Utilizzare un account tenant

StorageGRID software

NetApp
February 12, 2026

Sommario

Utilizzare un account tenant . . . 1
- Utilizzare un account tenant . . . 1
  - Che cos'è un account tenant? . . . 1
  - Come creare un account tenant . . . 1
- Come effettuare l'accesso e disconnettersi . . . 2
  - Accedi a Tenant Manager . . . 2
  - Disconnettersi da Tenant Manager . . . 3
- Comprendere la dashboard di Tenant Manager . . . 4
  - Informazioni sull'account tenant . . . 5
  - Utilizzo dello storage e delle quote . . . 5
  - Avvisi sull'utilizzo delle quote . . . 6
    - utilizzo limite di capacità . . . 7
  - Errori degli endpoint . . . 7
- API di gestione del tenant . . . 7
  - Comprendere l'API di gestione dei tenant . . . 7
  - Versione dell'API di gestione tenant . . . 10
  - Protezione contro la contraffazione delle richieste (CSRF) . . . 11
- Utilizzare connessioni di federazione di griglie . . . 12
  - Clonare utenti e gruppi tenant . . . 12
  - Clonare le chiavi di accesso S3 utilizzando l'API . . . 17
  - Gestire la replica cross-grid . . . 19
  - Visualizza connessioni di federazione di griglie . . . 24
- Gestire gruppi e utenti . . . 26
  - USA la federazione delle identità . . . 26
  - Gestire i gruppi di tenant . . . 31
  - Gestire gli utenti . . . 39
- Gestire le chiavi di accesso S3 . . . 44
  - Gestire le chiavi di accesso S3 . . . 44
  - Creare le proprie chiavi di accesso S3 . . . 44
  - Visualizzare le chiavi di accesso S3 . . . 46
  - Eliminare le proprie chiavi di accesso S3 . . . 46
  - Creare le chiavi di accesso S3 di un altro utente . . . 47
  - Visualizzare le chiavi di accesso S3 di un altro utente . . . 48
  - Eliminare le chiavi di accesso S3 di un altro utente . . . 49
- Gestire i bucket S3 . . . 49
  - Creare un bucket S3 . . . 49
  - Visualizza i dettagli del bucket . . . 53
  - Cos'è un branch bucket? . . . 55
  - Gestisci i bucket delle filiali . . . 57
  - Applicare un tag di criterio ILM a un bucket . . . 60
  - Gestire le policy del bucket . . . 61
  - Gestire la coerenza del bucket . . . 62
  - Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso . . . 64

Modificare la versione degli oggetti per un bucket . . . 66
USA il blocco oggetti S3 per conservare gli oggetti . . . 67
Aggiorna la conservazione predefinita del blocco oggetti S3 . . . 71
Configurare StorageGRID CORS per bucket e oggetti . . . 72
Eliminare gli oggetti nel bucket . . . 74
Elimina bucket S3 . . . 77
Utilizzare la console S3 . . . 78
Gestire i servizi della piattaforma S3 . . . 79
Servizi della piattaforma S3 . . . 80
Gestire gli endpoint dei servizi della piattaforma . . . 87
Configurare la replica di CloudMirror . . . 102
Configurare le notifiche degli eventi . . . 104
Configurare il servizio di integrazione della ricerca . . . 108

Utilizzare un account tenant

Utilizzare un account tenant

Un account tenant consente di utilizzare l'API REST S3 (Simple Storage Service) per memorizzare e recuperare gli oggetti in un sistema StorageGRID.

Che cos'è un account tenant?

Ogni account tenant ha i propri gruppi, utenti, bucket S3 e oggetti federati o locali.

Gli account tenant possono essere utilizzati per separare gli oggetti memorizzati da diverse entità. Ad esempio, è possibile utilizzare più account tenant per uno dei seguenti casi di utilizzo:

- **Caso d'utilizzo aziendale:** se il sistema StorageGRID viene utilizzato all'interno di un'azienda, lo storage a oggetti del grid potrebbe essere separato dai diversi reparti dell'organizzazione. Ad esempio, potrebbero essere presenti account tenant per il reparto Marketing, il reparto Assistenza clienti, il reparto risorse umane e così via.

  > Se si utilizza il protocollo client S3, è possibile utilizzare anche i bucket S3 e i criteri dei bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario creare account tenant separati. Vedi le istruzioni per l'implementazione"Bucket S3 e policy bucket" per maggiori informazioni.

- **Caso d'utilizzo del provider di servizi:** se il sistema StorageGRID viene utilizzato da un provider di servizi, lo storage a oggetti della griglia potrebbe essere separato dalle diverse entità che affittano lo storage. Ad esempio, potrebbero essere presenti account tenant per la società A, la società B, la società C e così via.

Come creare un account tenant

Gli account tenant vengono creati da un "Amministratore della griglia di StorageGRID che utilizza il gestore della griglia". Quando si crea un account tenant, l'amministratore della griglia specifica quanto segue:

- Informazioni di base, tra cui nome del tenant, tipo di client (S3) e quota di archiviazione opzionale.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine di identità, utilizzare S3 Select o utilizzare una connessione a federazione di griglie.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione di identità o SSO (Single Sign-on).

Inoltre, gli amministratori della griglia possono attivare l'impostazione blocco oggetti S3 per il sistema StorageGRID se gli account tenant S3 devono soddisfare i requisiti normativi. Quando S3 Object Lock è attivato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

Configurare i tenant S3

Dopo un "Viene creato l'account tenant S3", è possibile accedere a Tenant Manager per eseguire attività quali:

- Configurare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia)

- Gestire gruppi e utenti
- Utilizza la federazione di grid per il clone dell'account e la replica cross-grid
- Gestire le chiavi di accesso S3
- Creare e gestire i bucket S3
- Utilizzare i servizi della piattaforma S3
- USA S3 Select
- Monitorare l'utilizzo dello storage

Anche se è possibile creare e gestire bucket S3 con Tenant Manager, è necessario utilizzare un "Client S3" oppure "S3 Console" per acquisire e gestire gli oggetti.

Come effettuare l'accesso e disconnettersi

Accedi a Tenant Manager

È possibile accedere a Tenant Manager immettendo l'URL del tenant nella barra degli indirizzi di un "browser web supportato".

Prima di iniziare

- Si dispone delle credenziali di accesso.
- Si dispone di un URL per accedere a Tenant Manager, fornito dall'amministratore della griglia. L'URL sarà simile a uno dei seguenti esempi:

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

  https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
  ```

  L'URL include sempre un nome di dominio completo (FQDN), l'indirizzo IP di un nodo amministrativo o l'indirizzo IP virtuale di un gruppo ha di nodi amministrativi. Potrebbe anche includere un numero di porta, l'ID dell'account tenant a 20 cifre o entrambi.

- Se l'URL non include l'ID account a 20 cifre del tenant, si dispone di questo ID account.
- Si sta utilizzando un "browser web supportato".
- I cookie sono attivati nel browser Web.
- L'utente appartiene a un gruppo di utenti che dispone di "autorizzazioni di accesso specifiche".

Fasi

1. Avviare un "browser web supportato".
2. Nella barra degli indirizzi del browser, immettere l'URL per accedere a Tenant Manager.
3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser.

4. Accedi al tenant manager.

   La schermata di accesso che viene visualizzata dipende dall'URL immesso e dalla configurazione di SSO (Single Sign-on) per StorageGRID.

   Non si utilizza SSO

   Se StorageGRID non utilizza SSO, viene visualizzata una delle seguenti schermate:

   - Pagina di accesso a Grid Manager. Selezionare il collegamento **accesso tenant**.
   - La pagina di accesso del Tenant Manager. Il campo **Account** potrebbe essere già compilato.
     i. Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.
     ii. Immettere il nome utente e la password.
     iii. Selezionare **Accedi**.

     Viene visualizzata la dashboard di Tenant Manager.

     iv. Se hai ricevuto una password iniziale da un altro utente, seleziona ***Username*** > **Change password** per proteggere il tuo account.

   Utilizzo di SSO

   Se StorageGRID utilizza SSO, viene visualizzata una delle seguenti schermate:

   - La pagina SSO della tua organizzazione.

     Immettere le credenziali SSO standard e selezionare **Accedi**.

   - La pagina di accesso SSO di Tenant Manager.
     i. Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.
     ii. Selezionare **Accedi**.
     iii. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

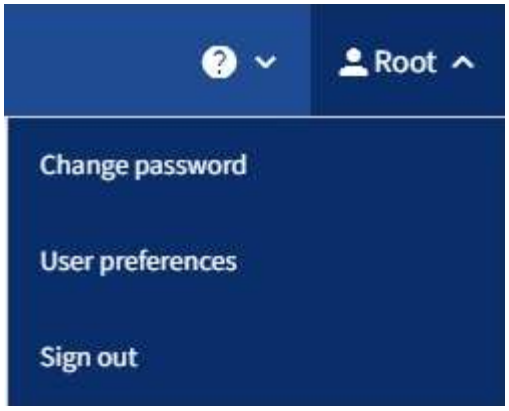
     Viene visualizzata la dashboard di Tenant Manager.

Disconnettersi da Tenant Manager

Una volta terminato il lavoro con il tenant manager, devi disconnetterti per garantire che gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnettersi dal sistema, in base alle impostazioni dei cookie del browser.

Fasi

1. Individuare il menu a discesa Username (Nome utente) nell'angolo in alto a destra dell'interfaccia utente.



2. Selezionare il nome utente, quindi selezionare **Disconnetti**.

   - Se SSO non è in uso:

     Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso del tenant manager.

     > Se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.

   - Se SSO è attivato:

     Si è disconnessi da tutti i nodi di amministrazione ai quali si stava accedendo. Viene visualizzata la pagina di accesso a StorageGRID. Il nome dell'account tenant a cui hai appena effettuato l'accesso viene elencato come predefinito nell'elenco a discesa **account recenti** e viene visualizzato l'ID account* del tenant.

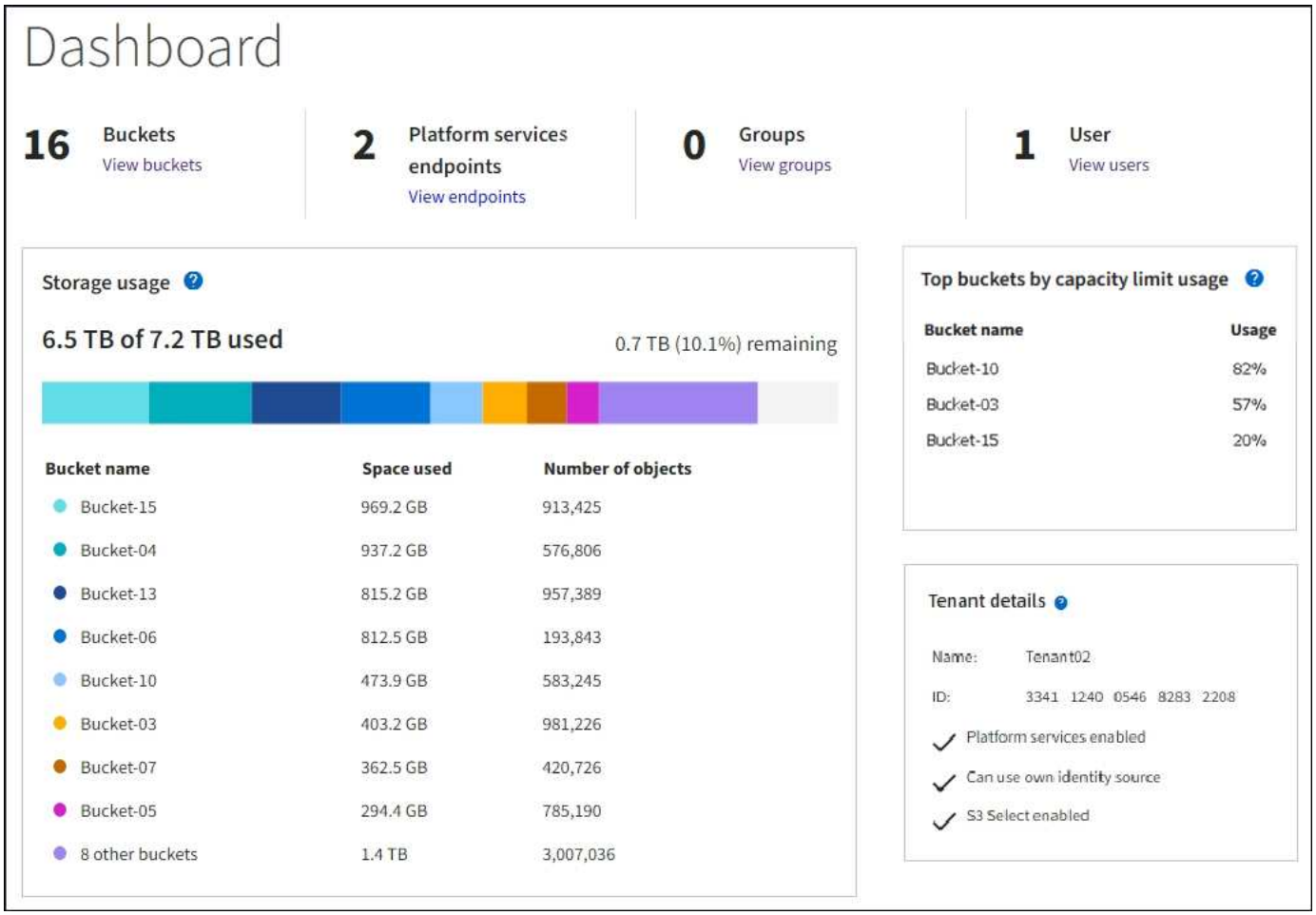
> Se SSO è attivato e si è anche connessi a Grid Manager, è necessario disconnettersi da Grid Manager per disconnettersi da SSO.

Comprendere la dashboard di Tenant Manager

La dashboard di Tenant Manager fornisce una panoramica della configurazione di un account tenant e della quantità di spazio utilizzata dagli oggetti nei bucket S3 del tenant. Se il tenant ha una quota, la dashboard mostra quanta quota è utilizzata e quanta ne rimane. Se si verificano errori relativi all'account del tenant, gli errori vengono visualizzati nella dashboard.

> La dimensione logica di tutti gli oggetti appartenenti a questo tenant include caricamenti multiparte incompleti e in corso. Le dimensioni non includono lo spazio fisico aggiuntivo utilizzato per le policy ILM. I valori dello spazio utilizzato sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo.

Una volta caricati gli oggetti, la dashboard è simile al seguente esempio:



Informazioni sull'account tenant

Nella parte superiore della dashboard viene indicato il numero di bucket o container configurati, gruppi e utenti. Visualizza inoltre il numero di endpoint dei servizi di piattaforma, se configurati. Selezionare i collegamenti per visualizzare i dettagli.

A seconda delle "autorizzazioni di gestione tenant"opzioni configurate e del tipo di dispositivo in uso, il resto della dashboard visualizza diverse combinazioni di linee guida, utilizzo dello storage, informazioni sugli oggetti e dettagli del tenant.

Utilizzo dello storage e delle quote

Il pannello Storage Use (utilizzo storage) contiene le seguenti informazioni:

- La quantità di dati oggetto per il tenant.

  Questo valore indica la quantità totale di dati dell'oggetto caricati e non rappresenta lo spazio utilizzato per memorizzare le copie di tali oggetti e dei relativi metadati.

- Se viene impostata una quota, la quantità totale di spazio disponibile per i dati dell'oggetto e la quantità e la percentuale di spazio rimanente. La quota limita la quantità di dati oggetto che è possibile acquisire.

L'utilizzo delle quote si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID controlla la quota quando un tenant avvia il caricamento degli oggetti e rifiuta le nuove ricerche se il tenant ha superato la quota. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente quando determina se la quota è stata superata. Se gli oggetti vengono eliminati, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti fino a quando l'utilizzo della quota non viene ricalcolato. I calcoli relativi all'utilizzo delle quote possono richiedere 10 minuti o più.

- Un grafico a barre che rappresenta le dimensioni relative dei bucket o dei container più grandi.

  È possibile posizionare il cursore su uno dei segmenti del grafico per visualizzare lo spazio totale consumato da quel bucket o container.

- Per corrispondere al grafico a barre, un elenco dei bucket o container più grandi, inclusa la quantità totale di dati oggetto e il numero di oggetti per ciascun bucket o container.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

  Se il tenant ha più di nove bucket o container, tutti gli altri bucket o container vengono combinati in una singola voce in fondo all'elenco.

Per modificare le unità per i valori di storage visualizzati in Tenant Manager, selezionare il menu a discesa User (utente) in alto a destra in Tenant Manager, quindi selezionare **User preferences** (Preferenze utente).

Avvisi sull'utilizzo delle quote

Se gli avvisi sull'utilizzo delle quote sono stati attivati in Grid Manager, questi avvisi vengono visualizzati in Tenant Manager quando la quota è bassa o superata, come segue:

- Se è stato utilizzato il 90% o più della quota di un tenant, viene attivato l'avviso **quota di utilizzo elevata del tenant**.

  Chiedere all'amministratore di rete di aumentare la quota.

- Se si supera la quota, una notifica informa che non è possibile caricare nuovi oggetti.

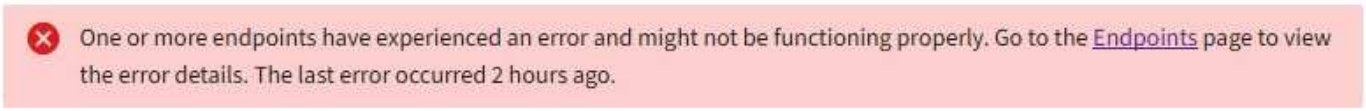
utilizzo limite di capacità

Se hai impostato un limite di capacità per i tuoi bucket, la dashboard di Tenant Manager visualizza un elenco dei bucket principali per utilizzo limite di capacità.

Se non viene impostato alcun limite per una benna, la sua capacità è illimitata. Tuttavia, se l'account tenant dispone di una quota di storage totale e tale quota viene raggiunta, non sarà possibile acquisire più oggetti indipendentemente dal limite di capacità rimanente in un bucket.

Errori degli endpoint

Se hai utilizzato Grid Manager per configurare uno o più endpoint da utilizzare con i servizi della piattaforma, la dashboard di Tenant Manager visualizza un avviso se si sono verificati errori degli endpoint negli ultimi sette giorni.



Per "errori degli endpoint dei servizi della piattaforma"visualizzare i dettagli su , selezionare **punti finali** per visualizzare la pagina punti finali.

API di gestione del tenant

Comprendere l'API di gestione dei tenant

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Tenant Management invece dell'interfaccia utente di Tenant Manager. Ad esempio, è possibile utilizzare l'API per automatizzare le operazioni o creare più entità, ad esempio gli utenti, più rapidamente.

L'API di gestione dei tenant:

- Utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di interagire con l'API. L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.
- Usi "versione per supportare aggiornamenti senza interruzioni".

Per accedere alla documentazione Swagger per l'API di gestione tenant:

1. Accedi al tenant manager.
2. Nella parte superiore di Tenant Manager, selezionare l'icona della guida e selezionare **documentazione API**.

Operazioni API

L'API di gestione tenant organizza le operazioni API disponibili nelle seguenti sezioni:

- **Account**: Operazioni sull'account tenant corrente, incluso il recupero delle informazioni sull'utilizzo dello storage.
- **Auth**: Operazioni per l'autenticazione della sessione utente.

  L'API di gestione tenant supporta lo schema di autenticazione del token del bearer. Per un accesso tenant, è necessario fornire un nome utente, una password e un ID account nel corpo JSON della richiesta di autenticazione (ovvero, `POST /api/v3/authorize`). Se l'utente viene autenticato correttamente, viene restituito un token di sicurezza. Questo token deve essere fornito nell'intestazione delle richieste API successive ("autorizzazione: Token portante").

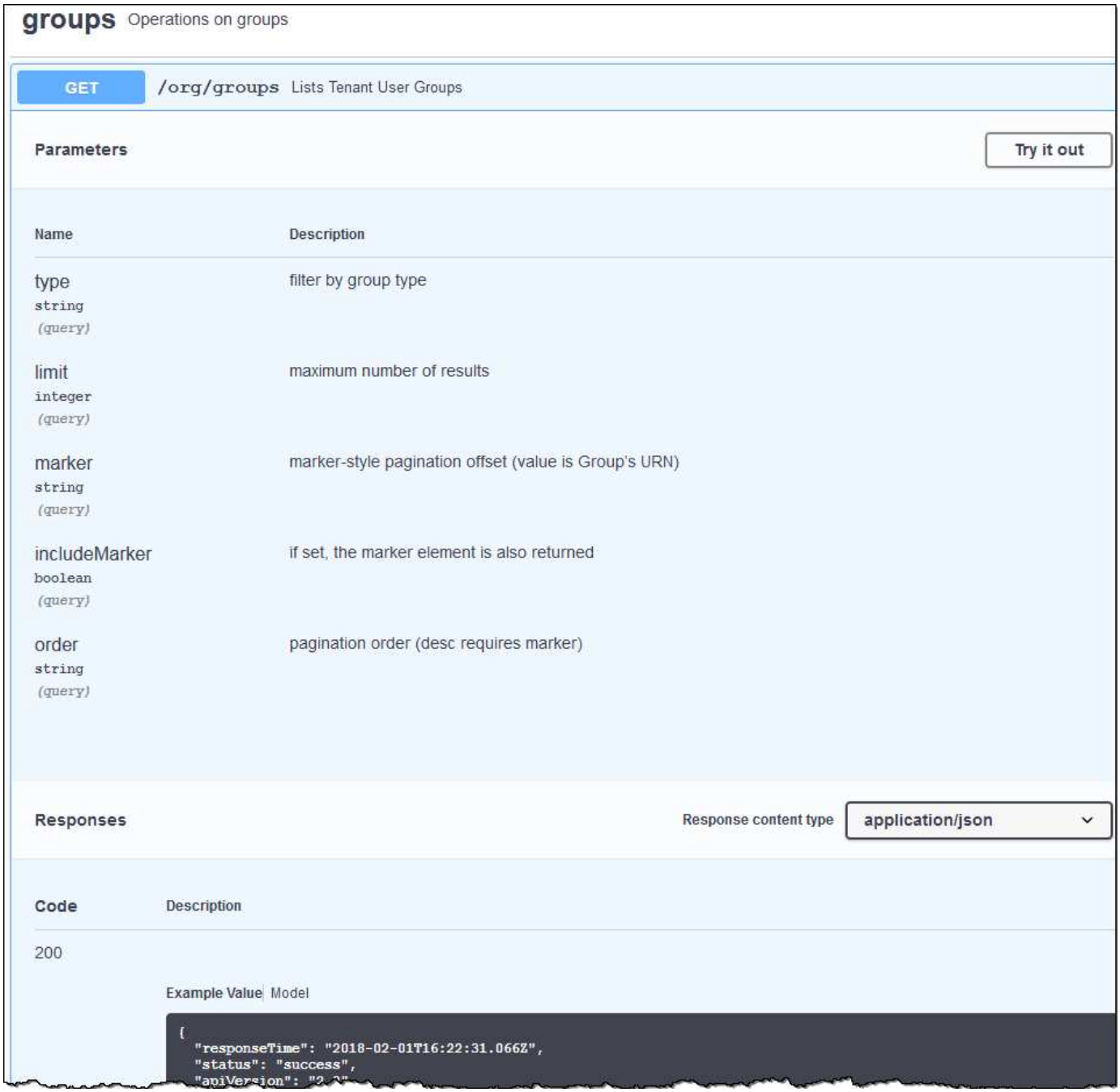
  Per informazioni sul miglioramento della protezione dell'autenticazione, vedere "Protezione contro la falsificazione di richieste cross-site".

  > Se per il sistema StorageGRID è attivato il Single Sign-on (SSO), è necessario eseguire diversi passaggi per l'autenticazione. Consultare la "Istruzioni per l'utilizzo dell'API Grid Management".

- **Config**: Operazioni relative alla release del prodotto e alle versioni dell'API di gestione tenant. È possibile elencare la versione di release del prodotto e le principali versioni dell'API supportate da tale release.
- **contenitori**: operazioni sui bucket S3.
- **Disattivato-funzioni**: Operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **Endpoint**: Operazioni per gestire un endpoint. Gli endpoint consentono a un bucket S3 di utilizzare un servizio esterno per la replica, le notifiche o l'integrazione della ricerca di StorageGRID CloudMirror.
- **Grid-Federation-Connections**: Operazioni su connessioni di federazione di grid e replica cross-grid.
- **Groups**: Operazioni per gestire gruppi tenant locali e recuperare gruppi tenant federati da un'origine di identità esterna.
- **Identity-source**: Operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm**: Operazioni sulle impostazioni ILM (Information Lifecycle Management).
- **Regioni**: Operazioni per determinare quali regioni sono state configurate per il sistema StorageGRID.
- **s3**: Operazioni per gestire le chiavi di accesso S3 per gli utenti del tenant.
- **s3-Object-lock**: Operazioni sulle impostazioni globali S3 Object Lock, utilizzate per supportare la conformità alle normative.
- **Utenti**: Operazioni per visualizzare e gestire gli utenti del tenant.

Dettagli dell'operazione

Quando si espandono le operazioni API, è possibile visualizzare l'azione HTTP, l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.



Emettere richieste API

> Tutte le operazioni API eseguite utilizzando la pagina Web documentazione API sono operazioni in tempo reale. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Fasi

1. Selezionare l'azione HTTP per visualizzare i dettagli della richiesta.
2. Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.
3. Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, è possibile selezionare **modello** per conoscere i requisiti di ciascun campo.

4. Selezionare **Provalo**.
5. Fornire i parametri richiesti o modificare il corpo della richiesta secondo necessità.
6. Selezionare **Esegui**.
7. Esaminare il codice di risposta per determinare se la richiesta ha avuto esito positivo.

Versione dell'API di gestione tenant

L'API di gestione tenant utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

`https://hostname_or_ip_address/api/v4/authorize`

La versione principale dell'API viene modificata quando vengono apportate modifiche che sono *non compatibili* con le versioni precedenti. La versione secondaria dell'API viene modificata quando vengono apportate modifiche che sono *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o di nuove proprietà.

Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene attivata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova release di funzionalità di StorageGRID, si continua ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.

> È possibile configurare le versioni supportate. Per ulteriori informazioni, vedere la sezione **config** della documentazione Swagger API"API di Grid Management". È necessario disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API per utilizzare la versione più recente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinare quali versioni API sono supportate nella release corrente

Utilizzare la `GET /versions` richiesta API per restituire un elenco delle versioni principali dell'API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione API utilizzando un parametro di percorso (`/api/v4`) o un'intestazione)(`Api-Version: 4`. Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protezione contro la contraffazione delle richieste (CSRF)

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

Per attivare la funzione, impostare il `csrfToken` parametro su `true` durante l'autenticazione. L'impostazione predefinita è `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando true, un `GridCsrfToken` cookie viene impostato con un valore casuale per i login al Grid Manager e il `AccountCsrfToken` cookie viene impostato con un valore casuale per i login al Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere una delle seguenti opzioni:

- L' `X-Csrf-Token`intestazione, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo codificato in forma: Un `csrfToken` parametro del corpo della richiesta codificato in forma.

Per configurare la protezione CSRF, utilizzare "API di Grid Management"o "API di gestione del tenant".

> Le richieste che dispongono di un set di cookie token CSRF applicheranno anche l'intestazione "Content-Type: Application/json" per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare connessioni di federazione di griglie

Clonare utenti e gruppi tenant

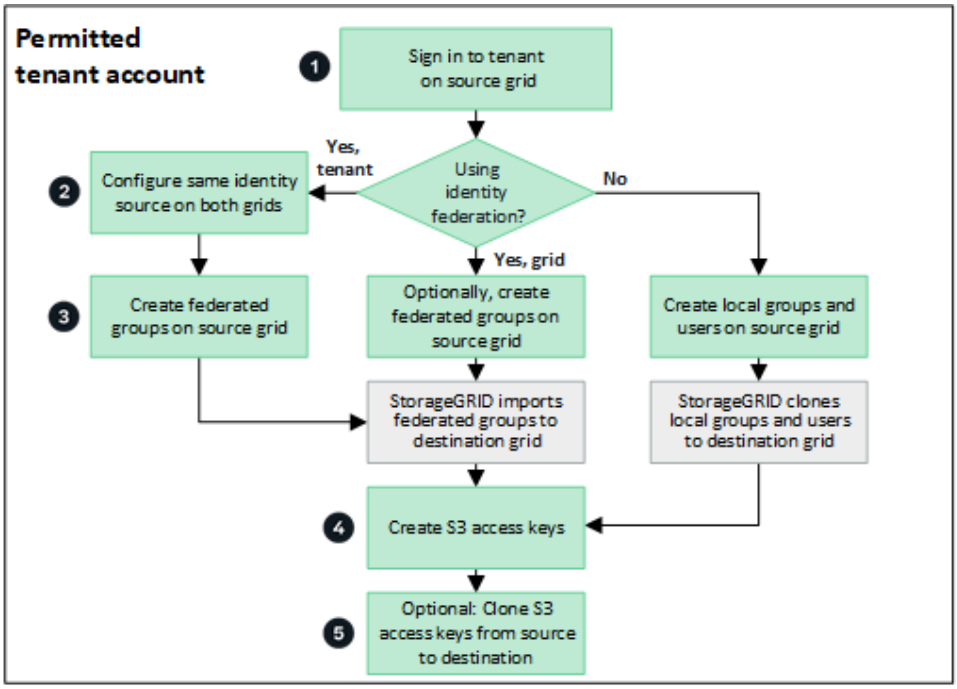
Se un tenant è stato creato o modificato per utilizzare una connessione federazione grid, tale tenant viene replicato da un sistema StorageGRID (il tenant di origine) a un altro sistema StorageGRID (il tenant di replica). Dopo la replica del tenant, tutti i gruppi e gli utenti aggiunti al tenant di origine vengono clonati sul tenant di replica.

Il sistema StorageGRID in cui il tenant viene originariamente creato è la *griglia di origine* del tenant. Il sistema StorageGRID in cui viene replicato il tenant è la *griglia di destinazione* del tenant. Entrambi gli account tenant hanno lo stesso ID account, nome, descrizione, quota di storage e autorizzazioni assegnate, tuttavia, il tenant di destinazione non dispone inizialmente di una password utente root. Per ulteriori informazioni, vedere "Cos'è il clone dell'account" e "Gestire i tenant autorizzati".

Il cloning delle informazioni dell'account tenant è necessario per "replica cross-grid" degli oggetti bucket. Avere gli stessi gruppi di tenant e gli stessi utenti su entrambe le griglie garantisce l'accesso ai bucket e agli oggetti corrispondenti su entrambe le griglie.

Workflow del tenant per il clone dell'account

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, consultare il diagramma del flusso di lavoro per visualizzare i passaggi che verranno eseguiti per clonare gruppi, utenti e chiavi di accesso S3.



Questi sono i passaggi principali del flusso di lavoro:

1 Accedere al tenant

Accedere all'account tenant sulla griglia di origine (la griglia in cui è stato creato il tenant).

2 Facoltativamente, configurare la federazione delle identità

Se l'account tenant dispone dell'autorizzazione **Usa origine identità propria** per utilizzare utenti e gruppi federati, configurare la stessa origine identità (con le stesse impostazioni) per gli account tenant di origine e di destinazione. I gruppi federati e gli utenti non possono essere clonati a meno che entrambe le griglie non utilizzino la stessa origine di identità. Per istruzioni, vedere "USA la federazione delle identità".

3 Creare gruppi e utenti

Quando si creano gruppi e utenti, iniziare sempre dalla griglia di origine del tenant. Quando si aggiunge un nuovo gruppo, StorageGRID lo clona automaticamente nella griglia di destinazione.

- Se la federazione delle identità è configurata per l'intero sistema StorageGRID o per l'account tenant, "creare nuovi gruppi tenant"importando gruppi federated dall'origine identità.
- Se non si utilizza la federazione delle identità,"creare nuovi gruppi locali" poi"creare utenti locali" .

4 Creare S3 chiavi di accesso

È possibile "creare le proprie chiavi di accesso" scegliere "creare le chiavi di accesso di un altro utente"tra la griglia di origine o la griglia di destinazione per accedere ai bucket su tale grid.

5 **In alternativa, è possibile clonare le chiavi di accesso S3**

Se è necessario accedere ai bucket con le stesse chiavi di accesso su entrambe le griglie, creare le chiavi di accesso nella griglia di origine e utilizzare l'API di Tenant Manager per clonarle manualmente nella griglia di destinazione. Per istruzioni, vedere "Clonare le chiavi di accesso S3 utilizzando l'API".

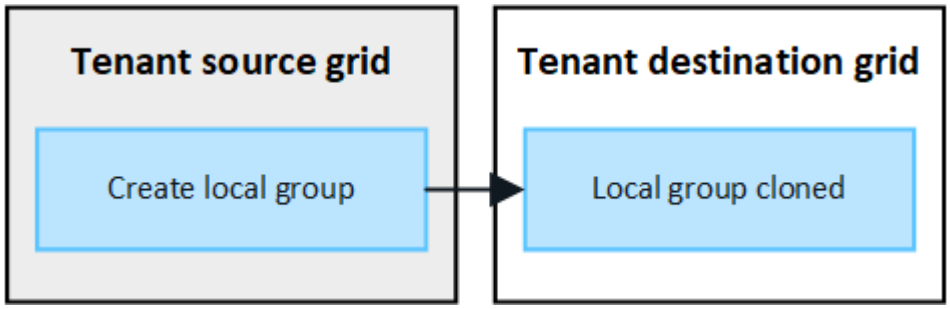
Come vengono clonati gruppi, utenti e chiavi di accesso S3?

Esaminare questa sezione per comprendere come vengono clonati gruppi, utenti e chiavi di accesso S3 tra la griglia di origine del tenant e la griglia di destinazione del tenant.

I gruppi locali creati sulla griglia di origine vengono clonati

Dopo aver creato e replicato un account tenant nella griglia di destinazione, StorageGRID clona automaticamente i gruppi locali aggiunti alla griglia di origine del tenant nella griglia di destinazione del tenant.

Sia il gruppo originale che il clone dispongono della stessa modalità di accesso, delle stesse autorizzazioni di gruppo e dei criteri di gruppo S3. Per istruzioni, vedere "Creare gruppi per il tenant S3".

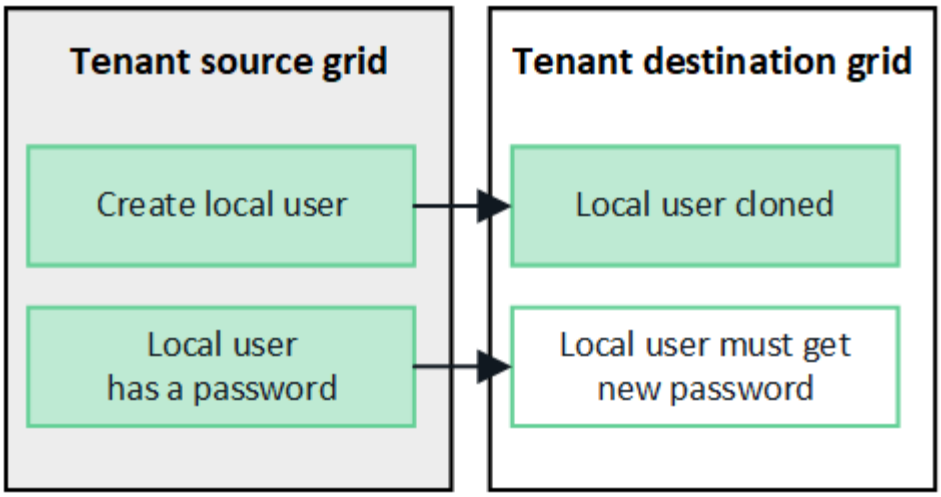


> Tutti gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando si crea il gruppo. Al momento della creazione degli utenti, selezionare il gruppo.

Gli utenti locali creati sulla griglia di origine vengono clonati

Quando si crea un nuovo utente locale sulla griglia di origine, StorageGRID clona automaticamente tale utente nella griglia di destinazione. Sia l'utente originale che il suo clone hanno lo stesso nome completo, lo stesso nome utente e l'impostazione **Nega accesso**. Entrambi gli utenti appartengono anche agli stessi gruppi. Per le istruzioni, vedere"Gestire gli utenti" .

Per motivi di sicurezza, le password degli utenti locali non vengono clonate nella griglia di destinazione. Se un utente locale deve accedere a Tenant Manager sulla griglia di destinazione, l'utente root dell'account tenant deve aggiungere una password per tale utente sulla griglia di destinazione. Per le istruzioni, vedere"Gestire gli utenti" .

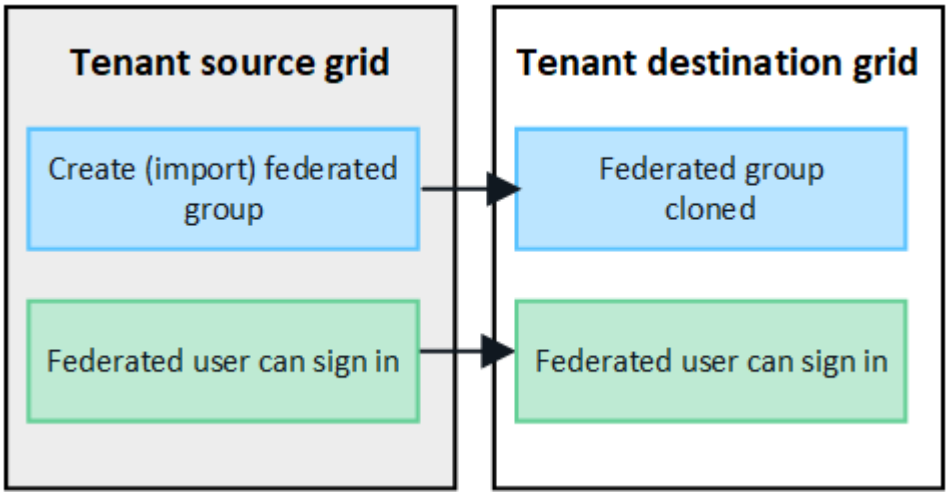


I gruppi federati creati sulla griglia di origine vengono clonati

Supponendo che i requisiti per l'utilizzo del clone dell'account con "single sign-on" e "federazione delle identità" siano stati soddisfatti, i gruppi federati creati (importazione) per il tenant sulla griglia di origine vengono clonati automaticamente nel tenant sulla griglia di destinazione.

Entrambi i gruppi dispongono della stessa modalità di accesso, delle stesse autorizzazioni di gruppo e dei criteri di gruppo S3.

Una volta creati i gruppi federati per il tenant di origine e clonati nel tenant di destinazione, gli utenti federati possono accedere al tenant su entrambi i grid.

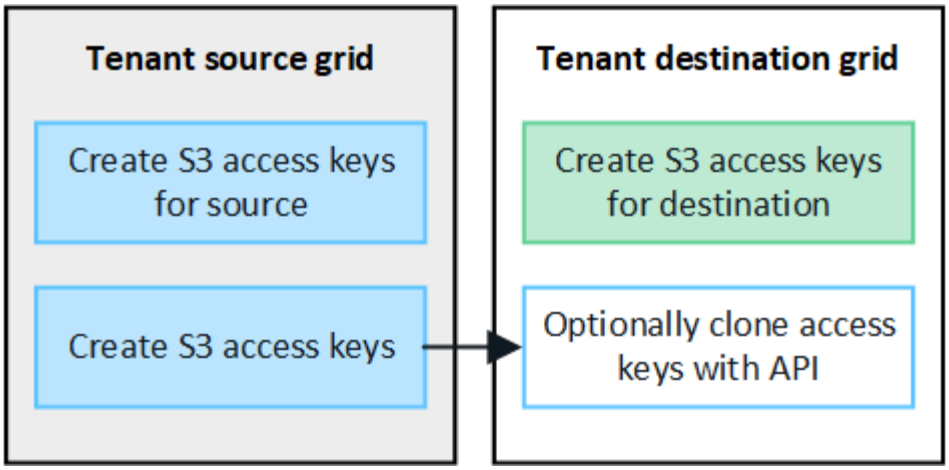


Le chiavi di accesso S3 possono essere clonate manualmente

StorageGRID non clonerà automaticamente le chiavi di accesso S3 perché la sicurezza è migliorata grazie alla presenza di chiavi diverse su ogni griglia.

Per gestire le chiavi di accesso sulle due griglie, è possibile eseguire una delle seguenti operazioni:

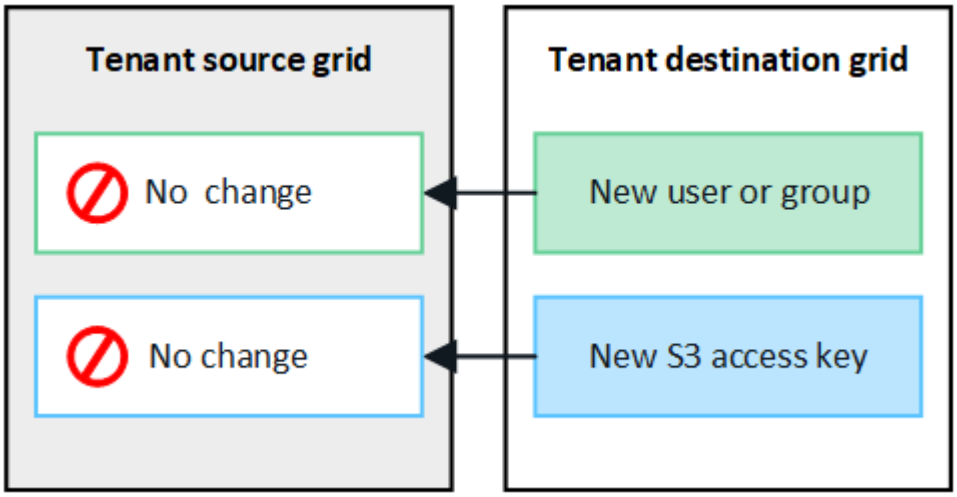
- Se non è necessario utilizzare gli stessi tasti per ogni griglia, è possibile "creare le proprie chiavi di accesso" o "creare le chiavi di accesso di un altro utente" su ogni griglia.
- Se è necessario utilizzare gli stessi tasti su entrambe le griglie, è possibile creare i tasti sulla griglia di origine e quindi utilizzare l'API di Tenant Manager per passare manualmente "clonare le chiavi" alla griglia di destinazione.



Quando si clonano le chiavi di accesso S3 per un utente federato, sia l'utente che le chiavi di accesso S3 vengono clonate nel tenant di destinazione.

I gruppi e gli utenti aggiunti alla griglia di destinazione non vengono clonati

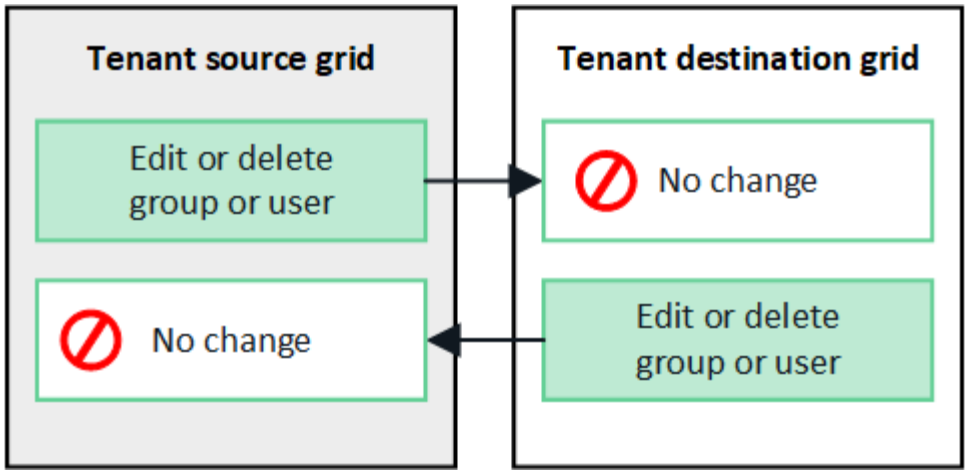
La clonazione avviene solo dalla griglia di origine del tenant alla griglia di destinazione del tenant. Se si creano o importano gruppi e utenti nella griglia di destinazione del tenant, StorageGRID non clonerà questi elementi nella griglia di origine del tenant.



I gruppi, gli utenti e le chiavi di accesso modificati o cancellati non vengono clonati

La clonazione avviene solo quando si creano nuovi gruppi e utenti.

Se si modificano o eliminano gruppi, utenti o chiavi di accesso in una griglia, le modifiche non verranno clonate nell'altra griglia.



Clonare le chiavi di accesso S3 utilizzando l'API

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile utilizzare l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione.

Prima di iniziare

- L'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**.
- La connessione a federazione di griglie ha uno stato **Connection** di **Connected**.
- L'utente ha effettuato l'accesso a Tenant Manager nella griglia di origine del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestisci le tue credenziali S3 o l'autorizzazione di accesso root".
- Se si clonano le chiavi di accesso per un utente locale, l'utente esiste già su entrambe le griglie.

> Quando si clonano le chiavi di accesso S3 per un utente federato, sia l'utente che le chiavi di accesso S3 vengono aggiunte al tenant di destinazione.

Clonare le proprie chiavi di accesso

È possibile clonare le proprie chiavi di accesso se è necessario accedere agli stessi bucket su entrambe le griglie.

Fasi

1. Utilizzando Tenant Manager nella griglia di origine e "creare le proprie chiavi di accesso"scaricare il `.csv` file.
2. Nella parte superiore di Tenant Manager, selezionare l'icona della guida e selezionare **documentazione API**.
3. Nella sezione **s3**, selezionare il seguente endpoint:

   ```
   POST /org/users/current-user/replicate-s3-access-key
   ```

4. Selezionare **Provalo**.
5. Nella casella di testo **body**, sostituire le voci di esempio per **accessKey** e **secretAccessKey** con i valori del file **.csv** scaricato.

   Assicurarsi di conservare le virgolette doppie intorno a ciascuna stringa.

6. Se la chiave scade, sostituire la voce di esempio **Expires** con la data e l'ora di scadenza come stringa nel formato dati-ora ISO 8601 (ad esempio, `2024-02-28T22:46:33-08:00`). Se la chiave non scade, inserire **Null** come valore per la voce **Expires** (oppure rimuovere la riga **Expires** e la virgola precedente).
7. Selezionare **Esegui**.
8. Verificare che il codice di risposta del server sia **204**, a indicare che la chiave è stata clonata correttamente nella griglia di destinazione.

Clonare le chiavi di accesso di un altro utente

È possibile clonare le chiavi di accesso di un altro utente se è necessario accedere agli stessi bucket su entrambe le griglie.

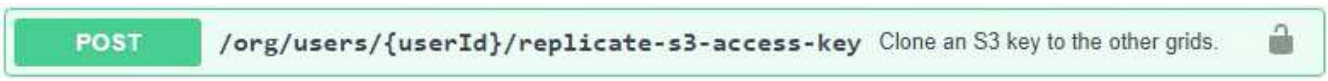
Fasi

1. Utilizzando Tenant Manager nella griglia di origine e "Creare le chiavi di accesso S3 dell'altro utente"scaricare il `.csv` file.
2. Nella parte superiore di Tenant Manager, selezionare l'icona della guida e selezionare **documentazione API**.
3. Ottenere l'ID utente. Questo valore è necessario per clonare le chiavi di accesso degli altri utenti.
   a. Nella sezione **users**, selezionare il seguente endpoint:

      `GET /org/users`

   b. Selezionare **Provalo**.
   c. Specificare i parametri da utilizzare per la ricerca degli utenti.
   d. Selezionare **Esegui**.
   e. Individuare l'utente di cui si desidera clonare le chiavi e copiare il numero nel campo **id**.
4. Nella sezione **s3**, selezionare il seguente endpoint:

   `POST /org/users/{userId}/replicate-s3-access-key`



5. Selezionare **Provalo**.
6. Nella casella di testo **ID utente**, incollare l'ID utente copiato.
7. Nella casella di testo **body**, sostituire le voci di esempio **example access key** e **secret access key** con i valori del file **.csv** dell'utente.

   Assicurarsi di conservare le virgolette doppie intorno alla stringa.

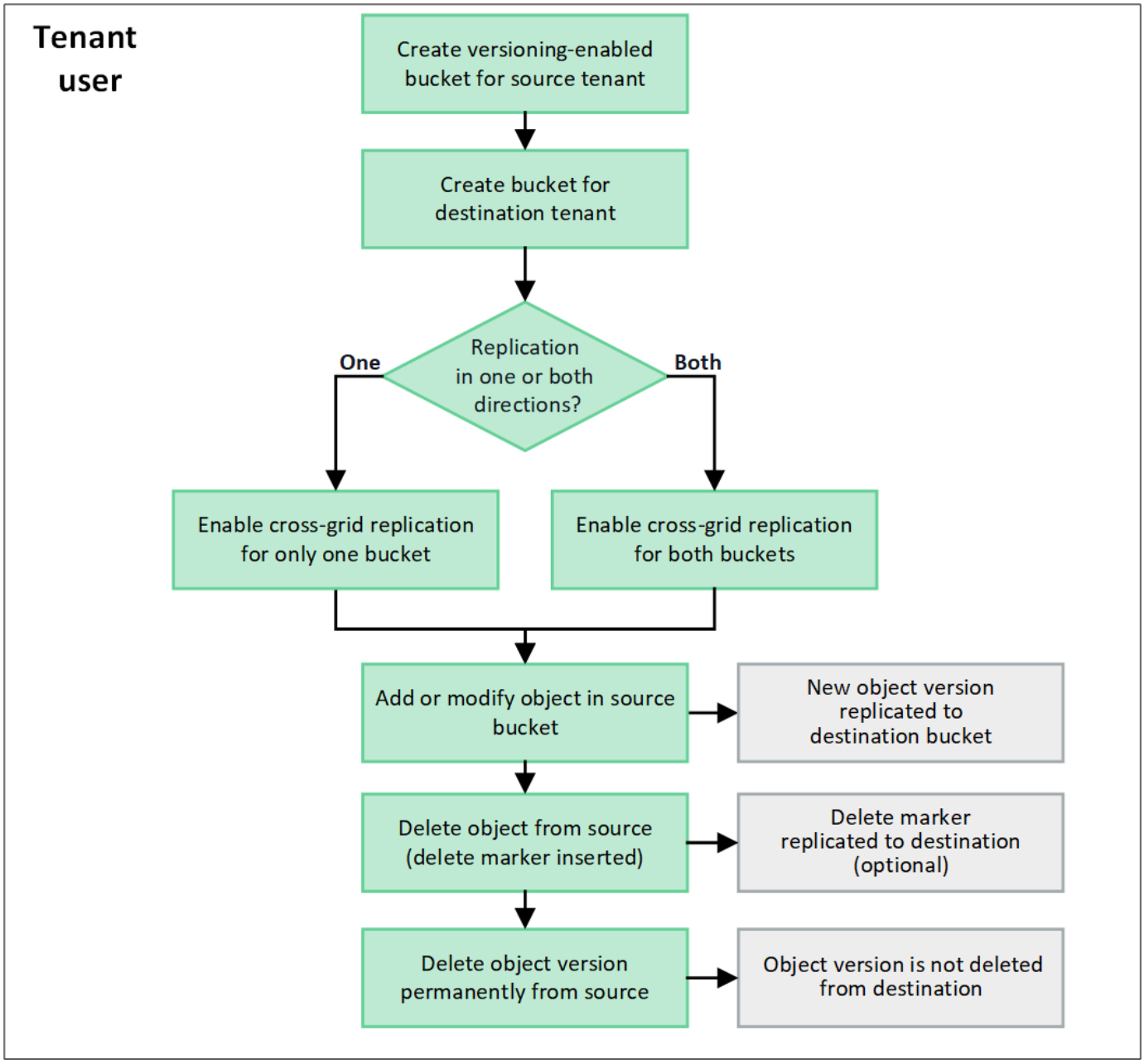
8. Se la chiave scade, sostituire la voce di esempio **Expires** con la data e l'ora di scadenza come stringa nel formato dati-ora ISO 8601 (ad esempio, `2023-02-28T22:46:33-08:00`). Se la chiave non scade, inserire **Null** come valore per la voce **Expires** (oppure rimuovere la riga **Expires** e la virgola precedente).
9. Selezionare **Esegui**.
10. Verificare che il codice di risposta del server sia **204**, a indicare che la chiave è stata clonata correttamente nella griglia di destinazione.

Gestire la replica cross-grid

Se all'account tenant è stata assegnata l'autorizzazione **Usa connessione federazione griglia** al momento della creazione, è possibile utilizzare la replica cross-grid per replicare automaticamente gli oggetti tra i bucket nella griglia di origine del tenant e i bucket nella griglia di destinazione del tenant. La replica cross-grid può avvenire in una o entrambe le direzioni.

Workflow per la replica cross-grid

Il diagramma del flusso di lavoro riassume i passaggi da eseguire per configurare la replica tra griglie tra bucket su due griglie. Questi passaggi sono descritti più dettagliatamente sotto il diagramma.



Configurare la replica cross-grid

Prima di poter utilizzare la replica tra griglie, è necessario accedere agli account tenant corrispondenti su ciascuna griglia e creare due bucket. Quindi, è possibile abilitare la replica tra griglie su uno o entrambi i bucket.

Prima di iniziare

- Hai esaminato i requisiti per la replicazione tra griglie. Fare riferimento a "Che cos'è la replica cross-grid" .
- Stai usando un"browser web supportato" .
- L'account tenant ha l'autorizzazione **Usa connessione federata di griglia** e su entrambe le griglie esistono account tenant identici. Fare riferimento a "Gestire i tenant consentiti per la connessione a federazione di grid" .
- L'utente tenant con cui stai effettuando l'accesso esiste già su entrambe le griglie e appartiene a un gruppo di utenti che ha"Autorizzazione di accesso root" .

- Se accedi alla griglia di destinazione del tenant come utente locale, l'utente root dell'account tenant ha impostato una password per il tuo account utente su quella griglia.

Crea due bucket

Come primo passo, accedi agli account tenant corrispondenti su ciascuna griglia e crea un bucket su ciascuna griglia.

Fasi

1. A partire da una delle due griglie della connessione a federazione di griglie, creare un nuovo bucket:
   a. Accedere all'account tenant utilizzando le credenziali di un utente tenant presente in entrambe le griglie.

      Se non riesci ad accedere alla griglia di destinazione del tenant come utente locale, verifica che l'utente root dell'account tenant abbia impostato una password per il tuo account utente.

   b. Seguire le istruzioni a "Creare un bucket S3".

      I nomi dei bucket e le regioni possono essere diversi su ogni griglia.

   c. Nella scheda **Manage object settings** (Gestisci impostazioni oggetto), selezionare **Enable object versioning** (attiva versione oggetto).
   d. Se S3 Object Lock è abilitato per il sistema StorageGRID , fare riferimento a"Replicazione cross-grid con S3 Object Lock" .
   e. Selezionare **Crea bucket**.
   f. Selezionare **fine**.
2. Ripetere questi passaggi per creare un bucket per lo stesso account tenant sull'altra griglia nella connessione di federazione della griglia.

   Secondo necessità, ogni benna può utilizzare una regione diversa.

Abilitare la replica cross-grid

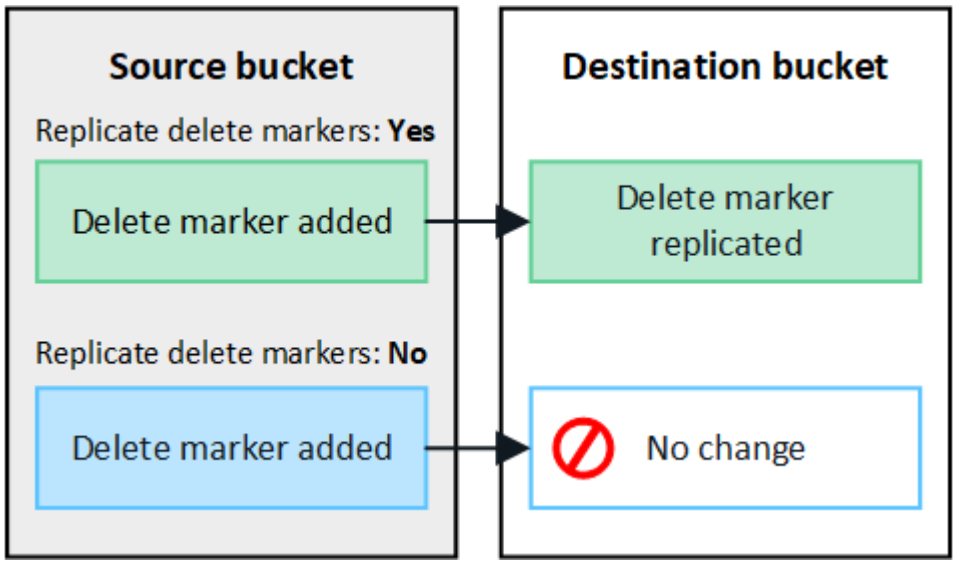
È necessario eseguire questi passaggi prima di aggiungere oggetti a uno dei bucket.

Fasi

1. A partire da una griglia di cui si desidera replicare gli oggetti, attivare "replica cross-grid in un'unica direzione":
   a. Accedi all'account tenant per il bucket.
   b. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
   c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
   d. Selezionare la scheda **Cross-grid Replication**.
   e. Selezionare **Enable** (attiva) ed esaminare l'elenco dei requisiti.
   f. Se tutti i requisiti sono stati soddisfatti, selezionare la connessione a federazione di griglia che si desidera utilizzare.
   g. Facoltativamente, modificare l'impostazione di **Replicate delete markers** per determinare cosa

accade nella griglia di destinazione se un client S3 invia una richiesta di eliminazione alla griglia di origine che non include un ID di versione:

- **Sì** (impostazione predefinita): Un marcatore di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione.
- **No**: un marcatore di eliminazione viene aggiunto al bucket di origine ma non viene replicato nel bucket di destinazione.



Se la richiesta di eliminazione include un ID versione, la versione dell'oggetto viene rimossa definitivamente dal bucket di origine. StorageGRID non replica le richieste di eliminazione che includono un ID versione, pertanto la stessa versione dell'oggetto non viene eliminata dalla destinazione.

Fare riferimento a"Che cos'è la replica cross-grid" per i dettagli.

a. In alternativa, modificare l'impostazione della categoria di controllo **Cross-Grid Replication** per gestire il volume dei messaggi di controllo:
   - **Errore** (impostazione predefinita): Solo le richieste di replica cross-grid non riuscite sono incluse nell'output di controllo.
   - **Normale**: Sono incluse tutte le richieste di replica cross-grid, il che aumenta significativamente il volume dell'output di controllo.
b. Rivedere le selezioni. Non è possibile modificare queste impostazioni a meno che entrambi i bucket non siano vuoti.
c. Selezionare **Enable (attiva) e test**.

   Dopo qualche istante, verrà visualizzato un messaggio di conferma dell'operazione. Gli oggetti aggiunti a questo bucket vengono ora replicati automaticamente nell'altra griglia. **La replica tra griglie** è visualizzata come funzionalità abilitata nella pagina dei dettagli del bucket.

2. Facoltativamente, passare al bucket corrispondente sull'altra griglia e "abilitare la replica cross-grid in entrambe le direzioni".

Test di replica tra griglie

Se la replica cross-grid è attivata per un bucket, potrebbe essere necessario verificare che la connessione e la

replica cross-grid funzionino correttamente e che i bucket di origine e di destinazione soddisfino ancora tutti i requisiti (ad esempio, il controllo delle versioni è ancora attivato).

Prima di iniziare

- Stai usando un"browser web supportato" .
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

Fasi

1. Accedi all'account tenant per il bucket.
2. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
3. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
4. Selezionare la scheda **Cross-grid Replication**.
5. Selezionare **Test di connessione**.

   Se la connessione è funzionante, viene visualizzato un banner di conferma. In caso contrario, verrà visualizzato un messaggio di errore che tu e l'amministratore della griglia potrete utilizzare per risolvere il problema. Per i dettagli, fare riferimento a"Risolvere i problemi relativi agli errori di federazione della griglia" .

6. Se la replica cross-grid è configurata per avvenire in entrambe le direzioni, passare al bucket corrispondente sull'altra griglia e selezionare **Test Connection** per verificare che la replica cross-grid funzioni nell'altra direzione.

Disattiva la replica cross-grid

Se non si desidera più copiare gli oggetti nell'altra griglia, è possibile interrompere in modo permanente la replica tra griglie.

Prima di disattivare la replica cross-grid, tenere presente quanto segue:

- La disattivazione della replica tra griglie non rimuove gli oggetti che sono già stati copiati tra le griglie. Ad esempio, oggetti in `my-bucket` sulla Griglia 1 che sono stati copiati in `my-bucket` sulla Griglia 2 non vengono rimossi se si disabilita la replica tra griglie per quel bucket. Se si desidera eliminare questi oggetti, è necessario rimuoverli manualmente.
- Se la replica cross-grid è stata attivata per ciascuno dei bucket (ovvero, se la replica si verifica in entrambe le direzioni), è possibile disattivare la replica cross-grid per uno o entrambi i bucket. Ad esempio, è possibile disattivare la replica degli oggetti da `my-bucket` sulla griglia 1 a `my-bucket` sulla griglia 2, continuando a replicare gli oggetti da `my-bucket` sulla griglia 2 a `my-bucket` sulla griglia 1.
- È necessario disabilitare la replica tra griglie prima di poter rimuovere l'autorizzazione di un tenant a utilizzare la connessione federata della griglia. Fare riferimento a "Gestire i tenant autorizzati" .
- Se si disabilita la replica tra griglie per un bucket contenente oggetti, non sarà possibile riabilitarla a meno che non si eliminino tutti gli oggetti sia dal bucket di origine che da quello di destinazione.

  Non è possibile riabilitare la replica a meno che entrambi i bucket non siano vuoti.

Prima di iniziare

- Stai usando un"browser web supportato" .
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

Fasi

1. Partendo dalla griglia di cui non si desidera più replicare gli oggetti, interrompere la replica cross-grid per il bucket:
   a. Accedi all'account tenant per il bucket.
   b. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
   c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
   d. Selezionare la scheda **Cross-grid Replication**.
   e. Selezionare **Disable Replication** (Disattiva replica).
   f. Se sei sicuro di voler disabilitare la replica tra griglie per questo bucket, digita **Sì** nella casella di testo e seleziona **Disabilita**.

      Dopo alcuni istanti, viene visualizzato un messaggio di successo. I nuovi oggetti aggiunti a questo bucket non possono più essere replicati automaticamente nell'altra griglia. **La replica cross-grid** non viene più visualizzata come funzione abilitata nella pagina bucket.

2. Se la replica cross-grid è stata configurata per avvenire in entrambe le direzioni, passare al bucket corrispondente sull'altra griglia e interrompere la replica cross-grid nell'altra direzione.

Visualizza connessioni di federazione di griglie

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile visualizzare le connessioni consentite.

Prima di iniziare

- L'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**.
- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

Fasi

1. Selezionare **STORAGE (S3)** > **Grid Federation Connections**.

   Viene visualizzata la pagina Grid Federation Connection (connessione federazione griglia) che include una tabella che riepiloga le seguenti informazioni:

Colonna	Descrizione
Nome della connessione	Le connessioni della federazione di griglie che il tenant dispone dell'autorizzazione per l'utilizzo.
Bucket con replica cross-grid	Per ogni connessione a federazione di grid, i bucket tenant con replica cross-grid attivata. Gli oggetti aggiunti a questi bucket verranno replicati nell'altra griglia della connessione.
Ultimo errore	Per ogni connessione a federazione di griglie, si verifica l'errore più recente, se presente, quando i dati venivano replicati nell'altra griglia. Vedere Eliminare l'ultimo errore.

2. Facoltativamente, selezionare un nome bucket in "visualizza i dettagli del bucket".

Cancella l'ultimo errore

Nella colonna **ultimo errore** potrebbe essere visualizzato un errore per uno dei seguenti motivi:

- Versione dell'oggetto di origine non trovata.
- Bucket di origine non trovato.
- Il bucket di destinazione è stato cancellato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il bucket di destinazione ha la versione sospesa.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più disponibile.

> In questa colonna viene visualizzato solo l'ultimo errore di replica tra griglie; gli errori precedenti che potrebbero essere stati rilevati non verranno visualizzati.

Fasi

1. Se nella colonna **ultimo errore** viene visualizzato un messaggio, visualizzare il testo del messaggio.

   Ad esempio, questo errore indica che il bucket di destinazione per la replica cross-grid era in uno stato non valido, probabilmente perché il controllo delle versioni era stato sospeso o S3 Object Lock era attivato.

2. Eseguire le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso nel bucket di destinazione per la replica cross-grid, riabilitare il controllo delle versioni per quel bucket.
3. Selezionare la connessione dalla tabella.
4. Selezionare **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.

   > Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.

7. Per determinare se alcuni oggetti non sono stati replicati a causa dell'errore bucket, vedere "Identificare e riprovare le operazioni di replica non riuscite".

Gestire gruppi e utenti

USA la federazione delle identità

L'utilizzo della federazione delle identità rende più rapida la configurazione di gruppi e utenti tenant e consente agli utenti tenant di accedere all'account tenant utilizzando credenziali familiari.

Configurare la federazione delle identità per Tenant Manager

È possibile configurare la federazione delle identità per Tenant Manager se si desidera che i gruppi e gli utenti dei tenant vengano gestiti in un altro sistema, ad esempio Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Stai utilizzando Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server come provider di identità.

> Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare l'assistenza tecnica.

- Se si intende utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere Linee guida per la configurazione del server OpenLDAP.
- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3. Vedere "Crittografia supportata per le connessioni TLS in uscita".

A proposito di questa attività

La possibilità di configurare un servizio di federazione delle identità per il tenant dipende dalla configurazione dell'account tenant. Il tenant potrebbe condividere il servizio di federazione delle identità configurato per Grid Manager. Se viene visualizzato questo messaggio quando si accede alla pagina Identity Federation, non è possibile configurare un'origine di identità federata separata per questo tenant.

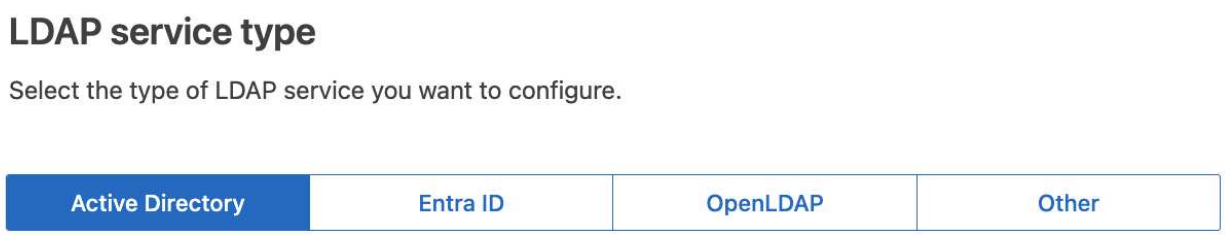
> This tenant account uses the LDAP server that is configured for the Grid Manager.
> Contact the grid administrator for information or to change this setting.

Inserire la configurazione

Quando si configura Identify Federation, vengono forniti i valori necessari a StorageGRID per connettersi a un servizio LDAP.

Fasi

1. Selezionare **Gestione accessi** > **Federazione identità**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.



Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP. In caso contrario, passare alla fase successiva.
   - **Nome univoco utente**: il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `uid` per OpenLDAP. Se stai configurando Oracle Directory Server, inserisci `uid` .
   - **UUID utente**: il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se stai configurando Oracle Directory Server, inserisci `nsuniqueid` . Il valore di ciascun utente per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
   - **Nome univoco del gruppo**: il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `cn` per OpenLDAP. Se stai configurando Oracle Directory Server, inserisci `cn` .
   - **UUID gruppo**: il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se stai configurando Oracle Directory Server, inserisci `nsuniqueid` . Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, inserire le informazioni richieste relative al server LDAP e alla connessione di rete nella sezione Configura server LDAP.
   - **Nome host**: Il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAP.
   - **Port** (porta): Porta utilizzata per la connessione al server LDAP.

     La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

   - **Username**: Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP.

     Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome principale dell'utente.

     L'utente specificato deve disporre dell'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

     - `sAMAccountName` o. `uid`
     - `objectGUID`, , `entryUUID` o `nsuniqueid`

- `cn`
- `memberOf` o. `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl` E `userPrincipalName`
- **ID di ingresso**: `accountEnabled` E `userPrincipalName`

◦ **Password**: La password associata al nome utente.

> Se si modifica la password in futuro, è necessario aggiornarla in questa pagina.

◦ **DN base gruppo**: Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), tutti i gruppi il cui nome distinto è relativo al DN di base (DC=storagegrid,DC=example,DC=com) possono essere utilizzati come gruppi federati.

> I valori **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

◦ **User base DN**: Percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.

> I valori **Nome univoco utente** devono essere univoci all'interno del **DN base utente** a cui appartengono.

◦ **Bind username format** (opzionale): Il modello di nome utente predefinito che StorageGRID deve utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il formato **bind username** perché può consentire agli utenti di accedere se StorageGRID non è in grado di collegarsi con l'account del servizio.

Immettere uno di questi modelli:

- **Modello UserPrincipalName (ID AD e Entra)**: `[USERNAME]@*example*.com`
- **Modello di nome di accesso di livello inferiore (ID AD e Entra)**: `*example*\[USERNAME]`
- **Modello di nome distinto**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Includi **[NOME UTENTE]** esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.
   ◦ **Usa STARTTLS**: usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Microsoft Entra ID.
   ◦ **Usa LDAPS**: l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Microsoft Entra ID.
   ◦ **Non utilizzare TLS**: il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Microsoft Entra ID.

L'utilizzo dell'opzione **Non utilizzare TLS** non è supportato se il server Active Directory impone la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.
   - **Usa certificato CA del sistema operativo**: Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
   - **Usa certificato CA personalizzato**: Utilizza un certificato di protezione personalizzato.

     Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

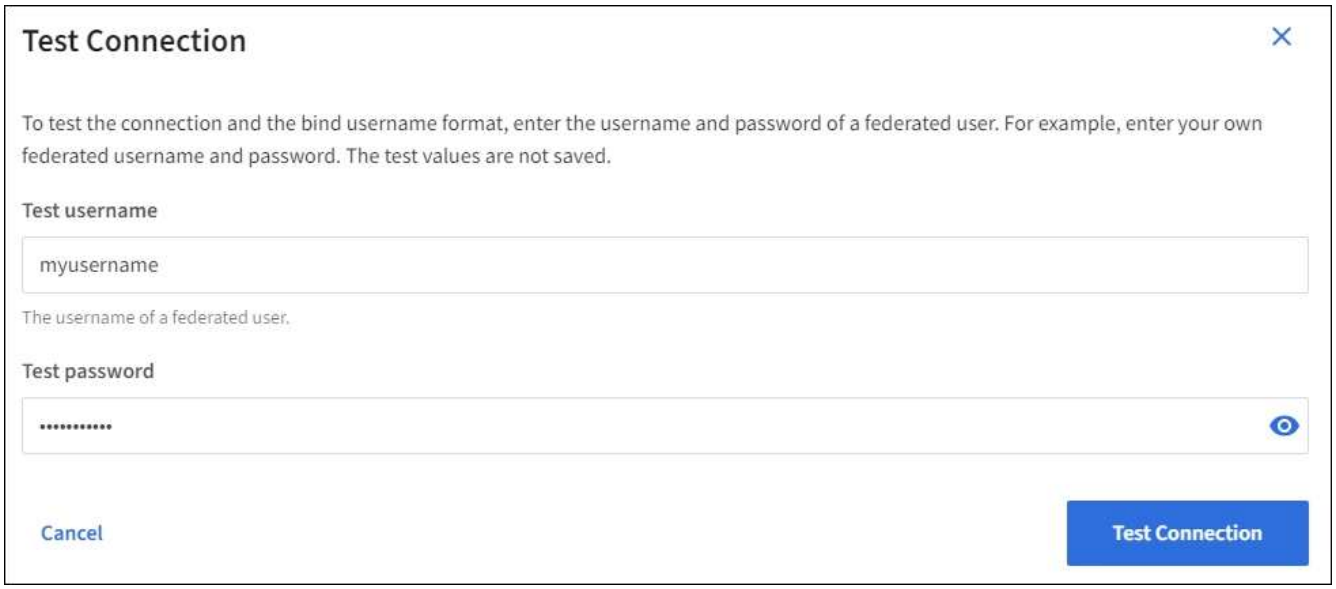
Verificare la connessione e salvare la configurazione

Dopo aver inserito tutti i valori, è necessario verificare la connessione prima di salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente BIND, se fornito.

Fasi

1. Selezionare **Test di connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
   - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
   - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risolvere eventuali problemi e verificare nuovamente la connessione.
3. Se è stato fornito un formato BIND Username, inserire il nome utente e la password di un utente federato valido.

   Ad esempio, inserire il proprio nome utente e la propria password. Non includere caratteri speciali nel nome utente, ad esempio @ o /.



   - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.

- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente BIND o il nome utente e la password di prova non sono validi. Risolvere eventuali problemi e verificare nuovamente la connessione.

Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

Fasi

1. Vai alla pagina Identity Federation.
2. Selezionare **Sync server** nella parte superiore della pagina.

   Il processo di sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.

   L'avviso **errore di sincronizzazione federazione identità** viene attivato se si verifica un problema durante la sincronizzazione di utenti e gruppi federati dall'origine dell'identità.

Disattiva la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione delle identità per gruppi e utenti. Quando la federazione delle identità è disabilitata, non c'è comunicazione tra StorageGRID e l'origine dell'identità. Tuttavia, tutte le impostazioni configurate vengono mantenute, consentendoti di riattivare facilmente la federazione delle identità in futuro.

A proposito di questa attività

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non verrà eseguita e non verranno generati avvisi per gli account che non sono stati sincronizzati.
- La casella di controllo **Abilita federazione delle identità** è disabilitata se lo stato Single Sign-On (SSO) è **Abilitato** o **Modalità sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere "Disattiva single sign-on" .

Fasi

1. Vai alla pagina Identity Federation.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).

Linee guida per la configurazione del server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.

Per le origini identità che non sono Active Directory o Microsoft Entra ID, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare tutte le chiavi S3 dell'utente o rimuovere l'utente da tutti i gruppi.

MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, vedere le istruzioni per la manutenzione dell'appartenenza al gruppo inverso nella "Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

Vedere le informazioni sulla manutenzione dell'appartenenza al gruppo inverso nella "Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Gestire i gruppi di tenant

Creare gruppi per un tenant S3

È possibile gestire le autorizzazioni per i gruppi di utenti S3 importando gruppi federati o creando gruppi locali.

Prima di iniziare

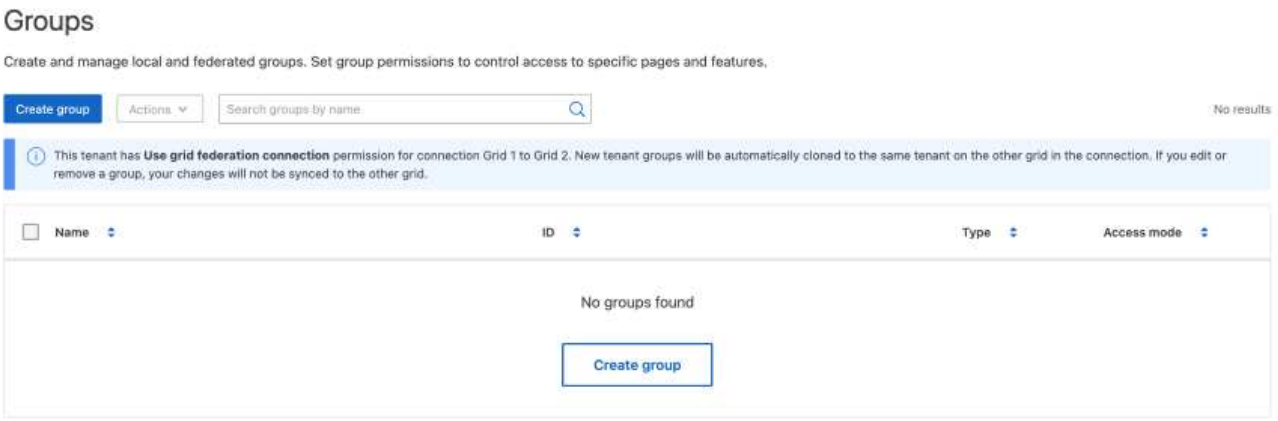
- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Se si prevede di importare un gruppo federated, si dispone di "federazione di identità configurata", e il gruppo Federated esiste già nell'origine identità configurata.
- Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è stato esaminato il flusso di lavoro e le considerazioni relative a "clonazione di utenti e gruppi tenant"e si è effettuato l'accesso alla griglia di origine del tenant.

Accedere alla procedura guidata Crea gruppo

Come prima fase, accedere alla procedura guidata Crea gruppo.

Fasi

1. Selezionare **Gestione accessi** > **Gruppi**.
2. Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, verificare che venga visualizzato un banner blu che indica che i nuovi gruppi creati in questa griglia verranno clonati nello stesso tenant nell'altra griglia della connessione. Se questo banner non viene visualizzato, potresti aver effettuato l'accesso alla griglia di destinazione del tenant.



3. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federated.

Fasi

1. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda **Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

   Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

2. Inserire il nome del gruppo.
   - **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.

     Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, si verificherà un errore di clonazione se lo stesso **nome univoco** esiste già per il tenant nella griglia di destinazione.

   - **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato all' `sAMAccountName`attributo. Per OpenLDAP, il nome univoco è il nome associato all' `uid`attributo.
3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

Le autorizzazioni di gruppo controllano le attività che gli utenti possono eseguire nelle API di gestione tenant e tenant Manager.

Fasi

1. Per la modalità **Access**, selezionare una delle seguenti opzioni:
   - **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
   - **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono

apportare modifiche o eseguire operazioni nell'API di gestione tenant Manager o tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

> Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

2. Selezionare una o più autorizzazioni per questo gruppo.

   Vedere "Permessi di gestione del tenant".

3. Selezionare **continua**.

Impostare i criteri di gruppo S3

I criteri di gruppo determinano le autorizzazioni di accesso S3 che gli utenti avranno.

Fasi

1. Selezionare il criterio che si desidera utilizzare per questo gruppo.

Policy di gruppo	Descrizione
Nessun accesso S3	Predefinito. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
Accesso in sola lettura	Gli utenti di questo gruppo hanno accesso in sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
Accesso completo	Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
Riduzione del ransomware	Questo criterio di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti. Gli utenti di tenant Manager che dispongono dell'autorizzazione **Gestisci tutti i bucket** possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.
Personalizzato	Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

2. Se si seleziona **Custom**, inserire il criterio di gruppo. Ogni policy di gruppo ha un limite di dimensione di 5,120 byte. Immettere una stringa valida formattata con JSON.

   Per informazioni dettagliate sui criteri di gruppo, incluse la sintassi del linguaggio e gli esempi, vedere "Criteri di gruppo di esempio".

3. Se si sta creando un gruppo locale, selezionare **continua**. Se si sta creando un gruppo federated, selezionare **Crea gruppo** e **fine**.

Aggiunta di utenti (solo gruppi locali)

È possibile salvare il gruppo senza aggiungere utenti oppure aggiungere utenti locali già esistenti.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando si crea il gruppo. Al momento della creazione degli utenti, selezionare il gruppo.

Fasi

1. Facoltativamente, selezionare uno o più utenti locali per questo gruppo.
2. Selezionare **Crea gruppo** e **fine**.

   Il gruppo creato viene visualizzato nell'elenco dei gruppi.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ci si trova nella griglia di origine del tenant, il nuovo gruppo viene clonato nella griglia di destinazione del tenant. **Success** viene visualizzato come **Cloning status** nella sezione Overview della pagina dei dettagli del gruppo.

Permessi di gestione del tenant

Prima di creare un gruppo tenant, prendere in considerazione le autorizzazioni che si desidera assegnare a tale gruppo. Le autorizzazioni di gestione del tenant determinano le attività che gli utenti possono eseguire utilizzando il tenant Manager o l'API di gestione del tenant. Un utente può appartenere a uno o più gruppi. Le autorizzazioni sono cumulative se un utente appartiene a più gruppi.

Per accedere a tenant Manager o utilizzare l'API di gestione tenant, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono accedere possono eseguire le seguenti operazioni:

- Visualizza la dashboard
- Modificare la propria password (per gli utenti locali)

Per tutte le autorizzazioni, l'impostazione della modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità.

> Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

È possibile assegnare le seguenti autorizzazioni a un gruppo.

Permesso	Descrizione	Dettagli
Accesso root	Fornisce l'accesso completo al tenant Manager e all'API di gestione del tenant.	
Gestisci le tue credenziali S3	Consente agli utenti di creare e rimuovere le proprie chiavi di accesso S3.	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu **STORAGE (S3)** > **My S3 access keys**.
Visualizza tutti i bucket	Consente agli utenti di visualizzare tutti i bucket e le relative configurazioni.	Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu **bucket**. Questa autorizzazione è sostituita dall'autorizzazione Gestisci tutti i bucket. Non influisce sui bucket S3 o sui criteri di gruppo utilizzati dai client S3 o dalla console S3.
Gestire tutti i bucket	Consente agli utenti di utilizzare Tenant Manager e l'API Tenant Management per creare ed eliminare bucket S3 e gestire le impostazioni per tutti i bucket S3 nell'account tenant, indipendentemente dal bucket S3 o dai criteri di gruppo.	Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu **bucket**. Questa autorizzazione sostituisce l'autorizzazione Visualizza tutti i bucket. Non influisce sui bucket S3 o sui criteri di gruppo utilizzati dai client S3 o dalla console S3.
Gestire gli endpoint	Consente agli utenti di utilizzare il gestore tenant o l'API di gestione tenant per creare o modificare gli endpoint del servizio della piattaforma, che vengono utilizzati come destinazione per i servizi della piattaforma StorageGRID.	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu **Platform Services Endpoint**.
Utilizzare la scheda Console S3	Se combinato con l'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket, consente agli utenti di visualizzare e gestire gli oggetti dalla scheda Console S3 nella pagina dei dettagli di un bucket.	

Gestire i gruppi

Gestire i gruppi di tenant in base alle esigenze per visualizzare, modificare o duplicare un gruppo e altro ancora.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".

- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".

Visualizzare o modificare il gruppo

È possibile visualizzare e modificare le informazioni di base e i dettagli di ciascun gruppo.

Fasi

1. Selezionare **Gestione accessi** > **Gruppi**.
2. Consultare le informazioni fornite nella pagina gruppi, che elenca le informazioni di base per tutti i gruppi locali e federati per questo account tenant.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si stanno visualizzando i gruppi nella griglia di origine del tenant:

   - Un messaggio banner indica che se si modifica o si rimuove un gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio di intestazione indica se i gruppi non sono stati clonati nel tenant sulla griglia di destinazione. È possibile riprovare a creare un clone di gruppo che non sia riuscito.
3. Se si desidera modificare il nome del gruppo:
   a. Selezionare la casella di controllo del gruppo.
   b. Selezionare **azioni** > **Modifica nome gruppo**.
   c. Inserire il nuovo nome.
   d. Selezionare **Salva modifiche.**
4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:
   - Selezionare il nome del gruppo.
   - Selezionare la casella di controllo relativa al gruppo e selezionare **azioni** > **Visualizza dettagli gruppo**.
5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun gruppo:
   - Nome visualizzato
   - Nome univoco
   - Tipo
   - Modalità di accesso
   - Permessi
   - Policy S3
   - Numero di utenti in questo gruppo
   - Ulteriori campi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando il gruppo nella griglia di origine del tenant:
     - Stato di cloning, **Success** o **Failure**
     - Un banner blu che indica che se modifichi o elimini questo gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
6. Modificare le impostazioni del gruppo secondo necessità. Fare riferimento a"Creare gruppi per un tenant S3" per i dettagli su cosa inserire.

a. Nella sezione Panoramica , modificare il nome visualizzato selezionando il nome o l'icona di modifica .

b. Nella scheda **permessi di gruppo**, aggiornare le autorizzazioni e selezionare **Salva modifiche**.

c. Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.

Facoltativamente, selezionare un criterio di gruppo S3 diverso o immettere la stringa JSON per un criterio personalizzato, a seconda delle necessità.

7. Per aggiungere uno o più utenti locali al gruppo:

a. Selezionare la scheda Users (utenti).

b. Selezionare **Aggiungi utenti**.

c. Selezionare gli utenti che si desidera aggiungere e selezionare **Aggiungi utenti**.

In alto a destra viene visualizzato il messaggio Success (operazione riuscita).

8. Per rimuovere utenti locali dal gruppo:

a. Selezionare la scheda Users (utenti).

b. Selezionare **Rimuovi utenti**.

c. Selezionare gli utenti che si desidera rimuovere e selezionare **Rimuovi utenti**.

In alto a destra viene visualizzato il messaggio Success (operazione riuscita).

9. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Gruppo duplicato

È possibile duplicare un gruppo esistente per creare nuovi gruppi più rapidamente.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si duplica un gruppo dalla griglia di origine del tenant, il gruppo duplicato verrà clonato nella griglia di destinazione del tenant.

Fasi

1. Selezionare **Gestione accessi** > **Gruppi**.
2. Selezionare la casella di controllo del gruppo che si desidera duplicare.
3. Selezionare **azioni** > **Duplica gruppo**.
4. Vedere"Creare gruppi per un tenant S3" per i dettagli su cosa inserire.
5. Selezionare **Crea gruppo**.

Riprova clone di gruppo

Per riprovare un clone non riuscito:

1. Selezionare ciascun gruppo che indica *(clonazione non riuscita)* sotto il nome del gruppo.
2. Selezionare **azioni** > **Clona gruppi**.
3. Visualizzare lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun gruppo da clonare.

Per ulteriori informazioni, vedere "Clonare utenti e gruppi tenant".

Eliminare uno o più gruppi

È possibile eliminare uno o più gruppi. Gli utenti che appartengono solo a un gruppo cancellato non potranno più accedere al tenant manager o utilizzare l'account tenant.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si elimina un gruppo, StorageGRID non eliminerà il gruppo corrispondente sull'altra griglia. Se è necessario mantenere queste informazioni sincronizzate, è necessario eliminare lo stesso gruppo da entrambe le griglie.

Fasi

1. Selezionare **Gestione accessi** > **Gruppi**.
2. Selezionare la casella di controllo per ciascun gruppo che si desidera eliminare.
3. Selezionare **azioni** > **Elimina gruppo** o **azioni** > **Elimina gruppi**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Delete group** (Elimina gruppo) o **Delete groups** (Elimina gruppi).

Imposta AssumeRole

Prima di iniziare

Per configurare AssumeRole devi essere un amministratore.

A proposito di questa attività

Per impostare AssumeRole, creare il gruppo di destinazione da assumere, se il gruppo non esiste già. Modificare i criteri S3 del gruppo per specificare le azioni consentite per l'assunzione di questo gruppo. Modificare i criteri di attendibilità S3 del gruppo per specificare gli utenti attendibili autorizzati ad assumere il ruolo del gruppo con l'API AssumeRole.

Credenziali di sicurezza temporanee create presupponendo che questo gruppo sia valido per una durata limitata. La sessione dura tra 15 minuti e 12 ore e la sessione predefinita è di 1 ora. Quando si rimuove l'utente dai criteri di attendibilità S3 del gruppo, l'utente non può più assumere questo gruppo.

Fasi

1. Selezionare **Gestione accessi** > **Gruppi**.
2. Fare clic sul nome del gruppo.
3. Selezionare la scheda **Criterio di attendibilità S3**.
4. Aggiungi i tuoi criteri di attendibilità S3, incluso un elenco di utenti che possono eseguire AssumeRole.
5. Selezionare **Save Changes** (Salva modifiche).

6. Selezionare la scheda **Criteri di gruppo S3**.
7. Modificare il criterio S3 per specificare solo le azioni S3 richieste per gli utenti attendibili aggiunti nel criterio di attendibilità S3 di questo gruppo.
8. Selezionare **Save Changes** (Salva modifiche).

Esempio di una policy di trust AssumeRole S3

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

Una volta completata la configurazione, gli utenti elencati nei criteri di attendibilità S3 possono eseguire AssumeRole e ricevere le credenziali. Le autorizzazioni finali sono determinate dai criteri di gruppo, dai criteri del bucket e dai criteri di sessione. Per ulteriori informazioni, consultare "Utilizzare le policy di accesso" .

Gestire gli utenti

È possibile creare utenti locali e assegnarli a gruppi locali per determinare a quali funzionalità possono accedere. È anche possibile importare utenti federati. Il Tenant Manager include un utente locale predefinito, denominato "root". Sebbene sia possibile aggiungere e rimuovere utenti locali, non è possibile rimuovere l'utente root.

> Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti locali non potranno accedere al Gestore tenant o all'API di gestione tenant, anche se possono utilizzare le applicazioni client per accedere alle risorse del tenant, in base alle autorizzazioni di gruppo.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root".
- Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è stato esaminato il flusso di lavoro e le considerazioni relative a "clonazione di utenti e gruppi tenant"e si è effettuato l'accesso alla griglia di origine del tenant.

Crea un utente locale

È possibile creare un utente locale e assegnarlo a uno o più gruppi locali per controllarne le autorizzazioni di accesso.

Gli utenti S3 che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o criteri di gruppo S3 applicati. Questi utenti potrebbero avere accesso al bucket S3 concesso tramite una policy bucket.

Accedere alla procedura guidata Crea utente

Fasi

1. Selezionare **Gestione accessi** > **Utenti**.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, un banner blu indica che si tratta della griglia di origine del tenant. Tutti gli utenti locali creati in questa griglia verranno clonati nell'altra griglia della connessione.

2. Selezionare **Crea utente**.

Immettere le credenziali

Fasi

1. Per il passo **inserire le credenziali utente**, completare i seguenti campi.

Campo	Descrizione
Nome completo	Il nome completo dell'utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
Nome utente	Il nome utilizzato dall'utente per l'accesso. I nomi utente devono essere univoci e non possono essere modificati. **Nota**: Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, si verificherà un errore di clonazione se lo stesso **Nome utente** esiste già per il tenant nella griglia di destinazione.
Password e Conferma password	La password che l'utente utilizzerà inizialmente al momento dell'accesso.

Campo	Descrizione
Negare l'accesso	Selezionare **Sì** per impedire a questo utente di accedere all'account tenant, anche se potrebbe ancora appartenere a uno o più gruppi. Ad esempio, selezionare **Sì** per sospendere temporaneamente la possibilità di accesso dell'utente.

2. Selezionare **continua**.

Assegnare ai gruppi

Fasi

1. Assegnare l'utente a uno o più gruppi locali per determinare quali attività possono eseguire.

   L'assegnazione di un utente ai gruppi è facoltativa. Se preferisci, puoi selezionare gli utenti quando crei o modifichi i gruppi.

   Gli utenti che non appartengono a nessun gruppo non disporranno di autorizzazioni di gestione. Le autorizzazioni sono cumulative. Gli utenti disporranno di tutte le autorizzazioni per tutti i gruppi a cui appartengono. Vedere "Permessi di gestione del tenant".

2. Selezionare **Crea utente**.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ci si trova nella griglia di origine del tenant, il nuovo utente locale viene clonato nella griglia di destinazione del tenant. **Success** viene visualizzato come **Cloning status** nella sezione Overview della pagina dei dettagli dell'utente.

3. Selezionare **fine** per tornare alla pagina utenti.

Visualizzare o modificare l'utente locale

Fasi

1. Selezionare **Gestione accessi** > **Utenti**.
2. Consultare le informazioni fornite nella pagina utenti, che elenca le informazioni di base per tutti gli utenti locali e federati per questo account tenant.

   Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando l'utente nella griglia di origine del tenant:

   - Un messaggio banner indica che se si modifica o si rimuove un utente, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio di intestazione indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. È possibile riprovare un clone utente non riuscito.
3. Se si desidera modificare il nome completo dell'utente:
   a. Selezionare la casella di controllo dell'utente.
   b. Selezionare **azioni** > **Modifica nome completo**.
   c. Inserire il nuovo nome.
   d. Selezionare **Salva modifiche.**

4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:
   - Selezionare il nome utente.
   - Selezionare la casella di controllo dell'utente e selezionare **azioni** > **Visualizza dettagli utente**.
5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
   - Nome completo
   - Nome utente
   - Tipo di utente
   - Accesso negato
   - Modalità di accesso
   - Appartenenza al gruppo
   - Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e l'utente viene visualizzato nella griglia di origine del tenant:
     - Stato di cloning, **Success** o **Failure**
     - Un banner blu che indica che se modifichi questo utente, le modifiche non verranno sincronizzate con l'altra griglia.
6. Modificare le impostazioni utente in base alle esigenze. Vedere Creare un utente locale per i dettagli su cosa immettere.
   a. Nella sezione Panoramica , modificare il nome completo selezionando il nome o l'icona di modifica .

      Impossibile modificare il nome utente.

   b. Nella scheda **Password**, modificare la password dell'utente e selezionare **Salva modifiche**.
   c. Nella scheda **accesso**, selezionare **No** per consentire all'utente di accedere o selezionare **Sì** per impedire all'utente di accedere. Quindi, selezionare **Salva modifiche**.
   d. Nella scheda **tasti di accesso**, selezionare **Crea tasto** e seguire le istruzioni per "Creazione delle chiavi di accesso S3 di un altro utente".
   e. Nella scheda **gruppi**, selezionare **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai gruppi. Quindi, selezionare **Save Changes** (Salva modifiche).
7. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Importa utenti federati

È possibile importare uno o più utenti federati, fino a un massimo di 100 utenti, direttamente nella pagina Utenti.

Fasi

1. Selezionare **Gestione accessi** > **Utenti**.
2. Seleziona **Importa utenti federati**.
3. Inserisci l'UUID o il nome utente di uno o più utenti federati.

   Per voci multiple, aggiungere ogni UUID o nome utente su una nuova riga.

4. Selezionare **Importa**.

Se l'importazione nel campo Utenti non riesce per uno o più utenti, procedere come segue:

a. Espandi **Utenti non importati** e seleziona **Copia utenti**.
b. Riprovare l'importazione selezionando **Precedente** e incollando gli utenti copiati nella finestra di dialogo **Importa utenti federati**.

Dopo aver chiuso la finestra di dialogo **Importa utenti federati**, le informazioni sugli utenti federati vengono visualizzate nella pagina Utenti per gli utenti importati correttamente.

Utente locale duplicato

È possibile duplicare un utente locale per creare un nuovo utente più rapidamente.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si duplica un utente dalla griglia di origine del tenant, l'utente duplicato verrà clonato nella griglia di destinazione del tenant.

Fasi

1. Selezionare **Gestione accessi** > **Utenti**.
2. Selezionare la casella di controllo dell'utente che si desidera duplicare.
3. Selezionare **azioni** > **utente duplicato**.
4. Vedere Creare un utente locale per i dettagli su cosa immettere.
5. Selezionare **Crea utente**.

Riprova clone utente

Per riprovare un clone non riuscito:

1. Selezionare ogni utente che indica *(clonazione non riuscita)* sotto il nome utente.
2. Selezionare **azioni** > **Clona utenti**.
3. Visualizzare lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun utente che si sta clonando.

Per ulteriori informazioni, vedere "Clonare utenti e gruppi tenant".

Eliminare uno o più utenti locali

È possibile eliminare in modo permanente uno o più utenti locali che non hanno più bisogno di accedere all'account tenant StorageGRID.

> Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si elimina un utente locale, StorageGRID non eliminerà l'utente corrispondente sull'altra griglia. Se è necessario mantenere queste informazioni sincronizzate, è necessario eliminare lo stesso utente da entrambe le griglie.

> Per eliminare gli utenti federati, è necessario utilizzare l'origine delle identità federate.

Fasi

1. Selezionare **Gestione accessi** > **Utenti**.

2. Selezionare la casella di controllo per ciascun utente che si desidera eliminare.
3. Selezionare **azioni** > **Elimina utente** o **azioni** > **Elimina utenti**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Delete user** (Elimina utente) o **Delete users** (Elimina utenti).

Gestire le chiavi di accesso S3

Gestire le chiavi di accesso S3

Ogni utente di un account tenant S3 deve disporre di una chiave di accesso per memorizzare e recuperare oggetti nel sistema StorageGRID. Una chiave di accesso è costituita da un ID della chiave di accesso e da una chiave di accesso segreta.

Le chiavi di accesso S3 possono essere gestite come segue:

- Gli utenti che dispongono dell'autorizzazione **Gestisci le tue credenziali S3** possono creare o rimuovere le proprie chiavi di accesso S3.
- Gli utenti che dispongono dell'autorizzazione **Root access** possono gestire le chiavi di accesso per l'account root S3 e tutti gli altri utenti. Le chiavi di accesso root forniscono l'accesso completo a tutti i bucket e gli oggetti per il tenant, a meno che non siano esplicitamente disabilitate da una policy bucket.

StorageGRID supporta l'autenticazione Firma versione 2 e Firma versione 4. L'accesso multiaccount non è consentito a meno che non sia esplicitamente abilitato da una policy bucket.

Creare le proprie chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare le proprie chiavi di accesso S3. Per accedere ai bucket e agli oggetti, è necessario disporre di una chiave di accesso.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestisci le tue credenziali S3 o l'autorizzazione di accesso root".

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 che consentono di creare e gestire i bucket per l'account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quante ne hai bisogno ed eliminare le chiavi che non stai utilizzando. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

- Impostare una scadenza per le chiavi in modo da limitare l'accesso a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre il rischio in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono

rimosse automaticamente.

- Se il rischio di sicurezza nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare un periodo di scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.

> È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.

   Viene visualizzata la pagina My access keys (i miei tasti di accesso) che elenca tutti i tasti di accesso esistenti.

2. Selezionare **Crea chiave**.
3. Effettuare una delle seguenti operazioni:
   - Selezionare **non impostare una scadenza** per creare una chiave che non scadrà. (Impostazione predefinita)
   - Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.

     > La data di scadenza può essere un massimo di cinque anni dalla data corrente. La scadenza può essere di almeno un minuto dall'ora corrente.

4. Selezionare **Crea chiave di accesso**.

   Viene visualizzata la finestra di dialogo Download access key (Scarica chiave di accesso), in cui sono elencati l'ID della chiave di accesso e la chiave di accesso segreta.

5. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   > Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni. Una volta chiusa la finestra di dialogo, non è possibile copiare o scaricare le chiavi.

6. Selezionare **fine**.

   La nuova chiave è elencata nella pagina i miei tasti di accesso.

7. Se l'account tenant dispone dell'autorizzazione **use grid Federation Connection**, utilizzare facoltativamente l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedere "Clonare le chiavi di accesso S3 utilizzando l'API".

Visualizzare le chiavi di accesso S3

Se si utilizza un locatario S3 e si dispone di "autorizzazione appropriata", è possibile visualizzare un elenco delle chiavi di accesso S3. È possibile ordinare l'elenco in base alla data di scadenza, in modo da determinare quali chiavi scadranno a breve. Se necessario, è possibile "creare nuove chiavi" o "eliminare le chiavi" che non si sta più utilizzando.

> È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone delle credenziali Manage your own S3 "permesso"(Gestisci le proprie credenziali 3D).

Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.
2. Dalla pagina My access keys (i miei tasti di accesso), ordinare le chiavi di accesso esistenti in base a **Expiration Time** (ora di scadenza) o **Access key ID** (ID chiave di accesso).
3. Se necessario, creare nuove chiavi o eliminare le chiavi che non si stanno più utilizzando.

   Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, è possibile iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

   Le chiavi scadute vengono rimosse automaticamente.

Eliminare le proprie chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le proprie chiavi di accesso S3. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- Si dispone di "Gestisci le tue autorizzazioni per le credenziali S3".

> È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **STORAGE (S3)** > **My access key**.

2. Nella pagina i miei tasti di accesso, selezionare la casella di controllo per ciascun tasto di accesso che si desidera rimuovere.
3. Selezionare **Delete key** (Elimina chiave).
4. Nella finestra di dialogo di conferma, selezionare **Elimina tasto**.

   Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina.

Creare le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare chiavi di accesso S3 per altri utenti, ad esempio applicazioni che richiedono l'accesso a bucket e oggetti.

Prima di iniziare

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

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 per altri utenti in modo che possano creare e gestire i bucket per il proprio account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quelle richieste dall'utente ed eliminare le chiavi che non vengono utilizzate. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

- Impostare una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre i rischi in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio di protezione nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare un tempo di scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.

> È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **Gestione accessi** > **Utenti**.
2. Selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

   Viene visualizzata la pagina User Detail (Dettagli utente).

3. Selezionare **Access keys**, quindi selezionare **Create key**.

4. Effettuare una delle seguenti operazioni:
   - Selezionare **non impostare un tempo di scadenza** per creare una chiave che non scade. (Impostazione predefinita)
   - Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.

   > La data di scadenza può essere un massimo di cinque anni dalla data corrente. La scadenza può essere di almeno un minuto dall'ora corrente.

5. Selezionare **Crea chiave di accesso**.

   Viene visualizzata la finestra di dialogo Download access key (Scarica chiave di accesso), che elenca l'ID della chiave di accesso e la chiave di accesso segreta.

6. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   > Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni. Una volta chiusa la finestra di dialogo, non è possibile copiare o scaricare le chiavi.

7. Selezionare **fine**.

   La nuova chiave è elencata nella scheda Access Keys della pagina User Details (Dettagli utente).

8. Se l'account tenant dispone dell'autorizzazione **use grid Federation Connection**, utilizzare facoltativamente l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedere "Clonare le chiavi di accesso S3 utilizzando l'API".

Visualizzare le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile visualizzare le chiavi di accesso S3 di un altro utente. È possibile ordinare l'elenco in base all'ora di scadenza, in modo da determinare quali chiavi scadranno a breve. Se necessario, è possibile creare nuove chiavi ed eliminare chiavi che non sono più in uso.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- Si dispone di "Autorizzazione di accesso root".

> È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **Gestione accessi** > **Utenti**.

2. Nella pagina utenti, selezionare l'utente di cui si desidera visualizzare i tasti di accesso S3.
3. Nella pagina User details (Dettagli utente), selezionare **Access keys** (chiavi di accesso).
4. Ordinare le chiavi in base a **scadenza** o **ID chiave di accesso**.
5. Se necessario, creare nuove chiavi ed eliminare manualmente le chiavi che non sono più in uso.

   Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, l'utente può iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

   Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

- "Creare le chiavi di accesso S3 di un altro utente"
- "Eliminare le chiavi di accesso S3 di un altro utente"

Eliminare le chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le chiavi di accesso S3 di un altro utente. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- Si dispone di "Autorizzazione di accesso root".

> È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **Gestione accessi** > **Utenti**.
2. Nella pagina utenti, selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.
3. Nella pagina User details (Dettagli utente), selezionare **Access keys** (chiavi di accesso), quindi selezionare la casella di controllo per ogni chiave di accesso che si desidera eliminare.
4. Selezionare **azioni** > **Elimina tasto selezionato**.
5. Nella finestra di dialogo di conferma, selezionare **Elimina tasto**.

   Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina.

Gestire i bucket S3

Creare un bucket S3

È possibile utilizzare Tenant Manager per creare bucket S3 per i dati dell'oggetto.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone dell'accesso root o Gestisci tutti i bucket "permesso". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

> Le autorizzazioni per impostare o modificare le proprietà di blocco degli oggetti S3 di bucket o oggetti possono essere concesse da"policy bucket o policy di gruppo" .

- Se si prevede di attivare il blocco oggetti S3 per un bucket, un amministratore della griglia ha attivato l'impostazione globale di blocco oggetti S3 per il sistema StorageGRID e sono stati esaminati i requisiti per i bucket e gli oggetti blocco oggetti S3.
- Se ogni tenant avrà 5.000 bucket, ogni nodo storage nella griglia ha un minimo di 64 GB di RAM.

> Ogni griglia può avere un massimo di 100.000 bucket, inclusi"secchi di rami" .

Accedere alla procedura guidata

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
2. Selezionare **Crea bucket**.

Inserire i dettagli

Fasi

1. Inserire i dettagli del bucket.

Campo	Descrizione
Nome bucket	Un nome per il bucket conforme alle seguenti regole: • Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). • Deve essere conforme al DNS. • Deve contenere almeno 3 e non più di 63 caratteri. • Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. • Non deve contenere periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. Per ulteriori informazioni, vedere "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione del bucket". **Nota**: Non è possibile modificare il nome del bucket dopo averlo creato.

Campo	Descrizione
Regione	La regione del bucket. L'amministratore StorageGRID gestisce le regioni disponibili. La regione di un bucket può influire sulla politica di protezione dei dati applicata agli oggetti. Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione. Se la regione predefinita è configurata su una regione diversa da `us-east-1` , questa altra regione viene inizialmente selezionata nel menu a discesa. **Nota**: Non è possibile modificare l'area dopo aver creato il bucket.

2. Selezionare **continua**.

Gestire le impostazioni

Fasi

1. Facoltativamente, attivare il controllo della versione degli oggetti per il bucket.

   Abilitare la versione degli oggetti se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto in base alle esigenze.

   È necessario abilitare il controllo delle versioni degli oggetti se:

   - Il bucket verrà utilizzato per la replica tra griglie.
   - Vuoi creare un"secchio di rami" da questo secchio.

2. Se l'impostazione globale S3 Object Lock (blocco oggetti S3) è attivata, attivare facoltativamente S3 Object Lock (blocco oggetti S3) per memorizzare gli oggetti utilizzando un modello WORM (Write-Once-Read-Many).

   Attivare il blocco oggetti S3 per un bucket solo se è necessario mantenere gli oggetti per un periodo di tempo fisso, ad esempio per soddisfare determinati requisiti normativi. S3 Object Lock è un'impostazione permanente che consente di evitare l'eliminazione o la sovrascrittura degli oggetti per un periodo di tempo fisso o indefinito.

   > Una volta attivata l'impostazione S3 Object Lock per un bucket, non è possibile disattivarla. Chiunque disponga delle autorizzazioni corrette può aggiungere a questo bucket oggetti che non possono essere modificati. Potrebbe non essere possibile eliminare questi oggetti o il bucket stesso.

   Se si attiva il blocco oggetti S3 per un bucket, il controllo della versione del bucket viene attivato automaticamente.

3. Se si seleziona **Enable S3 Object Lock** (attiva blocco oggetti S3), attivare facoltativamente **Default Retention** per questo bucket.

   > L'amministratore di rete deve concedere l'autorizzazione a "Utilizzare funzioni specifiche di blocco oggetti S3".

   Quando l'opzione **Default Retention** (conservazione predefinita) è attivata, i nuovi oggetti aggiunti al bucket saranno automaticamente protetti dall'eliminazione o dalla sovrascrittura. L'impostazione **Default Retention** non si applica agli oggetti che hanno periodi di conservazione propri.

a. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare una **modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Governance	• Gli utenti con `s3:BypassGovernanceRetention` autorizzazione possono utilizzare l' `x-amz-bypass-governance-retention: true`intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. **Nota**: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.

b. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare il **Default Retention Period** (periodo di conservazione predefinito) per il bucket.

   Il **Default Retention Period** indica per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

Un *massimo* periodo di conservazione, che può essere un valore compreso tra 1 giorno e 100 anni, viene impostato quando l'amministratore di rete crea il tenant. Quando si imposta un periodo di conservazione *default*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedere all'amministratore di rete di aumentare o diminuire il periodo di conservazione massimo.

4. Facoltativamente, seleziona **Abilita limite di capacità**, inserisci un valore e seleziona l'unità di capacità.

   Il limite di capacità è la capacità massima disponibile per gli oggetti di questa benna. Questo valore rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).

   Se non viene impostato alcun limite, la capacità di questa benna è illimitata. Per ulteriori informazioni, fare riferimento "Utilizzo del limite di capacità" a.

5. Facoltativamente, seleziona **Abilita limite conteggio oggetti**.

   Il limite del conteggio degli oggetti è il numero massimo di oggetti che questo bucket può contenere. Questo valore rappresenta un importo logico (conteggio oggetti). Se non viene impostato alcun limite, il numero di oggetti è illimitato.

6. Selezionare **Crea bucket**.

   Il bucket viene creato e aggiunto alla tabella nella pagina Bucket.

7. In alternativa, selezionare **Vai alla pagina dettagli bucket** per "visualizza i dettagli del bucket" ed eseguire una configurazione aggiuntiva.

Puoi anche"creare bucket di rami" secondo necessità.

Visualizza i dettagli del bucket

È possibile visualizzare i bucket nell'account tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione accesso root, Gestisci tutti i bucket o Visualizza tutti i bucket". Queste autorizzazioni hanno la precedenza sulle impostazioni di autorizzazione nei criteri di gruppo o bucket.

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.

   Viene visualizzata la pagina Bucket.

2. Rivedere la tabella di riepilogo per ciascun bucket.

   In base alle esigenze, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco in avanti e indietro.

   > I valori Conteggio oggetti, spazio utilizzato e utilizzo visualizzati sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi. Se nei bucket è attivata la versione, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

   Nome
   Il nome univoco del bucket, che non può essere modificato.

   Funzionalità attivate
   L'elenco delle funzioni attivate per il bucket.

   Blocco oggetti S3
   Se S3 Object Lock è attivato per il bucket.

   Questa colonna viene visualizzata solo se S3 Object Lock (blocco oggetti S3) è attivato per la griglia. Questa colonna mostra anche informazioni relative a qualsiasi bucket compatibile legacy.

   Regione
   La regione del bucket, che non può essere modificata. Questa colonna è nascosta per impostazione predefinita.

Numero di oggetti

Il numero di oggetti in questo bucket. Se nei bucket è attivata la versione, le versioni degli oggetti non correnti vengono incluse in questo valore.

Quando gli oggetti vengono aggiunti o cancellati, questo valore potrebbe non essere aggiornato immediatamente.

Spazio utilizzato

La dimensione logica di tutti gli oggetti nel bucket. La dimensione logica non include lo spazio effettivo richiesto per le copie replicate o codificate in cancellazione o per i metadati degli oggetti.

L'aggiornamento di questo valore può richiedere fino a 10 minuti.

Utilizzo

La percentuale utilizzata del limite di capacità della benna, se impostato.

Il valore di utilizzo si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID controlla il limite di capacità (se impostato) quando un tenant inizia a caricare gli oggetti e rifiuta le nuove acquisizioni in questo bucket se il tenant ha superato il limite di capacità. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente quando determina se il limite di capacità è stato superato. Se gli oggetti vengono eliminati, è possibile impedire temporaneamente a un tenant di caricare nuovi oggetti in questo bucket fino a quando l'utilizzo del limite di capacità non viene ricalcolato. I calcoli possono richiedere 10 minuti o più.

Questo valore indica le dimensioni logiche, non quelle fisiche necessarie per memorizzare gli oggetti e i relativi metadati.

Capacità

Se impostato, il limite di capacità per la benna.

Data di creazione

La data e l'ora di creazione del bucket. Questa colonna è nascosta per impostazione predefinita.

3. Per visualizzare i dettagli di un bucket specifico, selezionare il nome del bucket dalla tabella.
   a. Visualizzare le informazioni di riepilogo nella parte superiore della pagina Web per confermare i dettagli per il bucket, come ad esempio il numero di aree e oggetti.
   b. Visualizza le barre di utilizzo del limite di capacità e del limite di utilizzo del numero di oggetti. Se l'utilizzo è pari al 100% o vicino al 100%, valutare l'aumento del limite o l'eliminazione di alcuni oggetti.
   c. Se necessario, selezionare **Elimina oggetti nel bucket** e **Elimina bucket**.

Prestare particolare attenzione alle precauzioni visualizzate quando si seleziona ciascuna di queste opzioni. Per ulteriori informazioni, fare riferimento a:

- "Elimina tutti gli oggetti in un bucket"
- "Eliminare un bucket" (la benna deve essere vuota)

   d. Visualizzare o modificare le impostazioni del bucket in ciascuna delle schede, secondo necessità.
      - **S3 Console**: Consente di visualizzare gli oggetti per il bucket. Per ulteriori informazioni, fare riferimento a "Utilizzare la console S3".
      - **Opzioni bucket**: Consente di visualizzare o modificare le impostazioni delle opzioni. Alcune impostazioni, come blocco oggetti S3, non possono essere modificate dopo la creazione del

bucket.

  - "Gestire la coerenza del bucket"
  - "Aggiornamenti dell'ora dell'ultimo accesso"
  - "Limite di capacità"
  - "Limite del conteggio degli oggetti"
  - "Versione degli oggetti"
  - "Blocco oggetti S3"
  - "Ritenzione bucket predefinita"
  - "Gestire la replica cross-grid" (se consentito per il tenant)
- **Platform Services**: "Gestire i servizi della piattaforma" (Se consentito per il locatario)
- **Accesso bucket**: Consente di visualizzare o modificare le impostazioni delle opzioni. È necessario disporre di autorizzazioni di accesso specifiche.
  - Configurare"CORS per bucket e oggetti" in modo che il bucket e gli oggetti al suo interno siano accessibili alle applicazioni web in altri domini.
  - "Controllo dell'accesso degli utenti" Per un secchio S3 e oggetti in quel secchio.
- **Rami**: visualizza l'elenco dei bucket di rami per il bucket. "Crea un nuovo bucket di filiale o gestisci i bucket di filiale" .

Cos'è un branch bucket?

Un bucket di diramazione fornisce l'accesso agli oggetti in un bucket così come esistevano in un determinato momento.

Si crea un bucket di diramazione da un bucket esistente. Dopo aver creato un bucket di diramazione, il bucket originale da cui è stato creato viene chiamato *bucket di base*. Inoltre, è possibile creare un bucket di diramazione da un altro bucket di diramazione.

Un bucket di diramazione fornisce l'accesso ai dati protetti, ma non funge da backup. Per continuare a proteggere i dati, utilizzare queste funzionalità sui bucket di base:

- "Blocco oggetti S3"
- "Replica cross-grid"per secchi di base
- "Criteri dei bucket"per i bucket con versione per ripulire le vecchie versioni degli oggetti

Si noti le seguenti caratteristiche dei bucket di diramazione:

- È possibile accedere agli oggetti nei bucket di diramazione utilizzando"Console S3 per scaricare oggetti" .
- Quando i client accedono agli oggetti in un bucket di diramazione, il bucket di diramazione"politiche di accesso" , anziché le policy del bucket di base, determinano se l'accesso è concesso o negato.
- Gli oggetti creati in un bucket di base vengono valutati in base a come"Regole ILM" applicare al secchio di base. Gli oggetti creati in un bucket di diramazione vengono valutati in base al modo in cui le regole ILM si applicano al bucket di diramazione.
- La replica tra griglie non è supportata per i bucket branch.
- I servizi della piattaforma non sono supportati per i bucket di filiale.

Esempi di utilizzo del bucket di diramazione

- È possibile utilizzare un branch bucket per rimuovere oggetti danneggiati creando un branch bucket da un punto nel tempo precedente al verificarsi del danneggiamento e quindi indirizzando le applicazioni al branch bucket anziché al bucket di base che contiene oggetti danneggiati.
- Stai salvando i dati in un bucket con versione. Si è verificata una vulnerabilità accidentale che ha causato l'ingestione di molti oggetti indesiderati dopo il tempo *T*. È possibile creare un bucket di diramazione per il valore temporale Prima, *T*, e reindirizzare le operazioni client a tale bucket di diramazione. Quindi, solo gli oggetti ingeriti prima del tempo precedente *T* vengono esposti ai client.

Operazioni sugli oggetti nei bucket di diramazione

- Un'operazione PUT su un bucket di ramo crea un oggetto nel ramo.
- Un'operazione GET su un bucket di diramazione recupera un oggetto dal diramazione. Se l'oggetto non esiste nel bucket di diramazione, viene recuperato dal bucket di base.
- Le eliminazioni di oggetti dai bucket di diramazione avvengono come segue:

Operazione	Bersaglio	Risultato	Visibilità dell'oggetto nel bucket di base	Visibilità dell'oggetto nel bucket di diramazione
Elimina senza ID versione	Secchio di base	L'indicatore di eliminazione viene creato solo per il bucket di base	HEAD/GET restituisce L'oggetto non esiste, ma è ancora possibile accedere a versioni specifiche	HEAD/GET restituisce che l'oggetto esiste e che è ancora possibile accedere a versioni specifiche Il marcatore di eliminazione sarebbe stato creato dopo il bucket del ramo `beforeTime` .
Elimina con ID versione	Secchio di base	La versione specifica dell'oggetto viene eliminata sia per il bucket base che per quello branch	HEAD/GET restituisce La versione dell'oggetto non esiste	HEAD/GET restituisce La versione dell'oggetto non esiste
Elimina senza ID versione	Secchio per rami	Il marcatore di eliminazione viene creato solo per il bucket del ramo	HEAD/GET restituisce l'oggetto (l'oggetto bucket di base non è interessato)	HEAD/GET restituisce L'oggetto non esiste
Elimina con ID versione	Secchio per rami	La versione specifica dell'oggetto viene eliminata solo per il bucket di diramazione	HEAD/GET restituisce una versione specifica dell'oggetto (l'oggetto bucket di base non è interessato)	HEAD/GET restituisce La versione dell'oggetto non esiste

Fare riferimento anche a"Modalità di eliminazione degli oggetti con versione S3" .

Gestisci i bucket delle filiali

Utilizzare Tenant Manager per creare e visualizzare i dettagli dei bucket delle filiali.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un"browser web supportato" .
- Appartieni a un gruppo di utenti che ha accesso Root o"Gestisci autorizzazioni per tutti i bucket" . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- Il bucket di base da cui vuoi creare un ramo ha"controllo delle versioni abilitato" .
- Sei il proprietario del secchio base.

A proposito di questa attività

Notare le seguenti informazioni per i bucket di diramazione:

- Le autorizzazioni per impostare le proprietà di blocco degli oggetti S3 di bucket o oggetti possono essere concesse da"policy bucket o policy di gruppo" .
- Se si sospende il controllo delle versioni sul bucket di base, il contenuto del bucket di base non sarà più visibile nei relativi bucket rami.

> Dopo aver configurato e creato un bucket di diramazione, non è possibile modificare la configurazione.

Crea bucket di diramazione

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
2. Seleziona il bucket da cui vuoi creare un ramo (il "bucket di base").
3. Nella pagina dei dettagli del bucket, seleziona **Rami** > **Crea bucket ramo**.

   Il pulsante **Crea bucket di diramazione** è disabilitato se il bucket di base non ha il controllo delle versioni abilitato.

Inserire i dettagli

Fasi

1. Inserisci i dettagli per il bucket della filiale.

Campo	Descrizione
Nome del bucket di filiale	Un nome per il bucket di diramazione che rispetti queste regole: • Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). • Deve essere conforme al DNS. • Deve contenere almeno 3 e non più di 63 caratteri. • Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. • Non deve contenere periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. Per ulteriori informazioni, vedere "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione del bucket". **Nota**: non è possibile modificare il nome dopo aver creato il bucket di diramazione.
Regione (non modificabile per i bucket di filiale)	Regione del bucket del ramo. La regione del bucket di diramazione deve corrispondere alla regione del bucket di base, pertanto questo campo è disabilitato per i bucket di diramazione.
Prima del tempo	Tempo limite entro il quale le versioni degli oggetti create nel bucket di base devono essere accessibili dal bucket di diramazione. Il bucket branch fornisce l'accesso alle versioni degli oggetti create prima del tempo Prima. Prima del tempo deve esserci una data e un'ora trascorse. Non può essere una data futura.
Tipo di secchio per rami	• **Lettura-scrittura**: è possibile aggiungere o eliminare oggetti o versioni di oggetti nel bucket del ramo. • **Sola lettura**: non è possibile modificare gli oggetti nel bucket del ramo. **Nota**: è possibile impostare il tipo di bucket di diramazione su sola lettura solo se il bucket di diramazione è vuoto. Se il tipo per un bucket di branch esistente è impostato su lettura-scrittura e non hai scritto su di esso, puoi modificare il tipo in sola lettura.

2. Selezionare **continua**.

Gestisci le impostazioni dell'oggetto (facoltativo)

Le impostazioni degli oggetti per un bucket di diramazione non influiscono sulle versioni degli oggetti nel bucket di base.

Fasi

1. Se l'impostazione globale S3 Object Lock è abilitata, abilitare facoltativamente S3 Object Lock per il bucket

branch. Per abilitare S3 Object Lock, il bucket di diramazione deve essere un bucket di lettura-scrittura.

Abilitare S3 Object Lock per un bucket di diramazione solo se è necessario conservare gli oggetti per un periodo di tempo fisso, ad esempio per soddisfare determinati requisiti normativi. S3 Object Lock è un'impostazione permanente che consente di impedire che gli oggetti vengano eliminati o sovrascritti per un periodo di tempo fisso o indefinitamente.

> Dopo aver abilitato l'impostazione Blocco oggetto S3 per un bucket, non è più possibile disattivarla. Chiunque disponga delle autorizzazioni corrette può aggiungere al bucket del ramo oggetti che non possono essere modificati. Potresti non essere in grado di eliminare questi oggetti o il bucket di diramazione stesso.

2. Se hai selezionato **Abilita blocco oggetto S3**, abilita facoltativamente **Conservazione predefinita** per il bucket di diramazione.

> L'amministratore di rete deve concedere l'autorizzazione a "Utilizzare funzioni specifiche di blocco oggetti S3".

Quando è abilitata la **Conservazione predefinita**, i nuovi oggetti aggiunti al bucket del ramo saranno automaticamente protetti dall'eliminazione o dalla sovrascrittura. L'impostazione **Conservazione predefinita** non si applica agli oggetti che hanno un proprio periodo di conservazione.

a. Se è abilitata l'opzione **Conservazione predefinita**, specificare una **Modalità di conservazione predefinita** per il bucket di filiale.

Modalità di conservazione predefinita	Descrizione
Governance	• Gli utenti con `s3:BypassGovernanceRetention` autorizzazione possono utilizzare l' `x-amz-bypass-governance-retention: true`intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. **Nota**: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.

b. Se è abilitata l'opzione **Conservazione predefinita**, specificare il **Periodo di conservazione predefinito** per il bucket di filiale.

Il **Periodo di conservazione predefinito** indica per quanto tempo i nuovi oggetti aggiunti al bucket di

diramazione devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

Un *massimo* periodo di conservazione, che può essere un valore compreso tra 1 giorno e 100 anni, viene impostato quando l'amministratore di rete crea il tenant. Quando si imposta un periodo di conservazione *default*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedere all'amministratore di rete di aumentare o diminuire il periodo di conservazione massimo.

3. Facoltativamente, seleziona **Abilita limite di capacità**.

   Il limite di capacità è la capacità massima disponibile per il bucket di diramazione. Questo valore rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione su disco).

   Se non viene impostato alcun limite, la capacità del bucket di filiale è illimitata. Fare riferimento a "Utilizzo del limite di capacità" per maggiori informazioni.

   > Questa impostazione si applica solo agli oggetti inseriti direttamente nel bucket di diramazione e non agli oggetti visibili dal bucket di base attraverso il bucket di diramazione.

4. Facoltativamente, seleziona **Abilita limite conteggio oggetti**.

   Il limite del conteggio degli oggetti è il numero massimo di oggetti che il bucket di diramazione può contenere. Questo valore rappresenta un importo logico (conteggio oggetti). Se non viene impostato alcun limite, il numero di oggetti è illimitato.

   > Questa impostazione si applica solo agli oggetti inseriti direttamente nel bucket di diramazione e non agli oggetti visibili dal bucket di base attraverso il bucket di diramazione.

5. Selezionare **Crea bucket**.

   Il bucket di diramazione viene creato e aggiunto alla tabella nella pagina Bucket.

6. Facoltativamente, seleziona **Vai alla pagina dei dettagli del bucket** per"visualizza i dettagli del bucket di filiale" ed eseguire configurazioni aggiuntive.

   Nella pagina Dettagli bucket, alcune opzioni di configurazione relative alla modifica degli oggetti sono disabilitate per i bucket di sola lettura.

Applicare un tag di criterio ILM a un bucket

Scegli un tag di policy ILM da applicare a un bucket in base ai tuoi requisiti di storage a oggetti.

Il criterio ILM controlla la posizione di memorizzazione dei dati dell'oggetto e se vengono eliminati dopo un determinato periodo di tempo. L'amministratore di grid crea criteri ILM e li assegna ai tag dei criteri ILM quando si utilizzano più criteri attivi.

> Evitare di riassegnare frequentemente il tag di un bucket. In caso contrario, potrebbero verificarsi problemi di prestazioni.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione accesso root, Gestisci tutti i bucket o Visualizza tutti i bucket". Queste autorizzazioni hanno la precedenza sulle impostazioni di autorizzazione nei criteri di gruppo o bucket.

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.

   Viene visualizzata la pagina Bucket. In base alle esigenze, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco in avanti e indietro.

2. Selezionare il nome del bucket a cui si desidera assegnare un tag di criterio ILM.

   È inoltre possibile modificare l'assegnazione dei tag dei criteri ILM per un bucket a cui è già stato assegnato un tag.

   I valori Object Count (Conteggio oggetti) e Space used (spazio utilizzato) visualizzati sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi. Se nei bucket è attivata la versione, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

3. Nella scheda Opzioni bucket, espandere il tag criterio ILM fisarmonica. Questa fisarmonica viene visualizzata solo se l'amministratore della griglia ha attivato l'uso di tag di criteri personalizzati.
4. Leggere la descrizione di ciascun tag di criterio per determinare quale tag applicare al bucket.

   La modifica del tag di criterio ILM per un bucket attiva la rivalutazione ILM di tutti gli oggetti nel bucket. Se la nuova policy mantiene gli oggetti per un periodo di tempo limitato, gli oggetti meno recenti verranno eliminati.

5. Selezionare il pulsante di opzione per il tag che si desidera assegnare al bucket.
6. Selezionare **Save Changes** (Salva modifiche). Sul bucket viene impostata una nuova etichetta bucket S3 con la chiave `NTAP-SG-ILM-BUCKET-TAG` e il valore del tag criterio ILM.

   Assicurarsi che le applicazioni S3 non sovrascrivano o eliminino accidentalmente la nuova etichetta del bucket. Se questo tag viene omesso quando si applica un nuovo TagSet al bucket, gli oggetti nel bucket torneranno a essere valutati in base al criterio ILM predefinito.

   Impostare e modificare i tag dei criteri ILM utilizzando solo l'API di Tenant Manager o di Tenant Manager in cui il tag dei criteri ILM viene convalidato. Non modificare il `NTAP-SG-ILM-BUCKET-TAG` tag dei criteri ILM utilizzando l'API S3 PutBucketTagging o l'API S3 DeleteBucketTagging.

   La modifica del tag della policy assegnato a un bucket ha un impatto temporaneo sulle performance, mentre gli oggetti vengono rivalutati utilizzando la nuova policy ILM.

Gestire le policy del bucket

È possibile controllare l'accesso utente per un bucket S3 e gli oggetti in tale bucket.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root". Le autorizzazioni Visualizza tutti i bucket e Gestisci tutti i bucket consentono solo la visualizzazione.
- Hai verificato che il numero richiesto di nodi e siti storage è disponibile. Se due o più nodi di archiviazione non sono disponibili all'interno di un sito o se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

Fasi

1. Selezionare **bucket**, quindi selezionare il bucket che si desidera gestire.
2. Nella pagina dei dettagli del bucket, selezionare **accesso al bucket** > **criterio del bucket**.
3. Effettuare una delle seguenti operazioni:
   - Immettere un criterio bucket selezionando la casella di controllo **Abilita criterio**. Quindi immettere una stringa formattata JSON valida.

     Ogni criterio bucket ha un limite di dimensioni di 20.480 byte.

   - Modificare un criterio esistente modificando la stringa.
   - Disattivare un criterio deselezionando **attiva criterio**.

Per informazioni dettagliate sui criteri bucket, inclusi esempi e sintassi del linguaggio, vedere "Esempio di policy bucket".

Gestire la coerenza del bucket

I valori di coerenza possono essere utilizzati per specificare la disponibilità delle modifiche alle impostazioni del bucket e per fornire un equilibrio tra la disponibilità degli oggetti all'interno di un bucket e la coerenza di tali oggetti in diversi nodi e siti di archiviazione. È possibile modificare i valori di coerenza in modo che siano diversi dai valori predefiniti in modo che le applicazioni client possano soddisfare le proprie esigenze operative.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

Linee guida per la coerenza della benna

La coerenza del bucket viene utilizzata per determinare la coerenza delle applicazioni client che influiscono sugli oggetti all'interno del bucket S3. In generale, si dovrebbe usare la coerenza **Read-after-new-write** per i propri bucket.

modificare la coerenza del bucket

Se la coerenza **Read-after-new-write** non soddisfa i requisiti dell'applicazione client, è possibile modificare la coerenza impostando la coerenza del bucket o utilizzando l' `Consistency-Control`intestazione. La `Consistency-Control` testata esclude la coerenza della benna.

Quando si modifica la consistenza di un bucket, solo gli oggetti che vengono acquisiti dopo la modifica sono garantiti per soddisfare l'impostazione modificata.

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **.
4. Selezionare una coerenza per le operazioni eseguite sugli oggetti in questo bucket.
   - **Tutti**: Offre il massimo livello di coerenza. Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
   - **Strong-Global**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
   - **Strong-Site**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
   - **Read-after-new-write** (valore predefinito): Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
   - **Available**: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.
5. Selezionare **Save Changes** (Salva modifiche).

Cosa accade quando si modificano le impostazioni della benna

I bucket hanno impostazioni multiple che influiscono sul comportamento dei bucket e degli oggetti all'interno di tali bucket.

Per impostazione predefinita, le seguenti impostazioni del bucket utilizzano la coerenza **strong**. Se due o più nodi di archiviazione non sono disponibili all'interno di un sito o se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

- "Eliminazione bucket vuoto in background"
- "Ora ultimo accesso"
- "Ciclo di vita del bucket"
- "Politica del bucket"
- "Etichettatura della benna"
- "Versione bucket"
- "Blocco oggetti S3"
- "Crittografia bucket"

Il valore di coerenza per la versione bucket, blocco oggetto S3 e crittografia bucket non può essere impostato su un valore non fortemente coerente.

Le seguenti impostazioni della benna non utilizzano una forte coerenza e hanno una maggiore disponibilità per le modifiche. Le modifiche a queste impostazioni potrebbero richiedere del tempo prima di avere effetto.

- "Configurazione dei servizi della piattaforma: Integrazione di notifica, replica o ricerca"
- "Configurare StorageGRID CORS per bucket e oggetti"
- Modificare la coerenza della benna

Se la coerenza predefinita utilizzata durante la modifica delle impostazioni del bucket non soddisfa i requisiti dell'applicazione client, è possibile modificare la coerenza utilizzando l'`Consistency-Control` intestazione per "API REST S3"o utilizzando le `force` opzioni o `reducedConsistency` in "API di gestione del tenant".

Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso

Quando gli amministratori della griglia creano le regole ILM (Information Lifecycle Management) per un sistema StorageGRID, possono facoltativamente specificare che l'ultimo tempo di accesso di un oggetto deve essere utilizzato per determinare se spostare l'oggetto in una posizione di storage diversa. Se si utilizza un tenant S3, è possibile sfruttare tali regole attivando gli ultimi aggiornamenti del tempo di accesso per gli oggetti in un bucket S3.

Queste istruzioni si applicano solo ai sistemi StorageGRID che includono almeno una regola ILM che utilizza l'opzione **ultimo tempo di accesso** come filtro avanzato o come tempo di riferimento. È possibile ignorare queste istruzioni se il sistema StorageGRID non include tale regola. Per ulteriori informazioni, vedere "USA l'ultimo tempo di accesso nelle regole ILM" .

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

A proposito di questa attività

Ultimo tempo di accesso è una delle opzioni disponibili per l'istruzione di posizionamento **tempo di riferimento** per una regola ILM. L'impostazione del tempo di riferimento per una regola su ultimo tempo di accesso consente agli amministratori della griglia di specificare che gli oggetti devono essere posizionati in determinate posizioni di storage in base al momento dell'ultimo recupero (lettura o visualizzazione) di tali oggetti.

Ad esempio, per garantire che gli oggetti visualizzati di recente rimangano sullo storage più veloce, un amministratore della griglia può creare una regola ILM specificando quanto segue:

- Gli oggetti recuperati nell'ultimo mese devono rimanere sui nodi di storage locali.
- Gli oggetti che non sono stati recuperati nell'ultimo mese devono essere spostati in una posizione off-site.

Per impostazione predefinita, gli aggiornamenti dell'ultimo tempo di accesso sono disattivati. Se il sistema StorageGRID include una regola ILM che utilizza l'opzione **ultimo tempo di accesso** e si desidera che questa

opzione venga applicata agli oggetti in questo bucket, è necessario abilitare gli aggiornamenti dell'ultimo tempo di accesso per i bucket S3 specificati in tale regola.

> L'aggiornamento dell'ultimo tempo di accesso durante il recupero di un oggetto può ridurre le prestazioni di StorageGRID, in particolare per gli oggetti di piccole dimensioni.

Si verifica un impatto sulle performance con gli ultimi aggiornamenti dell'orario di accesso, perché StorageGRID deve eseguire questi passaggi aggiuntivi ogni volta che vengono recuperati gli oggetti:

- Aggiornare gli oggetti con nuovi timestamp
- Aggiungere gli oggetti alla coda ILM, in modo che possano essere rivalutati in base alle regole e ai criteri ILM correnti

La tabella riassume il comportamento applicato a tutti gli oggetti nel bucket quando l'ultimo tempo di accesso è disattivato o attivato.

Tipo di richiesta	Comportamento se l'ultimo tempo di accesso è disattivato (impostazione predefinita)		Comportamento se è attivata l'ultima ora di accesso	
	Ultimo aggiornamento dell'orario di accesso?	Oggetto aggiunto alla coda di valutazione ILM?	Ultimo aggiornamento dell'orario di accesso?	Oggetto aggiunto alla coda di valutazione ILM?
Richiesta di recupero dei metadati di un oggetto quando viene emessa un'operazione HEAD	No	No	No	No
Richiesta di recuperare un oggetto, il relativo elenco di controllo degli accessi o i relativi metadati	No	No	Sì	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì	Sì	Sì
Richiesta di elencare gli oggetti o le versioni degli oggetti	No	No	No	No

Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione
Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **ultimi aggiornamenti dell'ora di accesso**.
4. Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso.
5. Selezionare **Save Changes** (Salva modifiche).

Modificare la versione degli oggetti per un bucket

Se si utilizza un tenant S3, è possibile modificare lo stato di versione per i bucket S3.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Hai verificato che il numero richiesto di nodi e siti storage è disponibile. Se due o più nodi di archiviazione non sono disponibili all'interno di un sito o se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

A proposito di questa attività

È possibile attivare o sospendere il controllo delle versioni degli oggetti per un bucket. Una volta attivata la versione per un bucket, non è possibile tornare allo stato senza versione. Tuttavia, è possibile sospendere il controllo delle versioni per il bucket.

- Disabled (Disattivato): La versione non è mai stata attivata
- Enabled (attivato): Il controllo delle versioni è attivato
- Suspended (sospeso): Il controllo delle versioni era stato precedentemente attivato e sospeso

Per ulteriori informazioni, vedere quanto segue:

- "Versione degli oggetti"
- "Regole e criteri ILM per gli oggetti con versione S3 (esempio 4)"

- "Modalità di eliminazione degli oggetti"

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **versione oggetto**.
4. Selezionare uno stato di versione per gli oggetti in questo bucket.

   La versione degli oggetti deve rimanere abilitata per un bucket utilizzato per la replica cross-grid. Se S3 Object Lock (blocco oggetti S3) o legacy compliance (compliance legacy) è attivato, le opzioni **Object versioning** (versione oggetto) sono disattivate.

Opzione	Descrizione
Abilitare il controllo delle versioni	Abilitare la versione degli oggetti se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto in base alle esigenze. Gli oggetti già presenti nel bucket verranno sottoposti alla versione quando vengono modificati da un utente.
Sospendere il controllo delle versioni	Sospendere la versione degli oggetti se non si desidera più creare nuove versioni degli oggetti. È comunque possibile recuperare le versioni di oggetti esistenti.

5. Selezionare **Save Changes** (Salva modifiche).

USA il blocco oggetti S3 per conservare gli oggetti

È possibile utilizzare il blocco oggetti S3 se i bucket e gli oggetti devono soddisfare i requisiti normativi per la conservazione.

L'amministratore della griglia deve concedere l'autorizzazione per utilizzare funzioni specifiche di blocco oggetti S3.

Che cos'è il blocco oggetti S3?

La funzione blocco oggetti StorageGRID S3 è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon Simple Storage Service (Amazon S3).

Quando l'impostazione blocco oggetto S3 globale è abilitata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza blocco oggetto S3 abilitato. Se un bucket ha S3 Object Lock attivato, è necessario il controllo della versione del bucket e viene attivato automaticamente.

Un bucket senza blocco oggetti S3 può avere solo oggetti senza impostazioni di conservazione specificate. Nessun oggetto acquisito avrà impostazioni di conservazione.

Un bucket con blocco oggetti S3 può avere oggetti con e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con blocco oggetto S3 e conservazione predefinita configurata può avere caricato oggetti con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, poiché l'impostazione di conservazione non è stata configurata a livello di oggetto.

In effetti, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurata la conservazione predefinita. Gli oggetti esistenti senza impostazioni di conservazione degli oggetti rimangono invariati.

Modalità di conservazione

La funzione blocco oggetti di StorageGRID S3 supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità equivalgono alle modalità di conservazione Amazon S3.

- In modalità compliance:
  - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
  - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità governance:
  - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare alcune impostazioni di conservazione.
  - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
  - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione**: Conformità o governance.
- **Mantieni-fino-data**: Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere cancellato.
- **Conservazione legale**: L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa. Le conservazioni legali sono indipendenti dalla conservazione fino alla data odierna.

  > Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

  Per informazioni dettagliate sulle impostazioni dell'oggetto, vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita**: Conformità o governance.
- **Default Retention Period** (periodo di conservazione predefinito): Per quanto tempo le nuove versioni degli oggetti aggiunte a questo bucket devono essere conservate, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di proprie impostazioni di conservazione. Gli oggetti bucket esistenti non vengono influenzati quando si aggiungono o si modificano queste impostazioni predefinite.

Vedere "Creare un bucket S3" e "Aggiorna la conservazione predefinita del blocco oggetti S3".

S3 attività di blocco degli oggetti

Gli elenchi seguenti per gli amministratori di grid e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzione blocco oggetti S3.

Amministratore di grid

- Attiva l'impostazione blocco oggetti S3 globale per l'intero sistema StorageGRID.
- Assicurarsi che i criteri ILM (Information Lifecycle Management) siano *conformi*, ovvero che soddisfino la "Requisiti dei bucket con blocco oggetti S3 abilitato".
- Se necessario, consentire a un tenant di utilizzare la modalità di conservazione Compliance. In caso contrario, è consentita solo la modalità Governance.
- In base alle necessità, imposta il periodo di conservazione massimo per un tenant.

Utente tenant

- Esaminare le considerazioni per bucket e oggetti con blocco oggetto S3.
- Se necessario, contattare l'amministratore della griglia per abilitare l'impostazione blocco oggetti S3 globale e impostare le autorizzazioni.
- Crea bucket con blocco oggetti S3 abilitato.
- Facoltativamente, configurare le impostazioni di conservazione predefinite per un bucket:
  - Modalità di conservazione predefinita: Governance o conformità, se consentita dall'amministratore della griglia.
  - Periodo di conservazione predefinito: Deve essere minore o uguale al periodo di conservazione massimo impostato dall'amministratore di rete.
- Utilizzare l'applicazione client S3 per aggiungere oggetti e impostare facoltativamente la conservazione specifica degli oggetti:
  - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore del grid.
  - Mantieni fino alla data: Deve essere minore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti per i bucket con S3 Object Lock attivato

- Se l'impostazione blocco oggetto S3 globale è attivata per il sistema StorageGRID, è possibile utilizzare Gestione tenant, API di gestione tenant o API REST S3 per creare bucket con blocco oggetto S3 attivato.

- Se si intende utilizzare il blocco oggetti S3, è necessario attivare il blocco oggetti S3 quando si crea il bucket. Impossibile attivare il blocco oggetti S3 per un bucket esistente.
- Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket. Non puoi disattivare il blocco oggetti S3 o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione e un periodo di conservazione predefiniti per ciascun bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di proprie impostazioni di conservazione. È possibile eseguire l'override di queste impostazioni predefinite specificando una modalità di conservazione e conservarla fino alla data per ogni versione dell'oggetto al momento del caricamento.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con blocco oggetti S3 attivato.
- La replica di CloudMirror non è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure le impostazioni di conservazione per ciascuna versione dell'oggetto. È possibile specificare le impostazioni di conservazione a livello di oggetto utilizzando l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di conservazione legale per un oggetto protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

Ciclo di vita degli oggetti nei bucket con S3 Object Lock attivato

Ogni oggetto salvato in un bucket con S3 Object Lock attivato passa attraverso le seguenti fasi:

1. **Acquisizione oggetto**

   Quando una versione dell'oggetto viene aggiunta al bucket con S3 Object Lock attivato, le impostazioni di conservazione vengono applicate come segue:

   - Se per l'oggetto sono specificate le impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
   - Se non sono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se presenti.
   - Se non sono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

   Se vengono applicate le impostazioni di conservazione, vengono protetti sia l'oggetto che i metadati S3 definiti dall'utente.

2. **Conservazione ed eliminazione degli oggetti**

   StorageGRID memorizza più copie di ciascun oggetto protetto per il periodo di conservazione specificato. Il numero e il tipo esatti delle copie degli oggetti e le posizioni dello storage sono determinati dalle regole di conformità nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla modalità di conservazione.

- Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Posso comunque gestire i bucket conformi alle versioni precedenti?

La funzione blocco oggetti S3 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Se sono stati creati bucket conformi utilizzando una versione precedente di StorageGRID, è possibile continuare a gestire le impostazioni di questi bucket; tuttavia, non è più possibile creare nuovi bucket conformi. Per istruzioni, vedere "Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5".

Aggiorna la conservazione predefinita del blocco oggetti S3

Se al momento della creazione del bucket è stato attivato il blocco oggetti S3, è possibile modificare il bucket per modificare le impostazioni di conservazione predefinite. È possibile attivare (o disattivare) la conservazione predefinita e impostare una modalità di conservazione e un periodo di conservazione predefiniti.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Il blocco oggetti S3 è attivato globalmente per il sistema StorageGRID e il blocco oggetti S3 è stato attivato quando è stato creato il bucket. Vedere "USA il blocco oggetti S3 per conservare gli oggetti".

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **S3 Object Lock**.
4. Facoltativamente, attivare o disattivare **Default Retention** per questo bucket.

   Le modifiche apportate a questa impostazione non si applicano agli oggetti già presenti nel bucket o a qualsiasi oggetto che potrebbe avere periodi di conservazione propri.

5. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare una **modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Governance	• Gli utenti con `s3:BypassGovernanceRetention` autorizzazione possono utilizzare l' `x-amz-bypass-governance-retention: true`intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. **Nota**: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.

6. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare il **Default Retention Period** (periodo di conservazione predefinito) per il bucket.

   Il **Default Retention Period** indica per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

   Un *massimo* periodo di conservazione, che può essere un valore compreso tra 1 giorno e 100 anni, viene impostato quando l'amministratore di rete crea il tenant. Quando si imposta un periodo di conservazione *default*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedere all'amministratore di rete di aumentare o diminuire il periodo di conservazione massimo.

7. Selezionare **Save Changes** (Salva modifiche).

Configurare StorageGRID CORS per bucket e oggetti

È possibile configurare la condivisione delle risorse cross-origin (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- Per le richieste di configurazione GET CORS, l'utente appartiene a un gruppo di utenti che dispone di "Gestisci tutti i bucket o Visualizza tutti i bucket". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Per le richieste di configurazione PUT CORS, l'utente appartiene a un gruppo di utenti che dispone di "Gestisci autorizzazioni per tutti i bucket". Questa autorizzazione sovrascrive le impostazioni delle

autorizzazioni nei criteri di gruppo o bucket.

- "Autorizzazione di accesso root"Fornisce l'accesso a tutte le richieste di configurazione CORS.

A proposito di questa attività

La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Ad esempio, si supponga di utilizzare un bucket S3 denominato `Images` per memorizzare la grafica. Configurando CORS per il `Images` bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito Web `http://www.example.com`.

Abilitare il CORS per un bucket

Fasi

1. Utilizzare un editor di testo per creare l'XML richiesto. Questo esempio mostra l'XML utilizzato per abilitare il CORS per un bucket S3. In particolare:
   - Consente a qualsiasi dominio di inviare richieste GET al bucket
   - Consente solo al `http://www.example.com` dominio di inviare richieste GET, POST ed ELIMINAZIONE
   - Sono consentite tutte le intestazioni delle richieste

   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedMethod>POST</AllowedMethod>
           <AllowedMethod>DELETE</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
   </CORSConfiguration>
   ```

   Per ulteriori informazioni sull'XML di configurazione CORS, vedere "Documentazione di Amazon Web Services (AWS): Guida utente di Amazon Simple Storage Service".

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

   Viene visualizzata la pagina dei dettagli del bucket.

4. Dalla scheda **bucket access**, selezionare la fisarmonica **Cross-Origin Resource Sharing (CORS)**.
5. Selezionare la casella di controllo **Enable CORS** (attiva CORS*).

6. Incollare l'XML di configurazione CORS nella casella di testo.
7. Selezionare **Save Changes** (Salva modifiche).

Modificare l'impostazione CORS

Fasi

1. Aggiornare l'XML di configurazione CORS nella casella di testo oppure selezionare **Clear** per ricominciare.
2. Selezionare **Save Changes** (Salva modifiche).

Disattiva l'impostazione CORS

Fasi

1. Deselezionare la casella di controllo **Enable CORS** (attiva CORS*).
2. Selezionare **Save Changes** (Salva modifiche).

Informazioni correlate

"Configurare StorageGRID CORS per un'interfaccia di gestione"

Eliminare gli oggetti nel bucket

È possibile utilizzare Tenant Manager per eliminare gli oggetti in uno o più bucket.

Considerazioni e requisiti

Prima di eseguire questa procedura, tenere presente quanto segue:

- Quando si eliminano gli oggetti in un bucket, StorageGRID rimuove in modo permanente tutti gli oggetti e tutte le versioni degli oggetti in ogni bucket selezionato da tutti i nodi e siti nel sistema StorageGRID. StorageGRID rimuove anche i metadati degli oggetti correlati. Non sarà possibile recuperare queste informazioni.
- L'eliminazione di tutti gli oggetti in un bucket può richiedere minuti, giorni o persino settimane, in base al numero di oggetti, copie di oggetti e operazioni simultanee.
- Se un bucket ha "Blocco oggetti S3 attivato", potrebbe rimanere nello stato **Deleting Objects: Read-only** per *years*.

  Un bucket che utilizza il blocco oggetti S3 rimarrà nello stato **Deleting Objects: Read-only** (eliminazione oggetti: Sola lettura) fino a quando non viene raggiunta la data di conservazione per tutti gli oggetti e non vengono rimosse le conservazioni legali.

- Durante l'eliminazione degli oggetti, lo stato del bucket è **eliminazione degli oggetti: Sola lettura**. In questo stato, non è possibile aggiungere nuovi oggetti al bucket.
- Una volta cancellati tutti gli oggetti, il bucket rimane in stato di sola lettura. È possibile eseguire una delle seguenti operazioni:
  - Riportare il bucket in modalità di scrittura e riutilizzarlo per nuovi oggetti
  - Eliminare il bucket
  - Mantenere il bucket in modalità di sola lettura per riservare il proprio nome per un utilizzo futuro
- Se in un bucket è attivata la versione oggetto, è possibile rimuovere i marcatori di eliminazione creati in StorageGRID 11,8 o versioni successive utilizzando le operazioni Elimina oggetti nel bucket.

- Se in un bucket è attivata la versione oggetto, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11,7 o versioni precedenti. Vedere le informazioni sull'eliminazione di oggetti in un bucket in "Modalità di eliminazione degli oggetti con versione S3".
- Se si utilizza "replica cross-grid", tenere presente quanto segue:
  - L'utilizzo di questa opzione non elimina alcun oggetto dal bucket dell'altra griglia.
  - Se si seleziona questa opzione per il bucket di origine, l'avviso **errore replica cross-grid** verrà attivato se si aggiungono oggetti al bucket di destinazione sull'altra griglia. Se non è possibile garantire che nessuno aggiungerà oggetti al bucket sull'altra griglia, "disattiva la replica cross-grid" per quel bucket prima di eliminare tutti gli oggetti bucket.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root". Questa autorizzazione sovrascrive le impostazioni delle autorizzazioni nei criteri di gruppo o bucket.

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.

   Viene visualizzata la pagina bucket che mostra tutti i bucket S3 esistenti.

2. Utilizzare il menu **azioni** o la pagina dei dettagli per un bucket specifico.

   Menu delle azioni

   a. Selezionare la casella di controllo per ciascun bucket da cui si desidera eliminare gli oggetti.
   b. Selezionare **azioni** > **Elimina oggetti nel bucket**.

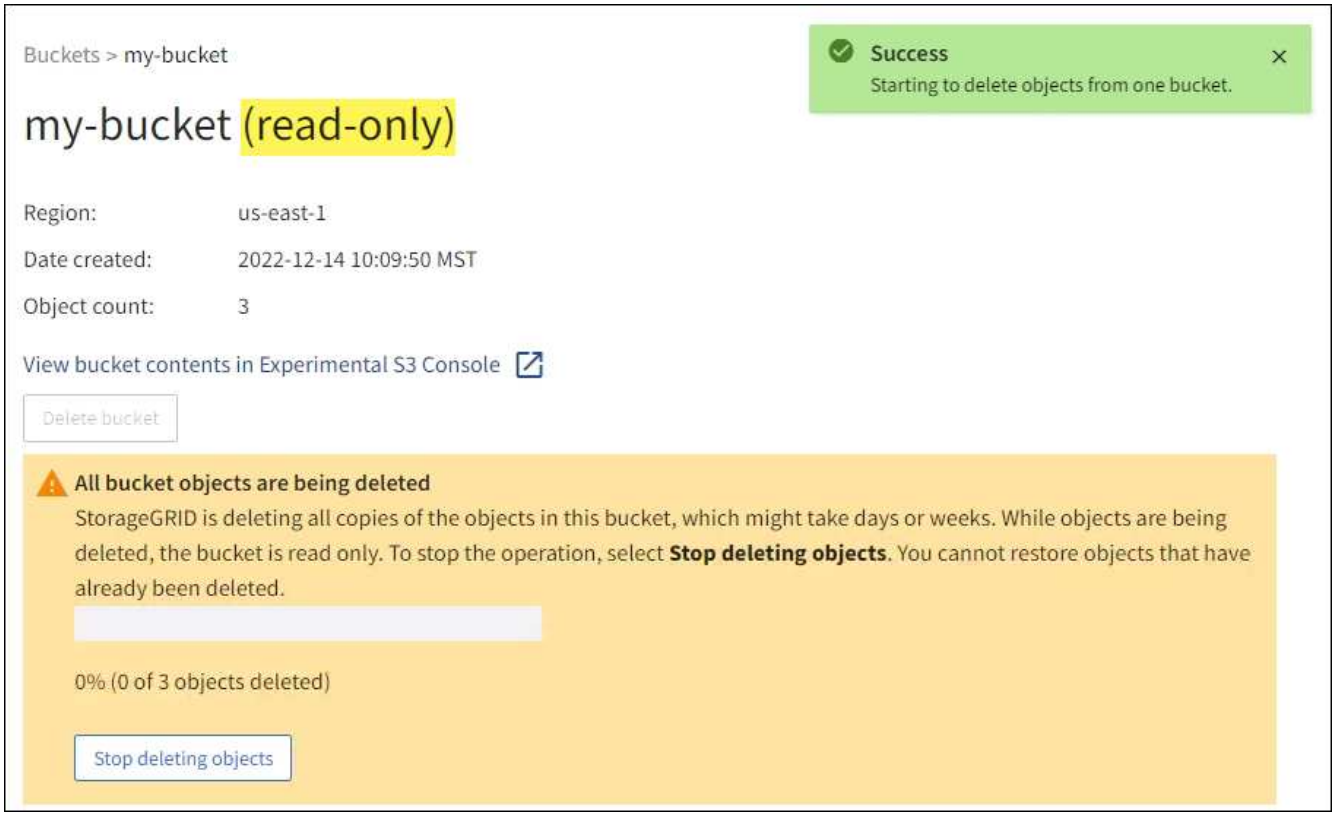
   Pagina dei dettagli

   a. Selezionare il nome di un bucket per visualizzarne i dettagli.
   b. Selezionare **Elimina oggetti nel bucket**.

3. Quando viene visualizzata la finestra di dialogo di conferma, rivedere i dettagli, inserire **Sì** e selezionare **OK**.
4. Attendere l'inizio dell'operazione di eliminazione.

   Dopo alcuni minuti:

   - Nella pagina dei dettagli del bucket viene visualizzato un banner di stato giallo. La barra di avanzamento indica la percentuale di oggetti eliminati.
   - * (sola lettura)* viene visualizzato dopo il nome del bucket nella pagina dei dettagli del bucket.
   - **(eliminazione di oggetti: Sola lettura)** viene visualizzato accanto al nome del bucket nella pagina bucket.

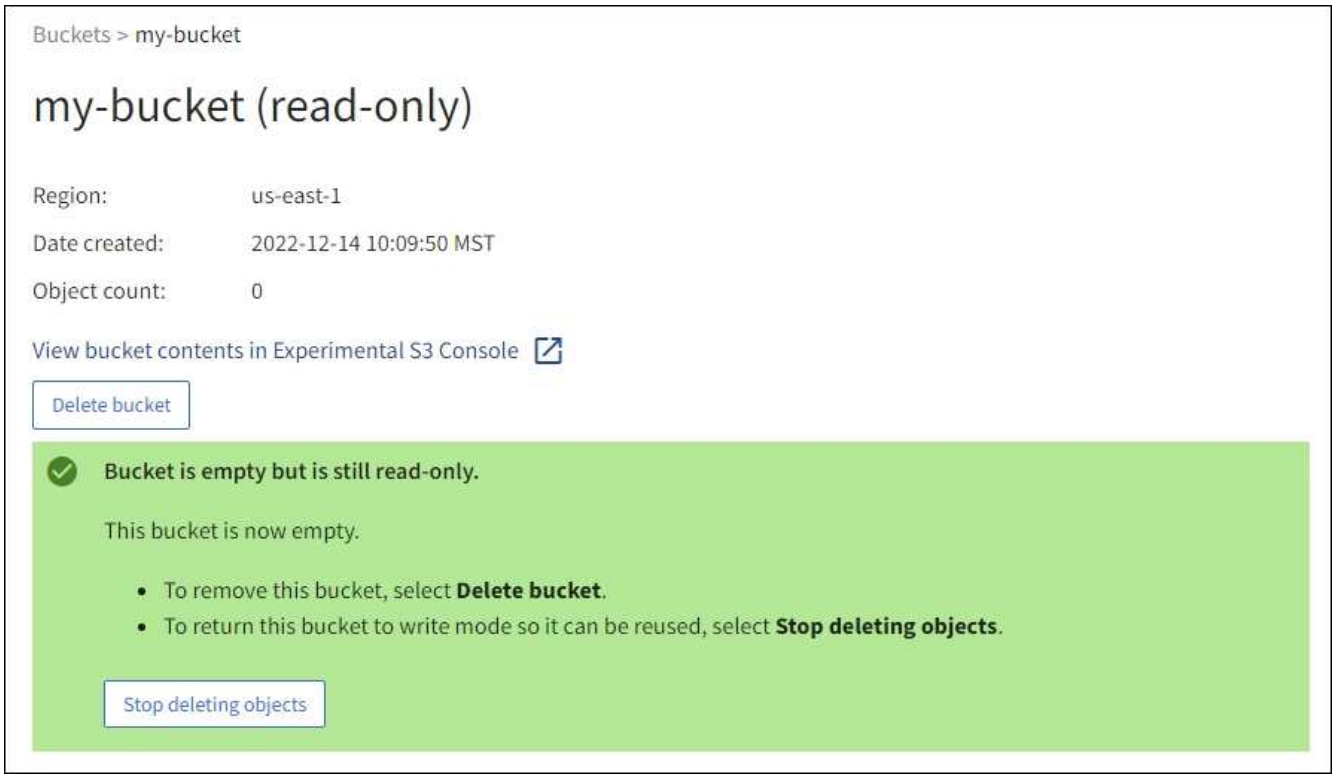


5. Quando l'operazione è in esecuzione, selezionare **Stop deleting objects** (Interrompi eliminazione oggetti) per interrompere il processo. Quindi, se si desidera, selezionare **Delete Objects in bucket** (Elimina oggetti nel bucket) per riprendere il processo.

   Quando si seleziona **Stop deleting objects**, il bucket torna alla modalità di scrittura; tuttavia, non è possibile accedere o ripristinare gli oggetti che sono stati cancellati.

6. Attendere il completamento dell'operazione.

   Quando il bucket è vuoto, il banner di stato viene aggiornato, ma il bucket rimane di sola lettura.



7. Effettuare una delle seguenti operazioni:
   - Uscire dalla pagina per mantenere il bucket in modalità di sola lettura. Ad esempio, è possibile mantenere un bucket vuoto in modalità di sola lettura per riservare il nome del bucket per un utilizzo futuro.
   - Eliminare il bucket. È possibile selezionare **Delete bucket** (Elimina bucket) per eliminare un singolo bucket o tornare alla pagina Bucket e selezionare **Actions** > **Delete** bucket (azioni* > **Delete** bucket) per rimuovere più bucket.

     Se non si riesce a eliminare un bucket con versione dopo l'eliminazione di tutti gli oggetti, i contrassegni di eliminazione potrebbero rimanere. Per eliminare il bucket, è necessario rimuovere tutti gli altri marker di eliminazione.

   - Riportare il bucket in modalità di scrittura e, se si desidera, riutilizzarlo per nuovi oggetti. È possibile selezionare **Interrompi eliminazione oggetti** per un singolo bucket o tornare alla pagina bucket e selezionare **azione** > **Interrompi eliminazione oggetti** per più bucket.

Elimina bucket S3

È possibile utilizzare Tenant Manager per eliminare uno o più bucket S3 vuoti.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- I bucket che si desidera eliminare sono vuoti. Se i bucket che si desidera eliminare sono *non* vuoti, "eliminare gli oggetti dal bucket".

A proposito di questa attività

Queste istruzioni descrivono come eliminare un bucket S3 utilizzando il Tenant Manager. È inoltre possibile eliminare i bucket S3 utilizzando "API di gestione del tenant"o "API REST S3".

Non è possibile eliminare un bucket S3 se contiene oggetti, versioni di oggetti non correnti o contrassegni di eliminazione. Per informazioni sull'eliminazione degli oggetti con versione S3, vedere "Modalità di eliminazione degli oggetti".

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.

   Viene visualizzata la pagina bucket che mostra tutti i bucket S3 esistenti.

2. Utilizzare il menu **azioni** o la pagina dei dettagli per un bucket specifico.

   Menu delle azioni

   a. Selezionare la casella di controllo per ciascun bucket che si desidera eliminare.

   b. Selezionare **azioni** > **Elimina bucket**.

   Pagina dei dettagli

   a. Selezionare il nome di un bucket per visualizzarne i dettagli.

   b. Selezionare **Delete bucket** (Elimina bucket).

3. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Sì**.

   StorageGRID conferma che ogni bucket è vuoto e quindi elimina ogni bucket. Questa operazione potrebbe richiedere alcuni minuti.

   Se un bucket non è vuoto, viene visualizzato un messaggio di errore. È necessario "eliminare tutti gli oggetti ed eventuali marcatori di eliminazione nel bucket" prima di poter eliminare il bucket.

Utilizzare la console S3

È possibile utilizzare S3 Console per visualizzare e gestire gli oggetti in un bucket S3.

La console S3 consente di:

- Caricamento, download, ridenominazione, copia, spostamento, ed eliminare gli oggetti
- Visualizzare, ripristinare, scaricare ed eliminare le versioni degli oggetti
- Cercare gli oggetti in base al prefisso
- Gestire tag di oggetti
- Visualizzare i metadati degli oggetti
- Visualizzare, creare, rinominare, copiare, spostare, ed eliminare le cartelle

La console S3 offre un'esperienza utente migliorata per i casi più comuni. Non è progettato per sostituire le operazioni CLI o API in tutte le situazioni.

Se l'utilizzo di S3 Console comporta un'operazione troppo lunga (ad esempio, minuti o ore), considerare quanto segue:

- Riduzione del numero di oggetti selezionati
- Utilizzando metodi non grafici (API o CLI) per accedere ai dati

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "browser web supportato".
- Se si desidera gestire gli oggetti, si appartiene a un gruppo di utenti che dispone dell'autorizzazione di accesso principale. In alternativa, si appartiene a un gruppo di utenti che dispone dell'autorizzazione Usa scheda Console S3 e dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket. Vedere "Permessi di gestione del tenant".
- Per l'utente è stato configurato un criterio di gruppo o bucket S3. Vedere "Utilizza policy di accesso a bucket e gruppi" .
- Conosci l'ID della chiave di accesso dell'utente e la chiave di accesso segreta. Facoltativamente, si dispone di un `.csv` file contenente queste informazioni. Consultare la "istruzioni per la creazione delle chiavi di accesso".

Fasi

1. Selezionare **Archiviazione** > **Bucket** > ***nome bucket***.
2. Selezionare la scheda Console S3.
3. Incollare l'ID della chiave di accesso e la chiave di accesso segreta nei campi. Altrimenti, selezionare **Upload access keys** e selezionare il `.csv` file.
4. Selezionare **Accedi**.
5. Viene visualizzata la tavola degli oggetti bucket. È possibile gestire gli oggetti in base alle esigenze.

Ulteriori informazioni

- **Cerca per prefisso**: La funzione di ricerca del prefisso ricerca solo gli oggetti che iniziano con una parola specifica relativa alla cartella corrente. La ricerca non include oggetti che contengono la parola altrove. Questa regola si applica anche agli oggetti all'interno delle cartelle. Ad esempio, una ricerca `folder1/folder2/somefile-` restituisce gli oggetti all'interno della `folder1/folder2/` cartella e inizia con la parola `somefile-`.
- **Trascinare e rilasciare**: È possibile trascinare i file dal file manager del computer a S3 Console. Tuttavia, non è possibile caricare le cartelle.
- **Operazioni sulle cartelle**: Quando si sposta, copia o rinomina una cartella, tutti gli oggetti nella cartella vengono aggiornati uno alla volta, il che potrebbe richiedere del tempo.
- **Eliminazione permanente quando la versione bucket è disattivata**: Quando si sovrascrive o si elimina un oggetto in un bucket con la versione disattivata, l'operazione è permanente. Vedere "Modificare la versione degli oggetti per un bucket".

Gestire i servizi della piattaforma S3

Servizi della piattaforma S3

Panoramica e considerazioni sui servizi di piattaforma

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

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

Panoramica dei servizi della piattaforma

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

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

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

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

Modalità di configurazione dei servizi della piattaforma

I servizi della piattaforma comunicano con endpoint esterni configurati tramite"Manager tenant" o il"API di gestione del tenant" . Ogni endpoint rappresenta una destinazione esterna, ad esempio un bucket StorageGRID S3, 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, è possibile attivare un servizio di piattaforma per un bucket aggiungendo la configurazione XML al bucket. La configurazione XML identifica gli oggetti su cui il bucket deve agire, l'azione che il bucket deve intraprendere e l'endpoint che il bucket deve utilizzare per il servizio.

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

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

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

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

Considerazioni sull'utilizzo dei servizi della piattaforma

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

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

Considerazioni sull'utilizzo del servizio di replica CloudMirror

Considerazione	Dettagli
Stato della replica	StorageGRID non supporta la `x-amz-replication-status` testata.
Dimensione dell'oggetto	La dimensione massima per gli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è 5 TIB, che corrisponde alla dimensione massima dell'oggetto *supportata*. **Nota**: La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.

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

Comprendere il servizio di replica CloudMirror

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

Ad esempio, è possibile utilizzare la replica di CloudMirror per eseguire il mirroring di record specifici dei clienti in Amazon S3 e sfruttare i servizi AWS per eseguire analisi dei dati.

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

CloudMirror e ILM

La replica CloudMirror funziona indipendentemente dalle policy ILM attive del grid. Il servizio CloudMirror replica gli oggetti memorizzati nel bucket di origine e li consegna al bucket di destinazione il prima possibile. La

consegna degli oggetti replicati viene attivata quando l'acquisizione degli oggetti ha esito positivo.

CloudMirror e replica cross-grid

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

Bucket Cloud Mirror e S3

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

Bucket esistenti

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

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

Bucket multipli di destinazione

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

Benne in versione o non in versione

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

Eliminazione, loop di replica ed eventi

Comportamento di eliminazione

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

Protezione dai loop di replica

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

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

Eventi nel bucket di destinazione

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

Comprendere le notifiche per i bucket

È possibile abilitare la notifica degli eventi per un bucket S3 se si desidera che StorageGRID invii notifiche su eventi specifici a un cluster Kafka di destinazione, a un endpoint webhook o ad Amazon Simple Notification Service.

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

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

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

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

- Sono supportati i seguenti tipi di evento:
  - S3:ObjectCreated:
  - s3:ObjectCreated:put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copy
  - s3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved:
  - s3:ObjectRemoved:Elimina
  - s3:ObjectRemoved:DeleteMarkerCreated
  - s3:ObjectRestore:Post
- Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ma non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nella tabella:

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

Comprendere il servizio di integrazione della ricerca

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

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

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

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

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

Integrazione di ricerca e bucket S3

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

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

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

Cerca notifiche

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

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

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

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

Servizio di integrazione della ricerca ed Elasticsearch

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

Gestire gli endpoint dei servizi della piattaforma

Configurare gli endpoint dei servizi della piattaforma

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

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

Che cos'è un endpoint di servizi di piattaforma?

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

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

Ogni tipo di servizio di piattaforma richiede un proprio endpoint, pertanto è necessario configurare almeno un endpoint per ogni servizio di piattaforma che si intende utilizzare. Dopo aver definito un endpoint di servizi di

piattaforma, si utilizza l'URN dell'endpoint come destinazione nel XML di configurazione utilizzato per attivare il servizio.

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

Endpoint per la replica di CloudMirror

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

Endpoint per le notifiche

StorageGRID supporta endpoint Amazon SNS, Kafka e webhook. Gli endpoint Simple Queue Service (SQS) e 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 di Elasticsearch possono trovarsi in un data center locale o in un cloud AWS o altrove.

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

Informazioni correlate

"Amministrare StorageGRID"

Specificare URN per l'endpoint dei servizi della piattaforma

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

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

Elementi DI URNA

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

- Se il servizio è ospitato su Amazon Web Services (AWS), utilizzare `arn:aws`

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

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

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

Servizio	Tipo
Replica di CloudMirror	`s3`
Notifiche	`sns`, `kafka` , O `webhook`
Integrazione della ricerca	`es`

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

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

Per gli endpoint webhook, la risorsa di destinazione è l'URI di destinazione stesso.

Servizio	Risorsa specifica
Replica di CloudMirror	`bucket-name`
Notifiche	`sns-topic-name` o. `kafka-topic-name` **Nota:** per gli endpoint webhook, l'elemento finale dell'URN può essere qualsiasi stringa, purché l'URN dell'endpoint sia univoco.
Integrazione della ricerca	`domain-name/index-name/type-name` **Nota:** se il cluster Elasticsearch è **non** configurato per creare gli indici automaticamente, è necessario creare l'indice manualmente prima di creare l'endpoint.

Urns per i servizi ospitati su AWS e GCP

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

- Replica di CloudMirror:

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

- Notifiche:

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

- Integrazione della ricerca:

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

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

Urns per servizi in hosting locale

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

- Replica di CloudMirror:

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

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

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

- Notifiche:

Specificare un endpoint di Amazon Simple Notification Service:

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

Specificare un endpoint Kafka:

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

Specificare 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 può essere qualsiasi stringa, `domain-name` purché l'URN dell'endpoint sia univoco.

Creare endpoint di servizi di piattaforma

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

Prima di iniziare

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

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

  - Nome risorsa univoco (URN)

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

  - Credenziali di autenticazione (se richieste):

Endpoint di integrazione della ricerca

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

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

Endpoint di replica CloudMirror

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

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

Endpoint Amazon SNS

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

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

Endpoint Kafka

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

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

  - Certificato di sicurezza (se è richiesta la verifica del certificato)

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

Fasi

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

   Il tipo di servizio 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 URI HTTPS e porta 80 per URI HTTP (la maggior parte degli endpoint)
- Porta 9092 per URI HTTPS e HTTP (solo endpoint Kafka)

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

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

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

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

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

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

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

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

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

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

> Se si desidera l'autenticazione per gli endpoint webhook, configurare Mutual Transport Layer Security (mTLS) inFase 9 .

Endpoint di integrazione della ricerca

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

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

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

Endpoint di replica CloudMirror

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

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

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

Endpoint Amazon SNS

Immettere o caricare le credenziali per un endpoint Amazon SNS.

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

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

Endpoint Kafka

Immettere o caricare le credenziali per un endpoint Kafka.

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

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

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

8. Selezionare **continua**.

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

La maggior parte degli endpoint

Verificare la connessione TLS per l'integrazione della ricerca, la replica di 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.
Disabili	La verifica del certificato è disabilitata. Questa opzione non è sicura.
USA certificato CA personalizzato	Il certificato CA personalizzato viene utilizzato per verificare l'identità del server durante la connessione all'endpoint.
Utilizzare il certificato CA del sistema operativo	Utilizzare il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.

Solo endpoint webhook

Verificare 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 TLS reciproche alla risorsa endpoint.
Disabili	La verifica del certificato è disabilitata. Questa opzione non è sicura.
USA certificato CA personalizzato	Il certificato CA personalizzato viene utilizzato per verificare l'identità del server durante la connessione all'endpoint.

Selezionando **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 del client	Il certificato client viene utilizzato per verificare l'identità del client durante la connessione all'endpoint.

Tipo di verifica del certificato	Descrizione
Chiave privata del cliente	La chiave privata per il certificato client. Se crittografato, deve utilizzare il formato tradizionale PKCS #1 (il formato PKCS #8 non è supportato).
Frase segreta della chiave privata del cliente	La passphrase per decifrare la chiave privata del client. Se la chiave privata non è crittografata, lasciare vuoto questo campo.

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

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

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

Informazioni correlate

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

Verifica della connessione per l'endpoint dei servizi della piattaforma

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

Prima di iniziare

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

A proposito di questa attività

StorageGRID non convalida che le credenziali dispongano delle autorizzazioni corrette.

Fasi

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

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

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

   Viene visualizzata la pagina dei dettagli dell'endpoint.

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

Modifica dell'endpoint dei servizi della piattaforma

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

Prima di iniziare

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

Fasi

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

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

2. Selezionare l'endpoint che si desidera modificare.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

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

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

   a. Per modificare il nome di visualizzazione per l'endpoint, selezionare l'icona di modifica .
   b. Se necessario, modificare l'URI.
   c. Se necessario, modificare il tipo di autenticazione.
      - Per l'autenticazione della chiave di accesso, modificare la chiave in base alle necessità selezionando **Modifica chiave S3** e incollando un nuovo ID della chiave di accesso e una chiave di accesso segreta. Se si desidera annullare le modifiche, selezionare **Ripristina modifica tasto S3**.
      - Per l'autenticazione CAP (C2S Access Portal), modificare l'URL delle credenziali temporanee o la passphrase della chiave privata del client opzionale e caricare nuovi file di certificato e chiavi in base alle necessità.

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

d. Se necessario, modificare il metodo di verifica dei certificati.

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

Eliminare l'endpoint dei servizi della piattaforma

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

Prima di iniziare

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

Fasi

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

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

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

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

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

   Viene visualizzato un messaggio di conferma.

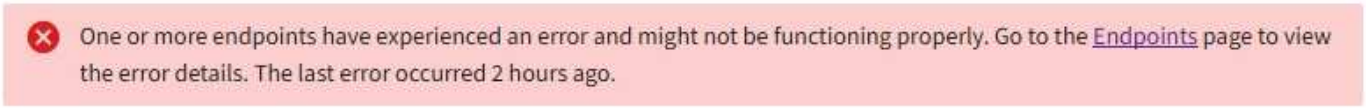
4. Selezionare **Delete endpoint** (Elimina endpoint).

Risolvere gli errori degli endpoint dei servizi della piattaforma

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi della piattaforma, viene visualizzato un messaggio sul dashboard. Nella pagina Platform Services Endpoint, la colonna Last error (ultimo errore) indica per quanto tempo si è verificato l'errore. Se le autorizzazioni associate alle credenziali di un endpoint non sono corrette, non viene visualizzato alcun errore.

Determinare se si è verificato un errore

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



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

Fasi

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

Controllare se l'errore è ancora aggiornato

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

Fasi

1. Selezionare l'endpoint.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

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

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

Risolvi gli errori degli endpoint

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

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

Fasi

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

4. Selezionare **connessione** > **verifica connessione**.

Credenziali endpoint con autorizzazioni insufficienti

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

Informazioni correlate

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

Configurare la replica di CloudMirror

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

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

- Quando si crea e si applica un XML di configurazione di replica bucket valido, è necessario utilizzare l'URN di un endpoint bucket S3 per ogni destinazione.
- La replica non è supportata per i bucket di origine o di destinazione con blocco oggetti S3 attivato.
- Se si attiva la replica CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket

vengono replicati, ma gli oggetti esistenti nel bucket non vengono replicati. È necessario aggiornare gli oggetti esistenti per attivare la replica.

- Se si specifica una classe di storage nell'XML di configurazione della replica, StorageGRID utilizza tale classe quando esegue operazioni sull'endpoint S3 di destinazione. L'endpoint di destinazione deve supportare anche la classe di storage specificata. Assicurarsi di seguire le raccomandazioni fornite dal vendor del sistema di destinazione.

Fasi

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

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

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

Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

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

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

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

Informazioni correlate

"Creare endpoint di servizi di piattaforma"

Configurare le notifiche degli eventi

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

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

Fasi

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

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

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

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

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

   b. Conferma che una notifica è stata recapitata all'argomento Amazon SNS di destinazione, all'argomento Kafka o all'endpoint webhook.

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

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

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

Informazioni correlate

- "Comprendere le notifiche per i bucket"
- "UTILIZZARE L'API REST S3"
- "Creare endpoint di servizi di piattaforma"

Configurare il servizio di integrazione della ricerca

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

Prima di iniziare

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

Elementi nella configurazione della notifica dei metadati XML:

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

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

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

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

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

Al termine

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

metodi:

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

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

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

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

Esempio: Configurazione della notifica di metadati con due regole

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

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

Formato di notifica dei metadati

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

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

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

Campi inclusi nel documento JSON

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

Informazioni su bucket e oggetti

`bucket`: Nome del bucket

`key`: Nome chiave oggetto

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

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

Metadati di sistema

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

`md5`: Hash oggetto

Metadati dell'utente

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

`key:value`

Tag

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

`key:value`

Come visualizzare i risultati in Elasticsearch

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

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