Gestisci gli endpoint dei servizi della piattaforma

StorageGRID software

NetApp
July 23, 2026

Sommario

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}

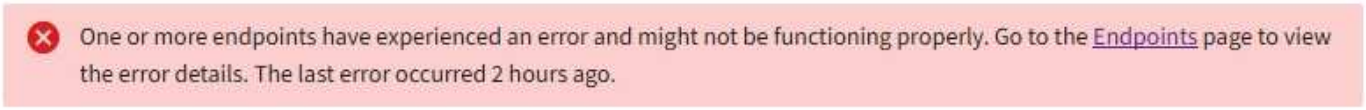
4. ${post_edited_translations.segment}

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}"

Informazioni sul copyright

Informazioni sul marchio commerciale