiche degli eventi per un bucket che contiene oggetti, le notifiche vengono inviate solo per le azioni eseguite dopo il salvataggio della configurazione della notifica.

Fasi

1. Abilita le notifiche per il bucket di origine:
   - Utilizzare un editor di testo per creare l'XML di configurazione delle notifiche richiesto per attivare le notifiche degli eventi, come specificato nell'API di notifica S3.
   - Quando si configura l'XML, utilizzare l'URN di un endpoint di notifica degli eventi come argomento di destinazione.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. In Tenant Manager, selezionare **STORAGE (S3)** > **Bucket**.
3. Selezionare il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services** > **Event Notifications**.

5. Selezionare la casella di controllo **attiva notifiche eventi**.
6. Incollare l'XML di configurazione della notifica nella casella di testo e selezionare **Salva modifiche**.

> I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID utilizzando l'API di gestione griglia o di gestione griglia. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che le notifiche degli eventi siano configurate correttamente:

   a. Eseguire un'azione su un oggetto nel bucket di origine che soddisfi i requisiti per l'attivazione di una notifica come configurato nel XML di configurazione.

      Nell'esempio, viene inviata una notifica di evento ogni volta che viene creato un oggetto con il `images/` prefisso.

   b. Conferma che è stata inviata una notifica all'argomento Amazon SNS o Kafka di destinazione.

      Ad esempio, se l'argomento di destinazione è ospitato su Amazon SNS, è possibile configurare il servizio in modo che invii un'e-mail al momento della consegna della notifica.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+ Se la notifica viene ricevuta nell'argomento di destinazione, il bucket di origine è stato configurato correttamente per le notifiche StorageGRID.

Informazioni correlate

"Comprendere le notifiche per i bucket"

"UTILIZZARE L'API REST S3"

"Creare endpoint di servizi di piattaforma"

Configurare il servizio di integrazione della ricerca

È possibile abilitare l'integrazione della ricerca per un bucket creando l'integrazione della ricerca XML e utilizzando Tenant Manager per applicare l'XML al bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- È già stato creato un bucket S3 di cui si desidera indicizzare il contenuto.
- L'endpoint che si intende utilizzare come destinazione per il servizio di integrazione della ricerca esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

Dopo aver configurato il servizio di integrazione della ricerca per un bucket di origine, la creazione di un oggetto o l'aggiornamento dei metadati o dei tag di un oggetto attiva l'invio dei metadati dell'oggetto all'endpoint di destinazione.

Se abiliti il servizio di integrazione della ricerca per un bucket che contiene già oggetti, le notifiche dei metadati non vengono inviate automaticamente per gli oggetti esistenti. Aggiornare questi oggetti esistenti per assicurarsi che i relativi metadati vengano aggiunti all'indice di ricerca della destinazione.

Fasi

1. Consentire l'integrazione della ricerca per un bucket:
    - Utilizzare un editor di testo per creare l'XML di notifica dei metadati necessario per abilitare l'integrazione della ricerca.
    - Quando si configura l'XML, utilizzare l'URN di un endpoint di integrazione della ricerca come destinazione.

      Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, è possibile inviare metadati per gli oggetti con il prefisso `images` a una destinazione e metadati per gli oggetti con il prefisso `videos` a un'altra. Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate quando vengono inviate. Ad esempio, una configurazione che include una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2` non è consentita.

      Se necessario, fare riferimento alla Esempi di XML di configurazione dei metadati.

      ```
      <MetadataNotificationConfiguration>
       <Rule>
          <Status>Enabled</Status>
          <Prefix></Prefix>
          <Destination>
             <Urn>/Urn>
             </Destination>
       </Rule>
      </MetadataNotificationConfiguration>
      ```

Elementi nella configurazione della notifica dei metadati XML:

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì

Nome	Descrizione	Obbligatorio
Urna	URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • `es` deve essere il terzo elemento. • L'URN deve terminare con l'indice e digitare dove sono memorizzati i metadati, nel formato `domain-name/myindex/mytype`. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'URN è incluso nell'elemento Destination.	Sì

2. In Tenant Manager, selezionare **STORAGE (S3)** > **Bucket**.
3. Selezionare il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services** > **Search Integration**
5. Selezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).
6. Incollare la configurazione di notifica dei metadati nella casella di testo e selezionare **Salva modifiche**.

   I servizi della piattaforma devono essere attivati per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che il servizio di integrazione della ricerca sia configurato correttamente:
   a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per l'attivazione di una notifica dei metadati come specificato nel file XML di configurazione.

      Nell'esempio illustrato in precedenza, tutti gli oggetti aggiunti al bucket attivano una notifica dei metadati.

   b. Verificare che un documento JSON contenente i metadati e i tag dell'oggetto sia stato aggiunto all'indice di ricerca specificato nell'endpoint.

Al termine

Se necessario, è possibile disattivare l'integrazione della ricerca per un bucket utilizzando uno dei seguenti

metodi:

- Selezionare **STORAGE (S3)** > **Bucket** e deselezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).
- Se si utilizza direttamente l'API S3, utilizzare una richiesta DI notifica DELETE Bucket metadata. Consultare le istruzioni per l'implementazione delle applicazioni client S3.

esempio: Configurazione di notifica dei metadati che si applica a tutti gli oggetti

In questo esempio, i metadati degli oggetti per tutti gli oggetti vengono inviati alla stessa destinazione.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Esempio: Configurazione della notifica di metadati con due regole

In questo esempio, i metadati degli oggetti corrispondenti al prefisso `/images` vengono inviati a una destinazione, mentre i metadati degli oggetti corrispondenti al prefisso `/videos` vengono inviati a una seconda destinazione.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Formato di notifica dei metadati

Quando si attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. La `test` benna non è in versione, quindi l' `versionId`etichetta è vuota.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Campi inclusi nel documento JSON

Il nome del documento include il nome del bucket, il nome dell'oggetto e l'ID della versione, se presente.

Informazioni su bucket e oggetti

`bucket`: Nome del bucket

`key`: Nome chiave oggetto

`versionID`: Versione oggetto, per gli oggetti nei bucket in versione

`region`: Area bucket, ad esempio `us-east-1`

Metadati di sistema

`size`: Dimensione dell'oggetto (in byte) come visibile a un client HTTP

`md5`: Hash oggetto

Metadati dell'utente

`metadata`: Tutti i metadati utente per l'oggetto, come coppie chiave-valore

`key:value`

Tag

`tags`: Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore

`key:value`

Come visualizzare i risultati in Elasticsearch

Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o

numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Attivare le mappature dinamiche dei campi nell'indice prima di configurare il servizio di integrazione della ricerca. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Informazioni sul copyright

Informazioni sul marchio commerciale