



Gestire gli endpoint dei servizi della piattaforma

StorageGRID software

NetApp
December 03, 2025

Sommario

Gestire gli endpoint dei servizi della piattaforma	1
Configurare gli endpoint dei servizi della piattaforma	1
Che cos'è un endpoint dei servizi di piattaforma?	1
Endpoint per la replica CloudMirror	1
Endpoint per le notifiche	1
Endpoint per il servizio di integrazione della ricerca	2
Specificare l'URN per l'endpoint dei servizi della piattaforma	2
Elementi URN	2
URN per servizi ospitati su AWS e GCP	3
URN per servizi ospitati localmente	3
Crea endpoint dei servizi della piattaforma	4
Prova la connessione per l'endpoint dei servizi della piattaforma	9
Modifica endpoint dei servizi della piattaforma	10
Elimina l'endpoint dei servizi della piattaforma	11
Risolvere gli errori degli endpoint dei servizi della piattaforma	12
Determina se si è verificato un errore	12
Controlla se l'errore è ancora attuale	12
Risolvi gli errori dell'endpoint	12
Credenziali dell'endpoint con autorizzazioni insufficienti	13

Gestire gli endpoint dei servizi della piattaforma

Configurare gli endpoint dei servizi della piattaforma

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

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

Che cos'è un endpoint dei servizi di piattaforma?

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

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

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

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

Endpoint per la replica CloudMirror

StorageGRID supporta endpoint di replica che rappresentano bucket S3. Questi bucket potrebbero essere ospitati su Amazon Web Services, sullo stesso o su una distribuzione StorageGRID remota, oppure su un altro servizio.

Endpoint per le notifiche

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

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

Endpoint per il servizio di integrazione della ricerca

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

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

Informazioni correlate

["Amministra StorageGRID"](#)

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

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

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

Elementi URN

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

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

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

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

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

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

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

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

URN per servizi ospitati su AWS e GCP

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

- Replica CloudMirror:

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

- Notifiche:

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

- Integrazione della ricerca:

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



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

URN per servizi ospitati localmente

Quando si utilizzano servizi ospitati localmente anziché servizi cloud, è possibile specificare l'URN in qualsiasi modo che crei un URN valido e univoco, purché l'URN includa gli elementi richiesti nella terza e ultima posizione. È possibile lasciare vuoti gli elementi indicati come facoltativi oppure specificarli in qualsiasi modo che aiuti a identificare la risorsa e a rendere univoco l'URN. Per esempio:

- Replica CloudMirror:

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

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

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

- Notifiche:

Specificare un endpoint Amazon Simple Notification Service:

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

Specificare un endpoint Kafka:

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

- Integrazione della ricerca:

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



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

Crea endpoint dei servizi della piattaforma

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

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore StorageGRID .
- 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:
 - Replica CloudMirror: bucket S3
 - Notifica evento: Amazon Simple Notification Service (Amazon SNS) o argomento Kafka
 - Notifica di ricerca: indice Elasticsearch, se il cluster di destinazione non è configurato per creare automaticamente indici.
- Hai le informazioni sulla risorsa di destinazione:
 - Host e porta per l'Uniform Resource Identifier (URI)



Se si prevede di utilizzare un bucket ospitato su un sistema StorageGRID come endpoint per la replica CloudMirror, contattare l'amministratore della griglia per determinare i valori da immettere.

- Nome univoco della risorsa (URN)

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

- Credenziali di autenticazione (se richieste):

Cerca endpoint di integrazione

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

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

Endpoint di replicazione CloudMirror

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

- Chiave di accesso: ID 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 utilizzare le seguenti credenziali:

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

Punti finali di 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 si utilizza un certificato CA personalizzato)
- Se le funzionalità di sicurezza di Elasticsearch sono abilitate, si dispone del privilegio di monitoraggio del cluster per i test di connettività e del privilegio di scrittura dell'indice oppure di entrambi i privilegi di indice ed eliminazione dell'indice per gli aggiornamenti dei documenti.

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Endpoint dei servizi di piattaforma**. Viene visualizzata la pagina Endpoint dei servizi della piattaforma.
2. Selezionare **Crea endpoint**.
3. Immettere un nome visualizzato per descrivere brevemente l'endpoint e il suo scopo.

Il tipo di servizio di piattaforma supportato dall'endpoint viene visualizzato accanto al nome dell'endpoint quando è elencato nella pagina Endpoint, quindi non è necessario includere tale informazione nel nome.

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

Utilizzare uno dei seguenti formati:

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

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

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

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

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

In questo esempio, `s3.example.com` rappresenta la voce DNS per l'IP virtuale (VIP) del gruppo ad alta disponibilità (HA) StorageGRID e 10443 rappresenta la porta definita nell'endpoint del bilanciatore del carico.



Se possibile, è opportuno connettersi a un gruppo HA di nodi di bilanciamento del carico per evitare un singolo punto di errore.

Allo stesso modo, 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. Inserisci il nome del bucket nel campo **URN**.

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



Non è possibile modificare l'URN di un endpoint dopo averlo creato.

6. Selezionare **Continua**.

7. Selezionare un valore per **Tipo di autenticazione**.

Cerca endpoint di integrazione

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

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con 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 replicazione CloudMirror

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

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con 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 (portale di accesso C2S)	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) • Passphrase della chiave privata del client (facoltativa)

Endpoint Amazon SNS

Inserisci o carica le credenziali per un endpoint Amazon SNS.

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con 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

Punti finali di Kafka

Inserisci o carica le credenziali per un endpoint Kafka.

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
SASL/PLAIN	Utilizza un nome utente e una password con testo normale per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-256	Utilizza un nome utente e una password tramite un protocollo challenge-response e l'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 challenge-response e l'hashing SHA-512 per autenticare le connessioni alla destinazione.	• Nome utente • Password

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

8. Selezionare **Continua**.

9. Selezionare un pulsante di opzione per **Verifica server** per scegliere come verificare la connessione TLS all'endpoint.

Tipo di verifica del certificato	Descrizione
Utilizza un certificato CA personalizzato	Utilizzare un certificato di sicurezza personalizzato. Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo Certificato CA .
Utilizzare il certificato CA del sistema operativo	Per proteggere le connessioni, utilizzare il certificato Grid CA predefinito installato sul sistema operativo.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non è verificato. Questa opzione non è sicura.

10. Selezionare **Test e crea endpoint**.

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



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

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

Informazioni correlate

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

Prova la connessione per l'endpoint dei servizi della piattaforma

Se la connessione a un servizio della piattaforma è cambiata, è possibile testare la connessione per l'endpoint per convalidare che la risorsa di destinazione esista e che possa essere raggiunta utilizzando le credenziali specificate.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti che ha il ["Gestisci endpoint o autorizzazione di accesso root"](#) .

Informazioni su questo compito

StorageGRID non convalida che le credenziali abbiano le autorizzazioni corrette.

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Endpoint dei servizi di piattaforma**.

Viene visualizzata la pagina Endpoint dei servizi di piattaforma, che mostra l'elenco degli endpoint dei servizi di piattaforma già configurati.

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

Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Test connessione**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di operazione riuscita. La connessione all'endpoint viene convalidata da un nodo in ogni sito.
- Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Se è necessario modificare l'endpoint per correggere l'errore, selezionare **Configurazione** e aggiornare le informazioni. Quindi, seleziona **Testa e salva modifiche**.

Modifica endpoint dei servizi della piattaforma

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

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Gestisci endpoint o autorizzazione di accesso root"](#).

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Endpoint dei servizi di piattaforma**.

Viene visualizzata la pagina Endpoint dei servizi di piattaforma, che mostra l'elenco degli endpoint dei servizi di piattaforma già configurati.

2. Seleziona l'endpoint che vuoi modificare.

Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Configurazione**.

4. Se necessario, modificare la configurazione dell'endpoint.



Non è possibile modificare l'URN di un endpoint dopo averlo creato.

- a. Per modificare il nome visualizzato per l'endpoint, seleziona l'icona di modifica .
- b. Se necessario, modificare l'URI.
- c. Se necessario, modificare il tipo di autenticazione.

- Per l'autenticazione con chiave di accesso, modificare la chiave secondo necessità selezionando **Modifica chiave S3** e incollando un nuovo ID chiave di accesso e una chiave di accesso segreta. Se devi annullare le modifiche, seleziona **Annulla modifica chiave S3**.
- Per l'autenticazione CAP (C2S Access Portal), modificare l'URL delle credenziali temporanee o la passphrase della chiave privata del client facoltativa e caricare nuovi file di certificato e chiave secondo necessità.



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

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

5. Seleziona **Testa e salva le modifiche**.

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

Elimina l'endpoint dei servizi della piattaforma

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

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha il ["Gestisci endpoint o autorizzazione di accesso root"](#).

Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Endpoint dei servizi di piattaforma**.

Viene visualizzata la pagina Endpoint dei servizi di piattaforma, che mostra l'elenco degli endpoint dei servizi di piattaforma già configurati.

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



Se si elimina un endpoint dei servizi di piattaforma in uso, il servizio di piattaforma associato verrà disabilitato per tutti i bucket che utilizzano l'endpoint. Tutte le richieste non ancora completate verranno eliminate. Tutte 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 irrecuperabili.

3. Selezionare **Azioni > Elimina endpoint**.

Appare un messaggio di conferma.

4. Selezionare **Elimina endpoint**.

Risolvere gli errori degli endpoint dei servizi della piattaforma

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi della piattaforma, viene visualizzato un messaggio nella dashboard. Nella pagina Endpoint dei servizi della piattaforma, la colonna Ultimo errore indica da quanto tempo si è verificato l'errore. Se le autorizzazioni associate alle credenziali di un endpoint sono errate, non viene visualizzato alcun errore.

Determina se si è verificato un errore

Se negli ultimi 7 giorni si sono verificati errori degli endpoint dei servizi della piattaforma, la dashboard di Tenant Manager visualizza un messaggio di avviso. Per maggiori dettagli sull'errore, puoi andare alla pagina Endpoint dei servizi della piattaforma.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

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

Passi

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

Controlla se l'errore è ancora attuale

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

Passi

1. Selezionare l'endpoint.

Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Selezionare **Connessione** > **Test connessione**.

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

Risolvi gli errori dell'endpoint

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

Passi

1. Selezionare l'endpoint.
2. Nella pagina dei dettagli dell'endpoint, seleziona **Configurazione**.
3. Modificare la configurazione dell'endpoint secondo necessità.
4. Selezionare **Connessione > Test connessione**.

Credenziali dell'endpoint con autorizzazioni insufficienti

Quando StorageGRID convalida un endpoint dei servizi della piattaforma, conferma che le credenziali dell'endpoint possono 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 determinate operazioni dei servizi della piattaforma. Per questo motivo, se si riceve un errore quando si tenta di utilizzare un servizio della piattaforma (ad esempio "403 Forbidden"), verificare le autorizzazioni associate alle credenziali dell'endpoint.

Informazioni correlate

- [Amministra StorageGRID > Risolvi i problemi dei servizi della piattaforma](#)
- ["Crea endpoint dei servizi della piattaforma"](#)
- ["Prova la connessione per l'endpoint dei servizi della piattaforma"](#)
- ["Modifica endpoint dei servizi della piattaforma"](#)

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.