Gestisci i servizi della piattaforma S3

StorageGRID software

NetApp
July 23, 2026

Sommario

Gestisci i servizi della piattaforma S3

servizi della piattaforma S3

Scopri i servizi della piattaforma per StorageGRID

Prima di implementare i servizi della piattaforma, dai un'occhiata alla panoramica e alle considerazioni per l'utilizzo di questi servizi.

Per informazioni su S3, vedi "${post_edited_translations.segment}".

Panoramica dei servizi della piattaforma

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

Poiché la posizione di destinazione per i servizi della piattaforma è in genere esterna alla tua distribuzione StorageGRID, i servizi della piattaforma ti 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 tuoi dati.

Puoi configurare qualsiasi combinazione di servizi della piattaforma per un singolo bucket S3. Ad esempio, puoi configurare sia "servizio CloudMirror" sia "notifiche" su un bucket S3 di StorageGRID così da poter replicare oggetti specifici su Amazon Simple Storage Service (S3), mentre invii una notifica relativa a ciascun oggetto a un'applicazione di monitoraggio di terze parti per aiutarti a tenere traccia delle tue spese AWS.

L'utilizzo dei servizi della piattaforma deve essere abilitato per ogni account tenant da un amministratore StorageGRID tramite il Grid Manager o la Grid Management API.

${post_edited_translations.segment}

I servizi della piattaforma comunicano con endpoint esterni che configuri usando il "${post_edited_translations.segment}" o il "API di gestione tenant". Ogni endpoint rappresenta una destinazione esterna, come un bucket Amazon S3 di StorageGRID, un bucket Amazon Web Services, un argomento Amazon SNS, un endpoint webhook o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

Dopo aver creato un endpoint esterno, puoi abilitare 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.

Devi aggiungere configurazioni XML separate per ciascun servizio di piattaforma che vuoi configurare. Ad esempio:

- Se vuoi che tutti gli oggetti le cui chiavi iniziano con `/images` vengano replicati in un bucket Amazon S3, devi aggiungere una configurazione di replica al bucket di origine.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

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

${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}
replicazione CloudMirror	• GetBucketReplication • PutBucketReplication	• "replicazione CloudMirror" • "Operazioni sui bucket"
Notifiche	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notifiche" • "Operazioni sui bucket"
Integrazione della ricerca	• GET Configurazione della notifica dei metadati del bucket • Configurazione della notifica dei metadati del bucket PUT	• "Integrazione della ricerca" • "Operazioni personalizzate di StorageGRID"

${post_edited_translations.segment}

Considerazione	Dettagli
${post_edited_translations.segment}	Devi monitorare la disponibilità di ciascun endpoint di destinazione. Se la connettività all'endpoint di destinazione viene persa per un periodo di tempo prolungato e si crea un grande backlog di richieste, le richieste client aggiuntive (come le richieste PUT) a StorageGRID falliranno. Devi riprovare queste richieste fallite quando l'endpoint diventa raggiungibile.
Limitazione dell'endpoint di destinazione	Il software StorageGRID potrebbe limitare le richieste S3 in entrata per un bucket se il tasso con cui vengono inviate le richieste supera il tasso con cui l'endpoint di destinazione può riceverle. La limitazione si verifica solo quando c'è un accumulo di richieste in attesa di essere inviate all'endpoint di destinazione. L'unico effetto visibile è che le richieste S3 in entrata impiegheranno più tempo per essere eseguite. Se inizi a rilevare prestazioni significativamente più lente, dovresti ridurre il tasso di acquisizione o usare un endpoint con una capacità maggiore. Se il backlog delle richieste continua a crescere, le operazioni S3 del client (come le richieste PUT) alla fine non andranno a buon fine. Le richieste CloudMirror hanno maggiori probabilità di essere influenzate dalle prestazioni dell'endpoint di destinazione perché in genere comportano un trasferimento di dati maggiore rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Considerazione	Dettagli
${post_edited_translations.segment}	StorageGRID garantisce l'ordinamento delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni su un oggetto vengono eseguite all'interno dello stesso sito, lo stato finale dell'oggetto (ai fini della replica) sarà sempre uguale allo stato in StorageGRID. StorageGRID fa del suo meglio per ordinare le richieste quando le operazioni vengono eseguite tra i siti StorageGRID. Ad esempio, se scrivi inizialmente un oggetto nel sito A e successivamente sovrascrivi lo stesso oggetto nel sito B, non è garantito che l'oggetto finale replicato da CloudMirror nel bucket di destinazione sia l'oggetto più recente.
${post_edited_translations.segment}	Per uniformarsi al comportamento di eliminazione di AWS CRR e Amazon Simple Notification Service, le richieste CloudMirror e 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, non vengono inviate richieste CloudMirror o di notifica degli eventi se una regola ILM elimina un oggetto dopo 14 giorni. ${post_edited_translations.segment}
${post_edited_translations.segment}	Per gli endpoint Kafka, il Mutual TLS non è supportato. Di conseguenza, se hai `ssl.client.auth` impostato su `required` nella configurazione del tuo broker Kafka, potrebbe causare problemi di configurazione dell'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 di nome utente e password. • SASL/PLAIN • ${post_edited_translations.segment} • SASL/SCRAM-SHA-512 **Nota:** Le impostazioni del proxy di archiviazione configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Considerazioni sull'utilizzo del servizio di replica CloudMirror

Considerazione	Dettagli
${post_edited_translations.segment}	StorageGRID non supporta l' `x-amz-replication-status`intestazione.
Dimensione dell'oggetto	La dimensione massima degli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è di 5 TiB, che equivale alla dimensione massima *supportata* dell'oggetto. **Nota**: la dimensione massima *consigliata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se hai oggetti di dimensioni superiori a 5 GiB, usa invece il multipart upload.

Considerazione	Dettagli
${post_edited_translations.segment}	Se il bucket S3 di origine in StorageGRID ha la gestione delle versioni abilitata, dovresti abilitarla anche per il bucket di destinazione. Quando usi il versioning, tieni presente che l'ordine delle versioni degli oggetti nel bucket di destinazione è approssimativo e non garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3. ${post_edited_translations.segment}
Etichettatura per le versioni degli oggetti	Il servizio CloudMirror non replica le richieste PutObjectTagging o DeleteObjectTagging che forniscono un ID versione, a causa di limitazioni nel protocollo S3. Poiché gli ID versione per la sorgente e la destinazione non sono correlati, non è possibile garantire che un aggiornamento dei tag a un ID versione specifico venga replicato. Al contrario, il servizio CloudMirror replica le richieste PutObjectTagging o DeleteObjectTagging che non specificano un ID versione. Queste richieste aggiornano i tag per la chiave più recente (o la versione più recente se il bucket è dotato di controllo delle versioni). Vengono replicate anche le normali acquisizioni con tag (non gli aggiornamenti dei tag).
Upload multiparte e valori `ETag`	Quando esegui il mirroring di oggetti caricati tramite un caricamento multipart, il servizio CloudMirror non conserva le parti. Di conseguenza, il valore `ETag` dell'oggetto duplicato sarà diverso dal valore `ETag` 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 provi a inserire un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione non riesce.
${post_edited_translations.segment}	La replica non è supportata per i bucket di origine o di destinazione con S3 Object Lock abilitato.

Scopri il servizio di replica CloudMirror di StorageGRID

Puoi abilitare la replica CloudMirror per un bucket S3 se vuoi che StorageGRID replichi gli oggetti specificati aggiunti al bucket in uno o più bucket di destinazione esterni.

Ad esempio, potresti utilizzare la replica CloudMirror per duplicare specifici record dei clienti in Amazon S3 e poi sfruttare i servizi AWS per eseguire analisi sui tuoi dati.

La replica CloudMirror non è supportata se il bucket di origine ha S3 Object Lock abilitato.

CloudMirror e ILM

La replica CloudMirror funziona in modo indipendente dalle policy ILM attive della grid. Il servizio CloudMirror replica gli oggetti man mano che vengono memorizzati nel bucket di origine e li consegna al bucket di destinazione il prima possibile. La consegna degli oggetti replicati viene avviata quando l'ingest dell'oggetto ha esito positivo.

CloudMirror e replicazione cross-grid

La replica CloudMirror presenta importanti somiglianze e differenze con la funzionalità di replica cross-grid. Consulta "Confronta la replica cross-grid e la replica CloudMirror".

CloudMirror e bucket S3

CloudMirror replication viene in genere configurata per utilizzare un bucket S3 esterno come destinazione. Tuttavia, puoi anche configurare la replica per utilizzare un'altra implementazione di StorageGRID o qualsiasi servizio compatibile con S3.

bucket esistenti

Quando abiliti la replica CloudMirror per un bucket esistente, vengono replicati solo i nuovi oggetti aggiunti a quel bucket. Gli oggetti già presenti nel bucket non vengono replicati. Per forzare la replica degli oggetti esistenti, puoi aggiornare i metadati dell'oggetto eseguendo una copia dell'oggetto.

> Se usi la replica CloudMirror per copiare oggetti in una destinazione Amazon S3, tieni 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, quell'oggetto non verrà replicato.

Bucket di destinazione multipli

Per replicare gli oggetti in un singolo bucket su più bucket di destinazione, specifica la destinazione per ciascuna regola nell'XML di configurazione della replica. Non puoi replicare un oggetto su più di un bucket contemporaneamente.

Bucket con versione o senza versione

Puoi configurare la replica CloudMirror su bucket con o senza versione. I bucket di destinazione possono essere con o senza versione. Puoi usare qualsiasi combinazione di bucket con e senza versione. Ad esempio, puoi specificare un bucket con versione come destinazione per un bucket di origine senza versione, o viceversa. Puoi anche replicare tra bucket senza versione.

${post_edited_translations.segment}

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 dotati di controllo delle versioni, il marcatore di eliminazione viene replicato. Se il bucket di destinazione non è dotato di controllo delle versioni, l'eliminazione di un oggetto nel bucket di origine non replica il marcatore di eliminazione nel bucket di destinazione né elimina l'oggetto di destinazione.

${post_edited_translations.segment}

Man mano che gli oggetti vengono replicati nel bucket di destinazione, StorageGRID li contrassegna come "repliche". Un bucket StorageGRID di destinazione non replicherà nuovamente 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 AWS CRR quando utilizzi un bucket Amazon S3 come destinazione.

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

${post_edited_translations.segment}

L'unicità e l'ordine degli eventi nel bucket di destinazione non sono garantiti. Più di una copia identica di un oggetto di origine potrebbe essere consegnata alla destinazione a seguito di 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.

Scopri le notifiche degli eventi di StorageGRID per i bucket S3

Puoi abilitare la notifica degli eventi per un bucket S3 se vuoi che StorageGRID invii notifiche relative a eventi specifici a una destinazione cluster Kafka, a un endpoint webhook o ad Amazon Simple Notification Service.

Ad esempio, puoi configurare avvisi da inviare agli amministratori per ogni oggetto aggiunto a un bucket, dove gli oggetti rappresentano file di registro associati a un evento critico del sistema.

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

L'unicità e l'ordine delle notifiche non sono garantiti. Più di una notifica di un evento potrebbe essere recapitata alla destinazione come risultato delle operazioni eseguite per garantire il successo della consegna. E poiché la consegna è asincrona, non è garantito che l'ordine temporale delle notifiche a livello di destinazione corrisponda all'ordine degli eventi sul bucket di origine, in particolare per le operazioni che hanno origine da diversi siti StorageGRID. Puoi utilizzare la chiave `sequencer` nel messaggio dell'evento per determinare l'ordine degli eventi per un particolare oggetto, come descritto nella documentazione di Amazon S3.

${post_edited_translations.segment}

- 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:Delete
  - s3:ObjectRemoved:DeleteMarkerCreated
  - s3:ObjectRestore:Post
- ${post_edited_translations.segment}

Nome chiave	${post_edited_translations.segment}
eventSource	`sgws:s3`
awsRegion	${post_edited_translations.segment}

Nome chiave	${post_edited_translations.segment}
x-amz-id-2	${post_edited_translations.segment}
arn	`urn:sgws:s3:::bucket_name`

Scopri il servizio di integrazione della ricerca StorageGRID

Puoi abilitare l'integrazione della ricerca per un bucket S3 se vuoi utilizzare un servizio esterno di ricerca e analisi dei dati per i metadati degli oggetti.

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

Ad esempio, potresti configurare i tuoi bucket in modo che inviino i metadati degli oggetti S3 a un servizio Elasticsearch remoto. Potresti quindi utilizzare Elasticsearch per eseguire ricerche tra i bucket e condurre analisi sofisticate dei modelli presenti nei metadati degli oggetti.

${post_edited_translations.segment}

> Poiché il servizio di integrazione della ricerca causa l'invio dei metadati dell'oggetto a una destinazione, il suo XML di configurazione viene definito "XML di configurazione delle notifiche dei *metadati*." Questo XML di configurazione è diverso dall'"XML di configurazione delle notifiche" utilizzato per abilitare le notifiche degli *eventi*.

Integrazione della ricerca e bucket S3

Puoi abilitare il servizio di integrazione della ricerca per qualsiasi bucket con o senza controllo delle versioni. L'integrazione della ricerca viene configurata associando al bucket l'XML di configurazione delle notifiche dei metadati, che specifica su quali oggetti agire e la destinazione per i metadati dell'oggetto.

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

> Per i tag e i metadati utente, StorageGRID trasmette date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo che interpreti queste stringhe come date o numeri, segui le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati data. Devi abilitare la mappatura dinamica dei campi sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo che un documento è stato indicizzato, non puoi modificare i tipi di campo del documento nell'indice.

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- Un oggetto viene eliminato, anche quando gli oggetti vengono eliminati a seguito dell'operazione della

policy ILM della griglia.

- I metadati o i tag dell'oggetto vengono aggiunti, aggiornati o eliminati. L'insieme completo di metadati e tag viene sempre inviato al momento dell'aggiornamento — non solo i valori modificati.

Dopo aver aggiunto l'XML di configurazione delle notifiche dei metadati a un bucket, le notifiche vengono inviate per tutti i nuovi oggetti che crei e per tutti gli oggetti che modifichi aggiornandone i dati, i metadati utente o i tag. Tuttavia, le notifiche non vengono inviate per gli oggetti già presenti nel bucket. Per garantire che i metadati dell'oggetto per tutti gli oggetti nel bucket vengano inviati alla destinazione, dovresti eseguire una delle seguenti operazioni:

- ${post_edited_translations.segment}
- Esegui un'azione su tutti gli oggetti già presenti nel bucket che attiverà l'invio di un messaggio di notifica dei metadati alla destinazione.

${post_edited_translations.segment}

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 è utilizzato nell'XML di configurazione del servizio. Utilizza il "Tool NetApp Interoperability Matrix" per determinare le versioni supportate di Elasticsearch.

Gestisci gli endpoint dei servizi della piattaforma

Configura gli endpoint dei servizi della piattaforma in StorageGRID

Prima di poter configurare un servizio della piattaforma per un bucket, devi configurare almeno un endpoint come destinazione per il servizio della piattaforma.

L'accesso ai servizi della piattaforma è abilitato per singolo tenant da un amministratore StorageGRID. Per creare o utilizzare un endpoint dei servizi della piattaforma, devi essere un utente tenant con autorizzazione "Gestisci endpoint" o accesso Root, in una grid la cui rete è stata configurata per consentire ai nodi di Storage di accedere alle risorse degli endpoint esterni. Per un singolo tenant, puoi configurare un massimo di 500 endpoint dei servizi della piattaforma. Contatta il tuo amministratore StorageGRID per ulteriori informazioni.

Che cos'è un endpoint dei servizi di piattaforma?

Un endpoint dei servizi della piattaforma specifica le informazioni di cui StorageGRID ha bisogno per accedere alla destinazione esterna.

Ad esempio, se vuoi replicare oggetti da un bucket StorageGRID a un bucket Amazon S3, devi creare un endpoint dei servizi della piattaforma che includa le informazioni e le credenziali di cui StorageGRID ha bisogno per accedere al bucket di destinazione su Amazon.

Ogni tipo di servizio della piattaforma richiede un endpoint dedicato, quindi devi configurare almeno un endpoint per ogni servizio della piattaforma che vuoi usare. Dopo aver definito un endpoint per i servizi della piattaforma, usi l'URN dell'endpoint come destinazione nel file XML di configurazione usato per abilitare il servizio.

Puoi usare lo stesso endpoint come destinazione per più di un bucket di origine. Ad esempio, puoi configurare diversi bucket di origine per inviare metadati degli oggetti allo stesso endpoint di integrazione della ricerca, così puoi eseguire ricerche su più bucket. Puoi anche configurare un bucket di origine per usare più di un endpoint come destinazione, il che ti permette di fare cose come inviare notifiche sulla creazione di oggetti a un topic di Amazon Simple Notification Service (Amazon SNS) e notifiche sull'eliminazione di oggetti a un

secondo topic di Amazon SNS.

Endpoint per la replica CloudMirror

StorageGRID supporta endpoint di replica che rappresentano bucket S3. Questi bucket possono essere ospitati su Amazon Web Services, sulla stessa implementazione di StorageGRID, su un'implementazione remota o su un altro servizio.

Endpoint per le notifiche

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

Per gli endpoint Kafka, il Mutual TLS non è supportato. Di conseguenza, se hai `ssl.client.auth` impostato su `required` nella configurazione del tuo broker Kafka, potrebbe causare problemi di configurazione dell'endpoint Kafka.

Endpoint per il servizio di integrazione della ricerca

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

L'endpoint di integrazione della ricerca fa riferimento a uno specifico indice e tipo di Elasticsearch. Devi creare l'indice in Elasticsearch prima di creare l'endpoint in StorageGRID, altrimenti la creazione dell'endpoint non riuscirà. Non serve creare il tipo prima di creare l'endpoint. StorageGRID creerà il tipo, se necessario, quando invia i metadati dell'oggetto all'endpoint.

Informazioni correlate

"${post_edited_translations.segment}"

Specificare un URN per un endpoint dei servizi della piattaforma StorageGRID

Quando crei un endpoint dei servizi di piattaforma, devi specificare un Unique Resource Name (URN). Utilizzerai l'URN per fare riferimento all'endpoint quando crei un XML di configurazione per il servizio di piattaforma. L'URN per ciascun endpoint deve essere univoco.

StorageGRID convalida gli endpoint dei servizi di piattaforma mentre li crei. Prima di creare un endpoint dei servizi di piattaforma, conferma che la risorsa specificata nell'endpoint esista e sia raggiungibile.

Elementi URN

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

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

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

${post_edited_translations.segment}

Servizio	Tipo
replicazione CloudMirror	`s3`
Notifiche	`sns`, `kafka`, o `webhook`
Integrazione della ricerca	`es`

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

Per la maggior parte degli endpoint, l'elemento finale dell'URN identifica la risorsa specifica di destinazione all'URI di destinazione, ad esempio `sns-topic-name`.

${post_edited_translations.segment}

Servizio	${post_edited_translations.segment}
replicazione CloudMirror	`bucket-name`
Notifiche	`sns-topic-name` o `kafka-topic-name` **Nota:** Per gli endpoint webhook, l'ultimo elemento dell'URN può essere una stringa qualsiasi, purché l'URN dell'endpoint sia univoco.
Integrazione della ricerca	`domain-name/index-name/type-name` ${post_edited_translations.segment}

${post_edited_translations.segment}

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

- Replicazione 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, il `domain-name` deve includere la stringa letterale `domain/`, come mostrato qui.

${post_edited_translations.segment}

Quando utilizzi servizi ospitati localmente anziché servizi cloud, puoi specificare l'URN in qualsiasi modo crei un URN valido e univoco, purché l'URN includa gli elementi richiesti nella terza e ultima posizione. Puoi lasciare vuoti gli elementi indicati come opzionali, oppure puoi specificarli in qualsiasi modo ti aiuti a identificare la risorsa e a rendere l'URN univoco. Ad esempio:

- Replicazione CloudMirror:

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

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

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

- Notifiche:

  ${post_edited_translations.segment}

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

  Specifica un endpoint Kafka:

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

  Specifica un endpoint webhook:

  ```
  urn:mysite:webhook:optional:optional:webhook-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 `domain-name` può essere qualsiasi stringa, purché l'URN dell'endpoint sia univoco.

Creare un endpoint dei servizi della piattaforma StorageGRID

Devi creare almeno un endpoint del tipo corretto prima di poter abilitare un servizio della piattaforma.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- I servizi della piattaforma sono stati abilitati per il tuo tenant account da un amministratore di StorageGRID.
- Tu appartieni a un gruppo di utenti che ha il "Gestisci endpoint o autorizzazione di accesso root".
- La risorsa a cui fa riferimento l'endpoint dei servizi della piattaforma è stata creata:
  - CloudMirror replication: bucket S3
  - Notifica degli eventi: topic Amazon Simple Notification Service (Amazon SNS), topic Kafka o endpoint webhook
  - Notifica di ricerca: indice Elasticsearch, se il cluster di destinazione non è configurato per creare automaticamente gli indici.
- Hai le informazioni sulla risorsa di destinazione:
  - Host e porta per l'Uniform Resource Identifier (URI)

    > Se prevedi di utilizzare un bucket ospitato su un sistema StorageGRID come endpoint per la replica CloudMirror, contatta l'amministratore della grid per sapere quali valori inserire.

  - Nome univoco della risorsa (URN)

    "Specifica l'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, puoi utilizzare le seguenti credenziali:

- Chiave di accesso: ID della chiave di accesso e chiave di accesso segreta
- HTTP di base: nome utente e password

endpoint di replica CloudMirror

Per gli endpoint di replica CloudMirror, puoi usare le seguenti credenziali:

- Chiave di accesso: ID della chiave di accesso e chiave di accesso segreta
- CAP (C2S Access Portal): URL delle credenziali temporanee, certificati server e client, chiavi client e una passphrase facoltativa per la chiave privata del client.

Endpoint Amazon SNS

Per gli endpoint Amazon SNS, puoi usare le seguenti credenziali:

- Chiave di accesso: ID della chiave di accesso e chiave di accesso segreta

Endpoint Kafka

Per gli endpoint Kafka, puoi 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 sicurezza (se è richiesta la verifica del certificato)

- Se le funzionalità di sicurezza di Elasticsearch sono abilitate, hai il privilegio di monitoraggio del cluster per i test di connettività e il privilegio di scrittura sull'indice oppure entrambi i privilegi di indicizzazione e cancellazione dell'indice per gli aggiornamenti dei documenti.

Passaggi

1. Seleziona **ARCHIVIAZIONE (S3)** > **Endpoint dei servizi della piattaforma**. Viene visualizzata la pagina Endpoint dei servizi della piattaforma.
2. Seleziona **Crea endpoint**.
3. Inserisci 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 questo è elencato nella pagina Endpoints, quindi non devi includere questa informazione nel nome.

4. Nel campo **URI**, specifica l'identificatore univoco della risorsa (URI) dell'endpoint.

   Usa uno dei seguenti formati:

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

Se non specifichi 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 il VIP (virtual IP) del gruppo HA (alta disponibilità) di StorageGRID, e `10443` rappresenta la porta definita nell'endpoint del load balancer.

> Quando possibile, dovresti connetterti a un gruppo HA di nodi di bilanciamento del carico per evitare un single point of failure.

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 va inserito nel campo **URN**.

5. Inserisci il nome univoco della risorsa (URN) per l'endpoint.

> Non puoi modificare l'URN di un endpoint dopo che è stato creato.

6. Seleziona **Continue**.
7. Seleziona un valore per **Tipo di autenticazione**.

> Se vuoi l'autenticazione per gli endpoint webhook, configura Mutual Transport Layer Security (mTLS) in Passo 9.

Endpoint di integrazione della ricerca

Inserisci o carica le credenziali per un endpoint di integrazione della ricerca.

Le credenziali che fornisci devono avere i permessi di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Consente accesso anonimo alla destinazione. Funziona solo per gli endpoint con la sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile 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

Inserisci o carica le credenziali per un endpoint di replica CloudMirror.

Le credenziali che fornisci devono avere i permessi di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Consente accesso anonimo alla destinazione. Funziona solo per gli endpoint con la sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta
CAP (C2S Access Portal)	Utilizza certificati e chiavi per autenticare le connessioni alla destinazione.	• URL delle credenziali temporanee • 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 crittografata) • Frase di accesso della chiave privata del client (facoltativa)

Endpoint Amazon SNS

Inserisci o carica le credenziali per un endpoint Amazon SNS.

Le credenziali che fornisci devono avere i permessi di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Consente accesso anonimo alla destinazione. Funziona solo per gli endpoint con la sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta

Endpoint Kafka

Inserisci o carica le credenziali per un endpoint Kafka.

Le credenziali che fornisci devono avere i permessi di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Consente accesso anonimo alla destinazione. Funziona solo per gli endpoint con la sicurezza disabilitata.	Nessuna autenticazione.
SASL/PLAIN	Utilizza un nome utente e una password in chiaro per autenticare le connessioni alla destinazione.	• Nome utente • Password
${post_edited_translations.segment}	Utilizza un nome utente e una password tramite un protocollo di challenge-response e l'algoritmo di hashing SHA-256 per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-512	Utilizza un nome utente e una password tramite un protocollo di challenge-response e l'algoritmo di hashing SHA-512 per autenticare le connessioni alla destinazione.	• Nome utente • Password

Seleziona **Usa l'autenticazione tramite delega** se il nome utente e la password derivano da un token di delega ottenuto da un cluster Kafka.

8. Seleziona **Continue**.
9. Seleziona un pulsante di opzione per **Verifica certificati** per scegliere come viene verificata la connessione TLS all'endpoint.

La maggior parte degli endpoint

Verifica la connessione TLS per l'integrazione Search, la replica CloudMirror, Amazon SNS o gli endpoint Kafka.

Tipo di verifica del certificato	Descrizione
TLS	Convalida il certificato del server per le connessioni TLS alla risorsa endpoint.
Disattivato	La verifica del certificato è disabilitata. Questa opzione non è sicura.
Usa un certificato CA personalizzato	Il certificato CA personalizzato viene utilizzato per verificare l'identità del server durante la connessione all'endpoint.
Usa il certificato CA del sistema operativo	Usa il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.

Solo endpoint Webhook

Verifica la connessione TLS per gli endpoint webhook.

Tipo di verifica del certificato	Descrizione
TLS	Convalida il certificato del server per le connessioni TLS alla risorsa endpoint.
mTLS	Convalida i certificati client e server per le connessioni Mutual TLS alla risorsa endpoint.
Disattivato	La verifica del certificato è disabilitata. Questa opzione non è sicura.
Usa un certificato CA personalizzato	Il certificato CA personalizzato viene utilizzato per verificare l'identità del server durante la connessione all'endpoint.

Quando selezioni **mTLS**, queste opzioni diventano disponibili.

Tipo di verifica del certificato	Descrizione
Non verificare il certificato del server	Disabilita la verifica del certificato del server, il che significa che l'identità del server non viene verificata. Questa opzione non è sicura.
Certificato client	${post_edited_translations.segment}

Tipo di verifica del certificato	Descrizione
Chiave privata del client	La chiave privata per il certificato client. Se crittografata, deve utilizzare il formato tradizionale PKCS #1 (il formato PKCS #8 non è supportato).
${post_edited_translations.segment}	La passphrase per decrittografare la chiave privata del client. Se la chiave privata non è crittografata, lascia questo campo vuoto.

10. Seleziona **Testa e crea endpoint**.
    - Se l'endpoint è raggiungibile con le credenziali specificate, viene visualizzato un messaggio di successo. La connessione all'endpoint viene convalidata da un nodo in ciascun sito.
    - Viene visualizzato un messaggio di errore se la convalida dell'endpoint non riesce. Se devi modificare l'endpoint per correggere l'errore, seleziona **Torna ai dettagli dell'endpoint** e aggiorna le informazioni. Poi seleziona **Verifica e crea endpoint**.

> La creazione dell'endpoint non riesce se i servizi di piattaforma non sono abilitati per il tuo account tenant. Contatta il tuo amministratore di StorageGRID.

Dopo aver configurato un endpoint, puoi usare il suo URN per configurare un servizio della piattaforma.

Informazioni correlate

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

Verifica la connessione per un endpoint dei servizi della piattaforma StorageGRID

${post_edited_translations.segment}

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Gestisci endpoint o autorizzazione di accesso root".

Informazioni su questa attività

${post_edited_translations.segment}

Passaggi

1. Seleziona **STORAGE (S3)** > **Platform services endpoints**.

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}

   Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Seleziona **Test connessione**.
   - Se l'endpoint è raggiungibile con le credenziali specificate, viene visualizzato un messaggio di successo. La connessione all'endpoint viene convalidata da un nodo in ciascun sito.
   - Viene visualizzato un messaggio di errore se la convalida dell'endpoint non riesce. Se devi modificare l'endpoint per correggere l'errore, seleziona **Configurazione** e aggiorna le informazioni. Poi seleziona **Verifica e salva le modifiche**.

Modifica un endpoint dei servizi della piattaforma in StorageGRID

Puoi modificare la configurazione di un endpoint dei servizi di piattaforma per cambiarne il nome, l'URI o altri dettagli. Ad esempio, potresti dover aggiornare le credenziali scadute o modificare l'URI per fare in modo che punti a un indice Elasticsearch di backup per il failover. Non puoi modificare l'URN di un endpoint dei servizi di piattaforma.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Gestisci endpoint o autorizzazione di accesso root".

Passaggi

1. Seleziona **STORAGE (S3)** > **Platform services endpoints**.

   ${post_edited_translations.segment}

2. Seleziona l'endpoint che desideri modificare.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Seleziona **Configurazione**.
4. ${post_edited_translations.segment}

   Non puoi modificare l'URN di un endpoint dopo che è stato creato.

   a. Per modificare il nome visualizzato dell'endpoint, seleziona l'icona di modifica .
   b. ${post_edited_translations.segment}
   c. Se necessario, cambia il tipo di autenticazione.
      - Per l'autenticazione tramite chiave di accesso, modifica la chiave come necessario selezionando **Modifica chiave S3** e incollando un nuovo ID della chiave di accesso e una nuova chiave di accesso segreta. Se devi annullare le modifiche, seleziona **Ripristina modifica chiave S3**.
      - Per l'autenticazione CAP (C2S Access Portal), modifica l'URL delle credenziali temporanee o la passphrase facoltativa della chiave privata del client e carica i nuovi file del certificato e della chiave, se necessario.

        ${post_edited_translations.segment}

   d. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
   - Se l'endpoint è raggiungibile utilizzando le credenziali specificate, viene visualizzato un messaggio di

successo. La connessione all'endpoint viene verificata da un nodo in ciascun sito.

- Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Modifica l'endpoint per correggere l'errore, quindi seleziona **Test e salva le modifiche**.

Eliminare un endpoint dei servizi della piattaforma StorageGRID

Puoi eliminare un endpoint se non vuoi più usare il servizio della piattaforma associato.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Gestisci endpoint o autorizzazione di accesso root".

Passaggi

1. Seleziona **STORAGE (S3)** > **Platform services endpoints**.

   ${post_edited_translations.segment}

2. Seleziona la casella di controllo per ogni endpoint che desideri eliminare.

   Se elimini un endpoint dei servizi della piattaforma che è in uso, il servizio della piattaforma associato verrà disabilitato per tutti i bucket che utilizzano tale endpoint. Tutte le richieste non ancora completate verranno scartate. Le nuove richieste continueranno a essere generate finché non modifichi la configurazione del bucket in modo che non faccia più riferimento all'URN eliminato. StorageGRID segnalerà queste richieste come errori irreversibili.

3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

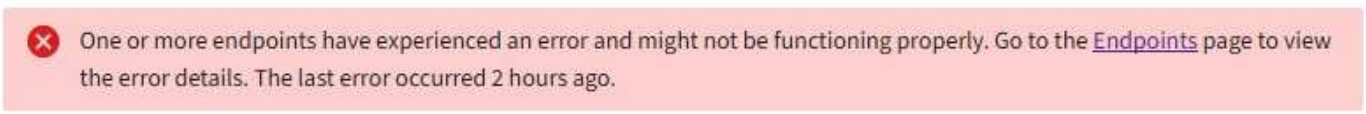
4. ${post_edited_translations.segment}

Risoluzione dei problemi relativi agli endpoint dei servizi della piattaforma StorageGRID

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi di piattaforma, viene visualizzato un messaggio sulla dashboard. Nella pagina Platform services endpoints, la colonna Last error indica quanto tempo fa si è verificato l'errore. Non viene visualizzato alcun errore se le autorizzazioni associate alle credenziali di un endpoint non sono corrette.

${post_edited_translations.segment}

Se si sono verificati errori degli endpoint dei servizi di piattaforma negli ultimi 7 giorni, la dashboard del Tenant Manager mostra un messaggio di avviso. Puoi andare alla pagina Endpoint dei servizi di piattaforma per visualizzare ulteriori dettagli sull'errore.



Lo stesso errore che compare nella dashboard appare anche nella parte superiore della pagina degli endpoint dei servizi della piattaforma. Per visualizzare un messaggio di errore più dettagliato:

Passaggi

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

${post_edited_translations.segment}

Alcuni errori potrebbero continuare a essere visualizzati nella colonna **Ultimo errore** anche dopo essere stati risolti. Per vedere se un errore è attuale o per forzare la rimozione di un errore risolto dalla tabella:

Passaggi

1. ${post_edited_translations.segment}

   Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Seleziona **Connessione** > **Test connessione**.

Selezionando **Test connection**, StorageGRID verifica che l'endpoint dei servizi di piattaforma esista e che sia raggiungibile con le credenziali correnti. La connessione all'endpoint viene verificata da un nodo in ciascun sito.

Risolvere gli errori degli endpoint

Puoi utilizzare il messaggio **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, può verificarsi un errore di CloudMirroring se StorageGRID non è in grado di accedere al bucket S3 di destinazione perché non dispone delle autorizzazioni di accesso corrette o la chiave di accesso è scaduta. Il messaggio è "È necessario aggiornare le credenziali dell'endpoint o l'accesso alla destinazione" e i dettagli sono "AccessDenied" o "InvalidAccessKeyId."

Se devi modificare l'endpoint per risolvere un errore, selezionando **Verifica e salva le modifiche** StorageGRID convalida l'endpoint aggiornato e conferma che è raggiungibile con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ciascun sito.

Passaggi

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Modifica la configurazione dell'endpoint secondo necessità.
4. Seleziona **Connessione** > **Test connessione**.

${post_edited_translations.segment}

Quando StorageGRID convalida un endpoint dei servizi della piattaforma, conferma che le credenziali dell'endpoint possano essere utilizzate per contattare la risorsa di destinazione ed esegue un controllo di base delle autorizzazioni. Tuttavia, StorageGRID non convalida tutte le autorizzazioni richieste per alcune operazioni dei servizi della piattaforma. Per questo motivo, se ricevi un errore quando provi a utilizzare un servizio della piattaforma (come "403 Forbidden"), controlla le autorizzazioni associate alle credenziali dell'endpoint.

Informazioni correlate

- "${post_edited_translations.segment}"
- "Crea un endpoint per i servizi della piattaforma"
- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"

Configura la replica CloudMirror in StorageGRID

Per abilitare la replica CloudMirror per un bucket, devi creare e applicare un file XML di configurazione valido per la replica del bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo tenant account da un amministratore di StorageGRID.
- Hai già creato un bucket che fungerà da origine di replica.
- L'endpoint che intendi utilizzare come destinazione per CloudMirror replication esiste già e ne possiedi l'URN.
- Appartieni a un gruppo di utenti che dispone delle "Gestisci tutti i bucket o autorizzazione di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o di bucket quando configuri il bucket tramite Tenant Manager.

Informazioni su questa attività

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

Per informazioni generali sulla replica dei bucket e su come configurarla, vedi "Documentazione di Amazon Simple Storage Service (S3): Replica degli oggetti". Per informazioni su come StorageGRID implementa GetBucketReplication, DeleteBucketReplication e PutBucketReplication, vedi il "Operazioni sui bucket".

CloudMirror replication presenta importanti somiglianze e differenze con la funzionalità di replica cross-grid. Per saperne di più, vedi "Confronta la replica cross-grid e la replica CloudMirror".

Nota i seguenti requisiti e caratteristiche quando configuri la replica CloudMirror:

- Quando crei e applichi un file XML di configurazione valido per la replica dei bucket, devi usare l'URN di un endpoint del bucket S3 per ogni destinazione.
- La replica non è supportata per i bucket di origine o di destinazione con S3 Object Lock abilitato.
- Se abiliti la replica CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket vengono replicati, ma gli oggetti già presenti nel bucket non vengono replicati. Devi aggiornare gli oggetti esistenti per attivare la replica.
- Se specifichi una classe di archiviazione nel file XML di configurazione della replica, StorageGRID utilizza quella classe quando esegue operazioni sull'endpoint S3 di destinazione. Anche l'endpoint di destinazione deve supportare la classe di archiviazione specificata. Assicurati di seguire tutte le raccomandazioni fornite dal fornitore del sistema di destinazione.

Passaggi

1. Abilita la replica per il tuo bucket di origine:
    - Utilizza un editor di testo per creare il file XML di configurazione della replica necessario per abilitare la replica, come specificato nell'API di replica di S3.

◦ Quando configuri l'XML:

- Tieni presente che StorageGRID supporta solo la V1 della configurazione di replica. Questo significa che StorageGRID non supporta l'uso dell'elemento `Filter` per le regole e segue le convenzioni della V1 per l'eliminazione delle versioni degli oggetti. Consulta la documentazione di Amazon sulla configurazione di replica per i dettagli.
- Usa l'URN di un endpoint di un bucket S3 come destinazione.
- Aggiungi facoltativamente l' `<StorageClass>` elemento e specifica uno dei seguenti:
  - `STANDARD`: La classe di archiviazione predefinita. Se non specifichi una classe di archiviazione quando carichi un oggetto, viene utilizzata la classe di archiviazione `STANDARD` predefinita.
  - `STANDARD_IA`: (Standard - accesso poco frequente.) Usa questa classe di archiviazione per i dati a cui accedi meno frequentemente, ma che richiedono comunque un accesso rapido quando necessario.
  - `REDUCED_REDUNDANCY`Usa questa classe di archiviazione per dati non critici e riproducibili che possono essere archiviati con meno ridondanza rispetto alla classe di archiviazione `STANDARD.
- Se specifichi un `Role` nel file di configurazione XML, 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. ${post_edited_translations.segment}
3. Seleziona il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Seleziona **Servizi della piattaforma** > **Replica**.
5. Seleziona la casella di controllo **Abilita replica**.
6. Incolla il file XML di configurazione della replica nella casella di testo e seleziona **Salva modifiche**.

   > I servizi della piattaforma devono essere abilitati per ogni tenant account da un amministratore StorageGRID utilizzando il Grid Manager o la Grid Management API. Contatta il tuo amministratore StorageGRID se si verifica un errore durante il salvataggio del file di configurazione XML.

7. Verifica che la replica sia configurata correttamente:

a. Aggiungi un oggetto al bucket di origine che soddisfi i requisiti per la replica come specificato nella configurazione di replica.

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

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

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

Informazioni correlate

"Crea un endpoint per i servizi della piattaforma"

Configura le notifiche degli eventi in StorageGRID

Puoi abilitare le notifiche per un bucket creando un file XML di configurazione delle notifiche e usando il Tenant Manager per applicare il file XML a un bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo tenant account da un amministratore di StorageGRID.
- Hai già creato un bucket che fungerà da origine delle notifiche.
- L'endpoint che intendi utilizzare come destinazione per le notifiche degli eventi esiste già e ne possiedi l'URN.
- Appartieni a un gruppo di utenti che dispone delle "Gestisci tutti i bucket o autorizzazione di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o di bucket quando configuri il bucket tramite Tenant Manager.

Informazioni su questa attività

Configuri le notifiche degli eventi associando un file XML di configurazione delle notifiche a un bucket di origine. Il file XML di configurazione delle notifiche segue le convenzioni S3 per la configurazione delle notifiche dei bucket, con la destinazione Amazon SNS topic, Kafka topic o endpoint webhook specificata come URN di un endpoint.

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

Nota i seguenti requisiti e caratteristiche quando configuri le notifiche di eventi per un bucket:

- Quando crei e applichi un file XML di configurazione delle notifiche valido, devi usare l'URN di un endpoint di notifiche degli eventi per ogni destinazione.
- Sebbene sia possibile configurare la notifica degli eventi su un bucket con S3 Object Lock abilitato, i metadati S3 Object Lock (inclusi Retain Until Date e Legal Hold status) degli oggetti non saranno inclusi nei messaggi di notifica.
- Dopo aver configurato le notifiche degli eventi, ogni volta che si verifica un evento specificato per un oggetto nel bucket di origine, viene generata una notifica e inviata all'argomento Amazon SNS, all'argomento Kafka o all'endpoint webhook utilizzato come destinazione.
- Se abiliti le notifiche degli eventi per un bucket che contiene oggetti, le notifiche vengono inviate solo per le azioni eseguite dopo il salvataggio della configurazione delle notifiche.

Passaggi

1. Abilita le notifiche per il tuo bucket di origine:
   - Utilizza un editor di testo per creare il file XML di configurazione delle notifiche necessario per abilitare le notifiche degli eventi, come specificato nell'API di notifica S3.
   - Durante la configurazione del file XML, usa l'URN di un endpoint di notifiche eventi come topic 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. Nel Tenant Manager, seleziona **STORAGE (S3)** > **Buckets**.
3. Seleziona il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Seleziona **Servizi della piattaforma** > **Notifiche eventi**.
5. Seleziona la casella di controllo **Abilita notifiche eventi**.
6. Incolla il file XML di configurazione delle notifiche nella casella di testo e seleziona **Salva modifiche**.

   I servizi della piattaforma devono essere abilitati per ogni tenant account da un amministratore StorageGRID utilizzando il Grid Manager o la Grid Management API. Contatta il tuo amministratore StorageGRID se si verifica un errore durante il salvataggio del file di configurazione XML.

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

   a. Esegui un'azione su un oggetto nel bucket di origine che soddisfa i requisiti per l'attivazione di una notifica come configurato nel file 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 una notifica sia stata recapitata all'argomento Amazon SNS di destinazione, all'argomento Kafka di destinazione o all'endpoint webhook di destinazione.

Ad esempio, se il tuo topic di destinazione è ospitato su Amazon SNS, puoi configurare il servizio per ricevere un'email quando la notifica viene recapitata.

```
{
   "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, hai configurato correttamente il bucket di origine per le notifiche StorageGRID.

Informazioni correlate

- "Comprendi le notifiche per i bucket"

- "${post_edited_translations.segment}"
- "Crea un endpoint per i servizi della piattaforma"

Configura il servizio di integrazione della ricerca in StorageGRID

Abiliti l'integrazione della ricerca per un bucket creando un file XML di integrazione della ricerca e usando Tenant Manager per applicare il file XML al bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo tenant account da un amministratore di StorageGRID.
- Hai già creato un bucket S3 di cui desideri indicizzare il contenuto.
- L'endpoint che intendi utilizzare come destinazione per il servizio di integrazione della ricerca esiste già e ne possiedi l'URN.
- Appartieni a un gruppo di utenti che dispone delle "Gestisci tutti i bucket o autorizzazione di accesso root". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o di bucket quando configuri il bucket tramite Tenant Manager.

Informazioni su questa attività

Dopo che hai 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 fa sì che i metadati dell'oggetto vengano inviati all'endpoint di destinazione.

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

Passaggi

1. Abilita l'integrazione della ricerca per un bucket:
    - Utilizza un editor di testo per creare il file XML di notifica dei metadati necessario per abilitare l'integrazione con la ricerca.
    - Durante la configurazione dell'XML, usa 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, puoi inviare metadati per oggetti con il prefisso `images` a una destinazione e metadati per 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 oggetti con il prefisso `test` e una seconda regola per oggetti con il prefisso `test2` non è consentita.

      Se necessario, fai riferimento a esempi per la configurazione dei metadati XML.

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

Elementi nel file XML di configurazione della notifica dei metadati:

Nome	Descrizione	Richiesto
MetadataNotificationConfiguration	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi Rule.	Sì
Regola	Etichetta contenitore 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	Identificativo univoco per la regola. Incluso nell'elemento Regola.	No
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Per le regole disabilitate non viene intrapresa alcuna azione. Incluso nell'elemento Regola.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per selezionare tutti gli oggetti, specifica un prefisso vuoto. Incluso nell'elemento Regola.	Sì
Destinazione	Etichetta contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	Sì

Nome	Descrizione	Richiesto
Urn	URN della destinazione a 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 il tipo in cui sono memorizzati i metadati, nel formato `domain-name/myindex/mytype`. Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. 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 del file XML di configurazione, altrimenti la configurazione fallirà con un errore 404. L'URN è incluso nell'elemento Destinazione.	Sì

2. Nel Tenant Manager seleziona **STORAGE (S3)** > **Buckets**.
3. Seleziona il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Seleziona **Servizi della piattaforma** > **Integrazione della ricerca**
5. Seleziona la casella di controllo **Abilita integrazione ricerca**.
6. Incolla la configurazione della notifica dei metadati nella casella di testo e seleziona **Salva modifiche**.

   > I servizi della piattaforma devono essere abilitati per ogni tenant account da un amministratore StorageGRID utilizzando il Grid Manager o la Management API. Contatta il tuo amministratore StorageGRID se si verifica un errore quando salvi il file XML di configurazione.

7. Verifica che il servizio di integrazione della ricerca sia configurato correttamente:
   a. Aggiungi un oggetto al bucket di origine che soddisfa i requisiti per attivare una notifica di metadati, come specificato nel file XML di configurazione.

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

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

Dopo aver finito

Se necessario, puoi disabilitare l'integrazione della ricerca per un bucket utilizzando uno dei seguenti metodi:

- Seleziona **STORAGE (S3)** > **Buckets** e deseleziona la casella di controllo **Enable search integration**.
- Se usi direttamente l'API S3, utilizza una richiesta di notifica dei metadati del bucket DELETE. Vedi le istruzioni per implementare le applicazioni client S3.

Esempio: configurazione di notifica dei metadati che si applica a tutti gli oggetti

In questo esempio, i metadati di 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 dei metadati con due regole

In questo esempio, i metadati degli oggetti che corrispondono al prefisso `/images` vengono inviati a una destinazione, mentre i metadati degli oggetti che corrispondono 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 abiliti il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato alla destinazione ogni volta che i metadati o i tag di un oggetto vengono aggiunti, aggiornati o eliminati.

Questo esempio mostra un esempio del JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. Il `test` bucket non è versionato, quindi il `versionId` tag è vuoto.

```
{
  "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 oggetto

`bucket`: Nome del bucket

`key`: Nome della chiave dell'oggetto

`versionID`: Versione dell'oggetto, per gli oggetti in bucket con versioning

`region`: Regione del bucket, per esempio `us-east-1`

Metadati di sistema

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

`md5`: Hash dell'oggetto

Metadati utente

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

`key:value`

Etichette

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

```
key:value
```

Come visualizzare i risultati in Elasticsearch

Per i tag e i metadati utente, StorageGRID trasmette date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo che interpreti queste stringhe come date o numeri, segui le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati data. Abilita le mappature dinamiche dei campi sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo che un documento è stato indicizzato, non puoi modificare i tipi di campo del documento nell'indice.

Informazioni sul copyright

Informazioni sul marchio commerciale