# Usa un tenant account

StorageGRID software

NetApp
July 23, 2026

# Sommario


Usa un tenant account . . . 1
Usa un account tenant di StorageGRID . . . 1
Che cos'è un tenant account? . . . 1
Come creare un tenant account . . . 1
${post_edited_translations.segment} . . . 2
${post_edited_translations.segment} . . . 2
Sign out di StorageGRID Tenant Manager . . . 3
Dashboard Tenant Manager in StorageGRID . . . 4
Informazioni sull'account del tenant . . . 5
Utilizzo dello storage e della quota . . . 5
Avvisi di utilizzo delle quote . . . 6
Utilizzo del limite di capacità . . . 7
Errori dell'endpoint . . . 7
API di gestione tenant . . . 7
Scopri l'API di gestione dei tenant di StorageGRID . . . 7
Versionamento dell'API di gestione dei tenant di StorageGRID . . . 10
Proteggi contro gli attacchi Cross-Site Request Forgery in StorageGRID . . . 11
${post_edited_translations.segment} . . . 12
Clona gruppi di tenant e utenti in StorageGRID . . . 12
Clona le chiavi di accesso S3 tra le grid StorageGRID utilizzando la Tenant Management API . . . 17
Gestisci la replica tra griglie in StorageGRID . . . 19
Visualizza le connessioni di federazione della griglia in StorageGRID . . . 24
Gestisci gruppi e utenti . . . 25
Usa la federazione delle identità in StorageGRID . . . 25
Gestisci i gruppi tenant . . . 30
Gestisci utenti tenant di StorageGRID . . . 38
${post_edited_translations.segment} . . . 43
Gestisci le chiavi di accesso S3 in StorageGRID . . . 43
Crea le tue chiavi di accesso S3 in StorageGRID . . . 43
Visualizza le tue chiavi di accesso S3 in StorageGRID . . . 44
Elimina le tue chiavi di accesso S3 in StorageGRID . . . 45
Crea le chiavi di accesso S3 di un altro utente in StorageGRID . . . 45
Visualizza le chiavi di accesso S3 di un altro utente in StorageGRID . . . 47
Elimina le chiavi di accesso S3 di un altro utente in StorageGRID . . . 47
${post_edited_translations.segment} . . . 48
Crea un bucket S3 di StorageGRID . . . 48
Visualizza i dettagli del bucket S3 in StorageGRID . . . 51
Scopri i bucket di ramo di StorageGRID . . . 53
Gestisci i bucket di filiale di StorageGRID . . . 55
Applica un tag di policy ILM a un bucket StorageGRID . . . 58
Gestisci la policy dei bucket di StorageGRID . . . 59
Gestire la coerenza dei bucket di StorageGRID . . . 60
Abilita o disabilita gli aggiornamenti dell'ora dell'ultimo accesso in StorageGRID . . . 62

Modifica la versione degli oggetti per un bucket S3 in StorageGRID . . . 64
Utilizza S3 Object Lock per conservare gli oggetti in StorageGRID . . . 65
Aggiorna la conservazione predefinita di S3 Object Lock in StorageGRID . . . 68
Configura CORS per i bucket S3 in StorageGRID . . . 70
Eliminare oggetti da un bucket S3 di StorageGRID . . . 72
Eliminare un bucket S3 di StorageGRID . . . 74
Usa la console S3 in StorageGRID . . . 75
Gestisci i servizi della piattaforma S3 . . . 76
servizi della piattaforma S3 . . . 77
Gestisci gli endpoint dei servizi della piattaforma . . . 84
Configura la replica CloudMirror in StorageGRID . . . 98
Configura le notifiche degli eventi in StorageGRID . . . 100
Configura il servizio di integrazione della ricerca in StorageGRID . . . 103

# Usa un tenant account

## Usa un account tenant di StorageGRID

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

### Che cos'è un tenant account?

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

Gli account tenant possono essere utilizzati per separare gli oggetti archiviati in base a entità diverse. Ad esempio, puoi utilizzare più account tenant per ciascuno di questi casi d'uso:

- **Caso d'uso aziendale:** Se il sistema StorageGRID viene utilizzato all'interno di un'azienda, lo storage a oggetti della grid potrebbe essere suddiviso in base ai diversi reparti dell'organizzazione. Ad esempio, potrebbero esserci account tenant per il reparto Marketing, il reparto Customer Support, il reparto Human Resources e così via.

  > Se usi il protocollo client S3, puoi anche usare i bucket S3 e le bucket policy per separare gli oggetti tra i reparti di un'azienda. Non devi creare account tenant separati. Consulta le istruzioni per implementare "Bucket S3 e policy dei bucket" per maggiori informazioni.

- **Caso d'uso del service provider:** Se il sistema StorageGRID viene utilizzato da un service provider, lo storage a oggetti della grid potrebbe essere segregato dalle diverse entità che noleggiano lo storage. Ad esempio, potrebbero esserci tenant account per Company A, Company B, Company C e così via.

### Come creare un tenant account

Gli account tenant vengono creati da un "Amministratore della griglia StorageGRID tramite Grid Manager". Quando crei un account tenant, l'amministratore della grid specifica quanto segue:

- Informazioni di base, inclusi il nome del tenant, il tipo di client (S3) e l'eventuale quota di storage.
- Autorizzazioni per il tenant account, ad esempio se il tenant account può utilizzare i servizi della piattaforma S3, configurare la propria origine di identità, utilizzare S3 Select o utilizzare una connessione di grid federation.
- L'access root iniziale per il tenant, in base al fatto che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione delle identità o single sign-on (SSO).

Inoltre, gli amministratori della griglia possono abilitare l'impostazione S3 Object Lock per il sistema StorageGRID se gli account tenant S3 devono essere conformi ai requisiti normativi. Quando S3 Object Lock è abilitato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

#### Configura i tenant S3

Dopo un "L'account tenant S3 è stato creato", puoi accedere a Tenant Manager per eseguire attività come le seguenti:

- Configura la federazione delle identità (a meno che l'origine dell'identità non sia condivisa con la grid)
- Gestisci gruppi e utenti

- Usa la federazione di griglia per clonare gli account e replicare tra griglie
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Usa S3 Select
- Monitora l'utilizzo dello storage

Anche se puoi creare e gestire bucket S3 con Tenant Manager, devi usare un "${post_edited_translations.segment}" o "Console S3" per acquisire e gestire gli oggetti.

# ${post_edited_translations.segment}

## ${post_edited_translations.segment}

Accedi al Tenant Manager inserendo l'URL del tenant nella barra degli indirizzi di un "browser web supportato".

**Prima di iniziare**

- Hai le tue credenziali di accesso.
- Disponi di un URL per accedere a Tenant Manager, fornito dall'amministratore della grid. L'URL sarà simile a uno di questi 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 fully qualified domain name (FQDN), l'indirizzo IP di un Admin Node o l'indirizzo IP virtuale di un gruppo HA di Admin Node. Potrebbe anche includere un numero di porta, l'ID dell'account tenant a 20 cifre o entrambi.

- ${post_edited_translations.segment}
- Stai usando un "browser web supportato".
- I cookie sono abilitati nel tuo browser web.
- Appartieni a un gruppo di utenti che ha "autorizzazioni di accesso specifiche".

**Passaggi**

1. Avvia un "browser web supportato".
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. Accedi al Tenant Manager.

   La schermata di accesso visualizzata dipende dall'URL inserito e dal fatto che single sign-on (SSO) sia

stato configurato o meno per StorageGRID.

**Non usi SSO**

${post_edited_translations.segment}

- La pagina di accesso di Grid Manager. Seleziona il link **Accesso tenant**.
- La pagina di accesso di Tenant Manager. Il campo **Account** potrebbe essere già compilato.
  i. ${post_edited_translations.segment}
  ii. ${post_edited_translations.segment}
  iii. Seleziona **Accedi**.

  Viene visualizzata la dashboard del Tenant Manager.

  iv. ${post_edited_translations.segment}

**Utilizzare SSO**

${post_edited_translations.segment}

- La pagina single sign-on della tua organizzazione.

  Inserisci le tue credenziali SSO standard e seleziona **Accedi**.

- La pagina di accesso SSO per il Tenant Manager.
  i. ${post_edited_translations.segment}
  ii. Seleziona **Accedi**.
  iii. Accedi con le tue credenziali SSO standard sulla pagina di accesso SSO della tua organizzazione.

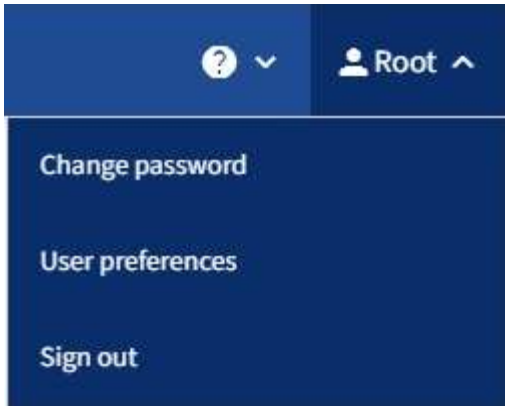
  Viene visualizzata la dashboard del Tenant Manager.

## Sign out di StorageGRID Tenant Manager

Quando hai finito di lavorare con il Tenant Manager, devi disconnetterti per assicurarti che gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnetterti dal sistema, a seconda delle impostazioni dei cookie del browser.

**Passaggi**

1. Individua il menu a tendina del nome utente nell'angolo in alto a destra dell'interfaccia utente.




2. Seleziona il nome utente e poi seleziona **Esci**.

   - ${post_edited_translations.segment}

     Hai effettuato la disconnessione dall'Admin Node. Viene visualizzata la pagina di accesso di Tenant Manager.

     > Se hai effettuato l'accesso a più di un nodo di amministrazione, devi disconnetterti da ciascun nodo.

   - Se SSO è abilitato:

     Hai effettuato il logout da tutti i nodi di amministrazione a cui stavi accedendo. Viene visualizzata la pagina di accesso di StorageGRID. Il nome dell'account tenant a cui hai appena avuto accesso è elencato come predefinito nel menu a tendina **Account recenti** e viene mostrato l'**Account ID** del tenant.

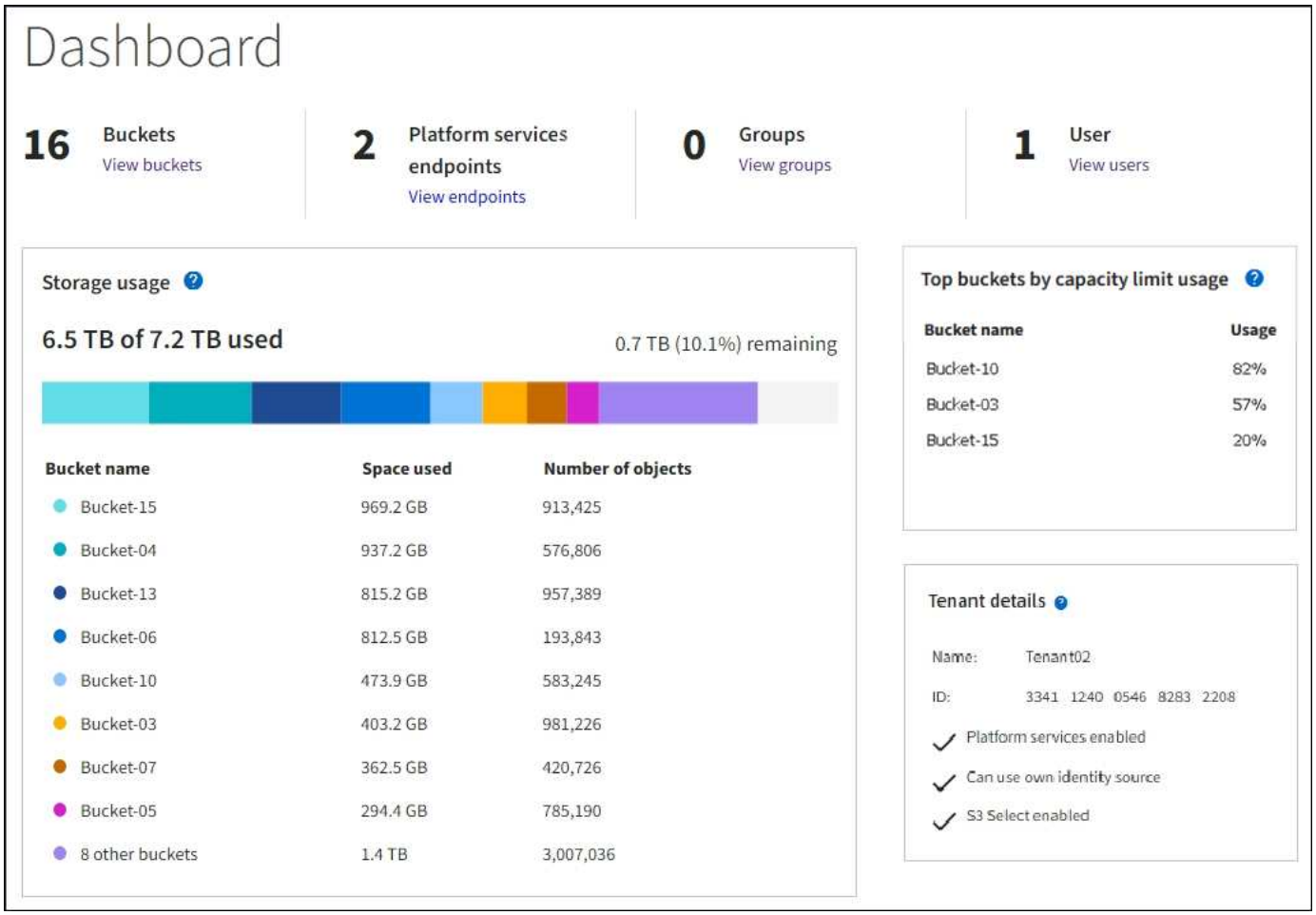
> ${post_edited_translations.segment}

# Dashboard Tenant Manager in StorageGRID

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

> La dimensione logica di tutti gli oggetti appartenenti a questo tenant include i caricamenti multipart incompleti e in corso. La dimensione non include lo spazio fisico aggiuntivo utilizzato per le policy ILM. I valori relativi allo spazio utilizzato sono stime. Queste stime sono influenzate dal momento dell'ingestione, dalla connettività di rete e dallo stato dei nodi.

Quando gli oggetti sono stati caricati, la dashboard appare come nel seguente esempio:




## Informazioni sull'account del tenant

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

A seconda delle "autorizzazioni di gestione tenant" che hai e delle opzioni che hai configurato, il resto del pannello di controllo mostra varie combinazioni di linee guida, utilizzo dello storage, informazioni sugli oggetti e dettagli sui tenant.

## Utilizzo dello storage e della quota

Il pannello Utilizzo dello storage contiene le seguenti informazioni:

- La quantità di dati oggetto per il tenant.

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

- Se è impostata una quota, vengono visualizzati lo spazio totale disponibile per i dati degli oggetti e la quantità e la % di spazio rimanente. La quota limita la quantità di dati degli oggetti che puoi inserire.

L'utilizzo della quota si basa su stime interne e potrebbe essere superato in alcuni casi. Ad esempio, StorageGRID verifica la quota quando un tenant inizia a caricare oggetti e rifiuta i nuovi caricamenti se il tenant ha superato la quota. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente per determinare se la quota è stata superata. Se vengono eliminati oggetti, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti fino al ricalcolo dell'utilizzo della quota. Il calcolo dell'utilizzo della quota può richiedere 10 minuti o più.

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

  Puoi posizionare il cursore su uno qualsiasi dei segmenti del grafico per vedere lo spazio totale occupato da quel bucket o container.


- In corrispondenza con il grafico a barre, un elenco dei bucket o container più grandi, comprensivo della quantità totale di dati degli oggetti e del 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 un'unica voce in fondo all'elenco.

Per modificare le unità di misura dei valori di archiviazione visualizzati nel Tenant Manager, seleziona il menu a tendina utente nell'angolo in alto a destra del Tenant Manager, poi seleziona **User preferences**.

## Avvisi di utilizzo delle quote

Se hai abilitato gli avvisi di utilizzo della quota nel Grid Manager, questi avvisi vengono visualizzati nel 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 **Tenant quota usage high**.

  Valuta di chiedere al tuo amministratore di grid di aumentare la quota.

- Se superi la quota, una notifica ti informa che non puoi caricare nuovi oggetti.

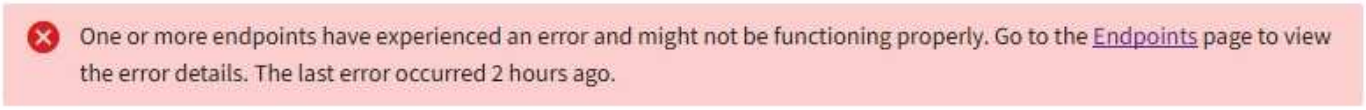
### Utilizzo del limite di capacità

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

Se non è impostato alcun limite per un bucket, la sua capacità è illimitata. Tuttavia, se il tuo tenant account ha una quota di archiviazione totale e tale quota è stata raggiunta, non potrai inserire altri oggetti, indipendentemente dal limite di capacità rimanente sul bucket.

## Errori dell'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 in uno qualsiasi degli endpoint negli ultimi sette giorni.




Per vedere i dettagli su "errori dell'endpoint dei servizi della piattaforma", seleziona **Endpoint** per visualizzare la pagina Endpoint.

# API di gestione tenant

## Scopri l'API di gestione dei tenant di StorageGRID

Puoi eseguire le attività di gestione del sistema utilizzando l'API REST di Tenant Management anziché l'interfaccia utente di Tenant Manager. Ad esempio, potresti voler utilizzare l'API per automatizzare le operazioni o per creare più entità, come gli utenti, in modo più rapido.

API di gestione tenant:

- Utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che permette sia a sviluppatori che a non sviluppatori di interagire con l'API. L'interfaccia utente di Swagger fornisce dettagli e documentazione completi per ogni operazione dell'API.
- Usa "gestione delle versioni per supportare aggiornamenti non disruptivi".

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

1. Accedi al Tenant Manager.
2. Dalla parte superiore di Tenant Manager, seleziona l'icona di aiuto e seleziona **API documentation**.

### operazioni API

L'API di gestione dei 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 eseguire l'autenticazione della sessione utente.

  L'API di gestione dei tenant supporta lo schema di autenticazione Bearer Token. Per accedere come tenant, devi fornire nome utente, password e accountId nel corpo JSON della richiesta di autenticazione (cioè `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 ("Authorization: Bearer token").

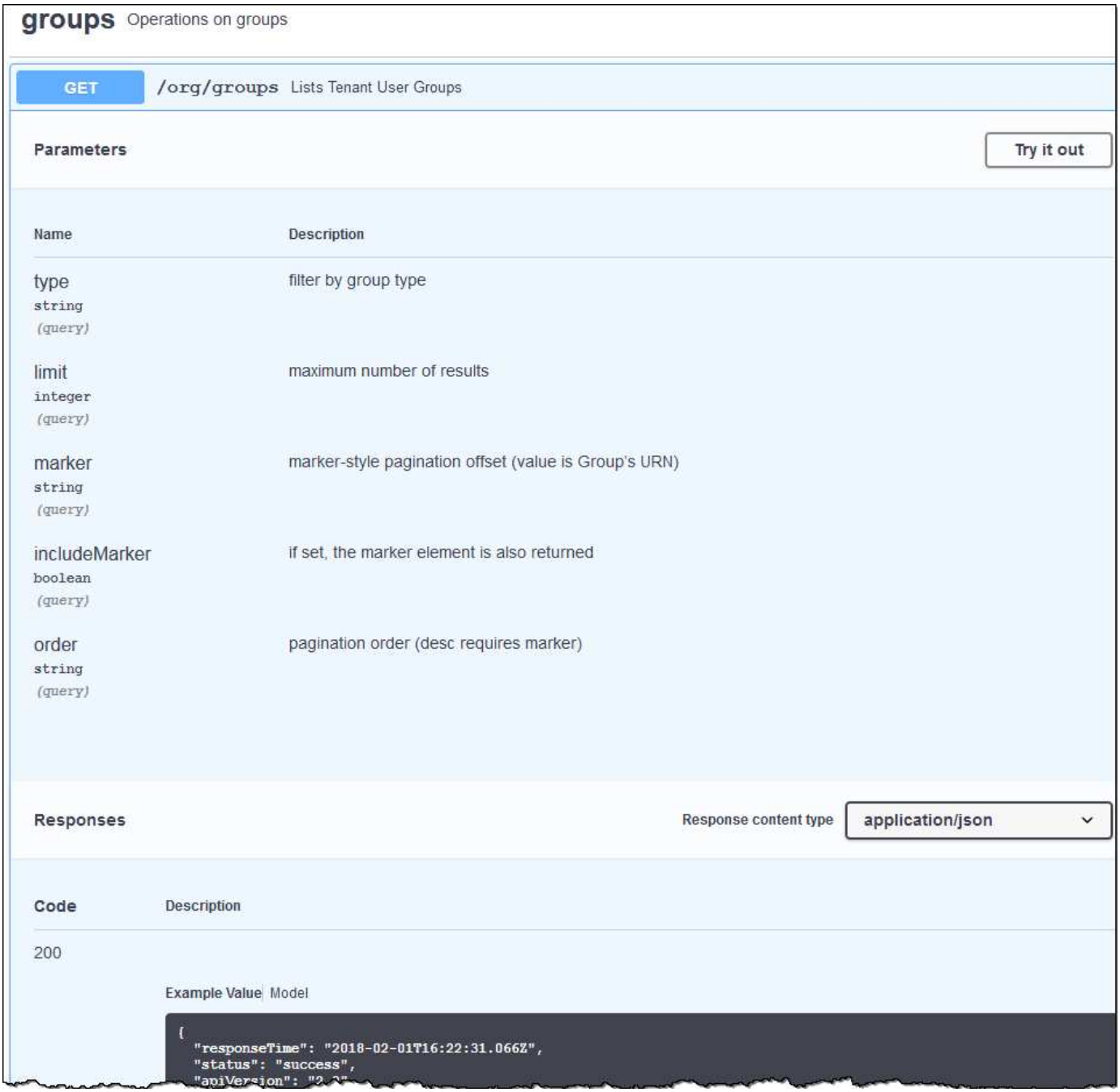
  Per informazioni su come migliorare la sicurezza con autenticazione, vedi "Proteggi dalle falsificazioni di richieste tra siti (Cross-Site Request Forgery)".

  > Se il single sign-on (SSO) è abilitato per il sistema StorageGRID, devi seguire passaggi diversi per autenticarti. Vedi la "Istruzioni per usare l'API di gestione della griglia".

- **config**: Operazioni relative alla release del prodotto e alle versioni dell'API di gestione del tenant. Puoi elencare la versione della release del prodotto e le versioni principali dell'API supportate da quella release.
- **container**: Operazioni sui bucket S3.
- **funzionalità-disattivate**: Operazioni per visualizzare le funzionalità 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 StorageGRID CloudMirror, le notifiche o l'integrazione della ricerca.
- **grid-federation-connections**: Operazioni sulle connessioni di federazione di griglia e sulla replica tra griglie.
- **gruppi**: Operazioni per gestire i gruppi di tenant locali e per recuperare i gruppi di tenant federati da una fonte di identità esterna.
- **identity-source**: Operazioni per configurare un'origine di identità esterna e per sincronizzare manualmente le informazioni di gruppi e utenti federati.
- **ilm**: Operazioni sulle impostazioni di gestione del ciclo di vita delle informazioni (ILM).
- **regioni**: Operazioni per determinare quali regioni sono state configurate per il sistema StorageGRID.
- **s3**: Operazioni per la gestione delle chiavi di accesso S3 per gli utenti del tenant.
- **s3-object-lock**: Operazioni sulle impostazioni globali di S3 Object Lock, utilizzate per supportare la conformità normativa.
- **Utenti**: Operazioni per visualizzare e gestire gli utenti del tenant.

### Dettagli operativi

Espandendo ciascuna operazione API, puoi vedere l'azione HTTP, l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se richiesto) e le possibili risposte.




### Invia richieste API

> Qualsiasi operazione API che esegui tramite la pagina web della documentazione API è un'operazione live. Fai attenzione a non creare, aggiornare o eliminare per errore dati di configurazione o altri dati.

### Passaggi

1. Seleziona l'azione HTTP per visualizzare i dettagli della richiesta.
2. Verifica se la richiesta richiede parametri aggiuntivi, come un ID di gruppo o un ID utente. Quindi, recupera questi valori. Potresti dover prima effettuare una richiesta API diversa per ottenere le informazioni di cui hai bisogno.
3. Determina se devi modificare il corpo della richiesta di esempio. In tal caso, puoi selezionare **Model** per conoscere i requisiti di ciascun campo.

4. ${post_edited_translations.segment}
5. Fornisci i parametri richiesti o modifica il corpo della richiesta come necessario.
6. Seleziona **Esegui**.
7. Esamina il codice di risposta per determinare se la richiesta è andata a buon fine.

## Versionamento dell'API di gestione dei tenant di StorageGRID

### ${post_edited_translations.segment}

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

L'esempio seguente illustra come la versione dell'API viene incrementata in base al tipo di modifiche apportate.

| **${post_edited_translations.segment}** | **Vecchia versione** | **${post_edited_translations.segment}** |
|---|---|---|
| ${post_edited_translations.segment} | 2,1 | 2,2 |
| Non compatibile con le versioni precedenti | 2,1 | 3,0 |

Quando installi il software StorageGRID per la prima volta, viene abilitata solo la versione più recente dell'API. Tuttavia, quando esegui l'upgrade a una nuova release di funzionalità di StorageGRID, continui ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.

> Puoi configurare le versioni supportate. Consulta la sezione **config** della documentazione dell'API Swagger per "API di gestione della griglia" ulteriori informazioni. Dovresti disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API alla versione più recente.

Le richieste obsolete sono contrassegnate come deprecate nei seguenti modi:

- L'intestazione della risposta è "Deprecated: true"
- Il corpo della risposta JSON include "deprecated": true
- Viene aggiunto un avviso di deprecazione a nms.log. Ad esempio:

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

#### Determina quali versioni API sono supportate nella release corrente

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

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

#### Specifica una versione API per una richiesta

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

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

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

## Proteggi contro gli attacchi Cross-Site Request Forgery in StorageGRID

Puoi aiutare a proteggerti dagli attacchi Cross-Site Request Forgery (CSRF) contro StorageGRID usando i token CSRF per rafforzare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; gli altri client API possono scegliere se abilitarla quando effettuano l'accesso.

Un utente malintenzionato in grado di attivare una richiesta a un sito diverso (ad esempio tramite un modulo HTTP POST) può far sì che determinate richieste vengano effettuate utilizzando i cookie dell'utente autenticato.

StorageGRID contribuisce a proteggere dagli attacchi CSRF tramite l'utilizzo di token CSRF. Quando questa funzionalità è abilitata, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro specifico del corpo di una richiesta POST.

Per abilitare la funzione, imposta il `csrfToken` parametro su `true` durante l'autenticazione. Il valore predefinito 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 è true, viene impostato un cookie `GridCsrfToken` con un valore casuale per gli accessi al Grid Manager e il cookie `AccountCsrfToken` viene impostato con un valore casuale per gli accessi al Tenant Manager.

${post_edited_translations.segment}

- 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 formato form-encoded: un parametro del corpo della richiesta codificato in formato `csrfToken`form-encoded.

Per configurare la protezione CSRF, usa "API di gestione della griglia" o "API di gestione tenant".

> Le richieste che includono un cookie CSRF token impongono anche l'intestazione "Content-Type: application/json" per qualsiasi richiesta che si aspetti un corpo della richiesta in formato JSON, come ulteriore protezione contro gli attacchi CSRF.

# ${post_edited_translations.segment}

## Clona gruppi di tenant e utenti in StorageGRID

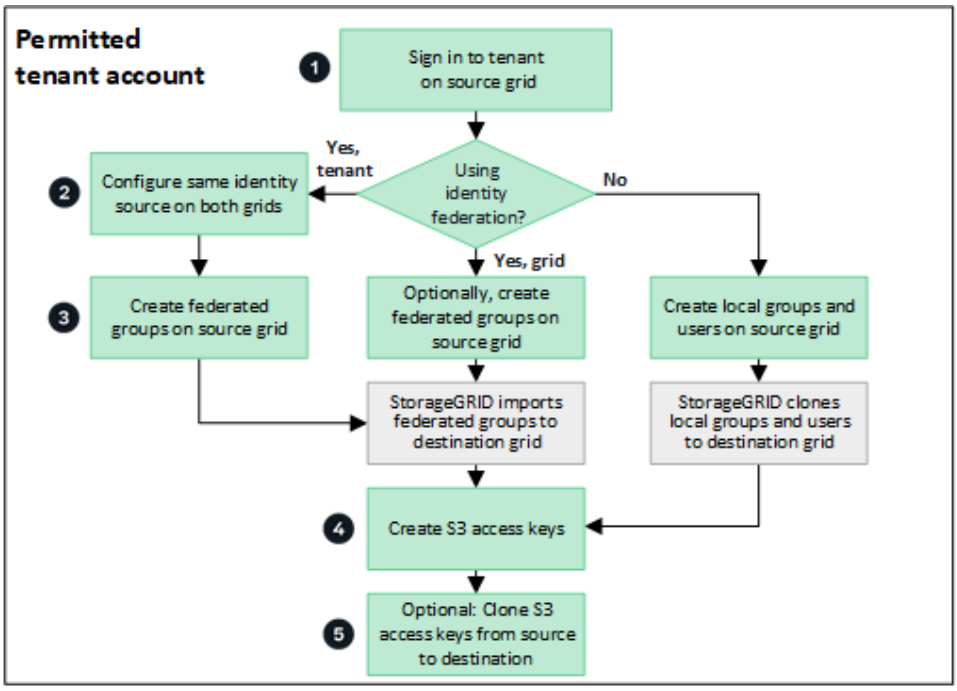
Se un tenant è stato creato o modificato per utilizzare una connessione di federazione grid, quel tenant viene replicato da un sistema StorageGRID (il tenant di origine) a un altro sistema StorageGRID (il tenant replica). Dopo che il tenant è stato replicato, tutti i gruppi e gli utenti aggiunti al tenant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

Il sistema StorageGRID in cui il tenant viene originariamente creato è la *griglia di origine* del tenant. Il sistema StorageGRID in cui il tenant viene replicato è la *griglia di destinazione* del tenant. Entrambi gli account tenant hanno lo stesso ID account, nome, descrizione, quota di archiviazione e autorizzazioni assegnate, ma il tenant di destinazione inizialmente non ha una password utente root. Per i dettagli, vedi "Cos'è un account clone" e "Gestisci i tenant autorizzati".

La clonazione delle informazioni dell'account tenant è necessaria per "replicazione cross-grid" degli oggetti bucket. Avere gli stessi gruppi tenant e utenti su entrambe le griglie garantisce che tu possa accedere ai bucket e agli oggetti corrispondenti su entrambe le griglie.

### Flusso di lavoro del tenant per la clonazione dell'account

Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione grid**, consulta il diagramma del flusso di lavoro per vedere quali passaggi eseguirai per clonare gruppi, utenti e chiavi di accesso S3.




Questi sono i passaggi principali del flusso di lavoro:

### 1 Accedi al tenant

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

### 2 Facoltativamente, configura la federazione delle identità

Se il tuo tenant account dispone dell'autorizzazione **Usa la tua origine di identità** per utilizzare gruppi e utenti federati, configura la stessa origine di identità (con le stesse impostazioni) sia per il tenant account di origine che per quello di destinazione. I gruppi e gli utenti federati non possono essere clonati a meno che entrambe le griglie utilizzino la stessa origine di identità. Per istruzioni, consulta "${post_edited_translations.segment}".

### 3 Crea gruppi e utenti

Quando crei gruppi e utenti, inizia sempre dalla grid di origine del tenant. Quando aggiungi un nuovo gruppo, StorageGRID lo clona automaticamente nella grid di destinazione.

- Se la federazione delle identità è configurata per l'intero sistema StorageGRID o per il tuo tenant, "crea nuovi gruppi tenant" importando i gruppi federati dall'origine delle identità.
- Se non stai utilizzando la federazione delle identità, "creare nuovi gruppi locali" e poi "crea utenti locali".

### 4 Crea le chiavi di accesso S3

Puoi "crea le tue chiavi di accesso" o "creare le chiavi di accesso di un altro utente" sulla griglia di origine o sulla griglia di destinazione per accedere ai bucket su quella griglia.

### 5 Facoltativamente, clona le chiavi di accesso S3

Se devi accedere ai bucket con le stesse chiavi di accesso su entrambe le griglie, crea le chiavi di accesso sulla griglia di origine e poi usa l'API di Tenant Manager per clonarle manualmente sulla griglia di destinazione. Per istruzioni, vedi "${post_edited_translations.segment}".

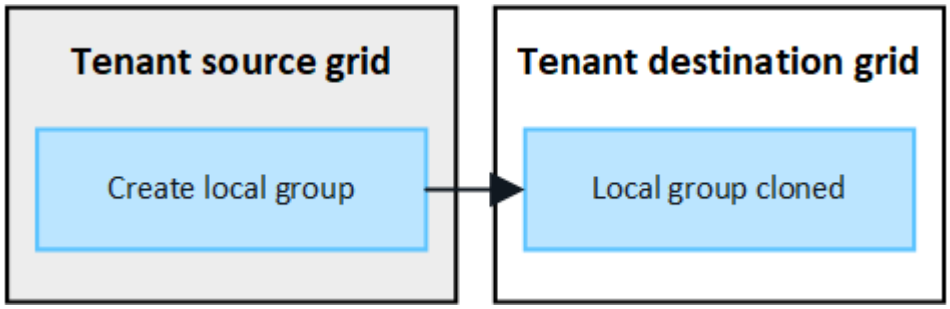
## Come vengono clonati gruppi, utenti e chiavi di accesso S3?

Consulta questa sezione per capire come vengono clonati gruppi, utenti e chiavi di accesso S3 tra la grid tenant di origine e la grid tenant di destinazione.

#### I gruppi locali creati sulla griglia di origine vengono clonati

Dopo che un account tenant è stato creato e replicato nella griglia di destinazione, StorageGRID clona automaticamente tutti i gruppi locali che aggiungi alla griglia di origine del tenant nella griglia di destinazione del tenant.

Sia il gruppo originale che il suo clone hanno la stessa modalità di accesso, le stesse autorizzazioni di gruppo e gli stessi criteri di gruppo S3. Per istruzioni, vedi "Crea gruppi per tenant S3".

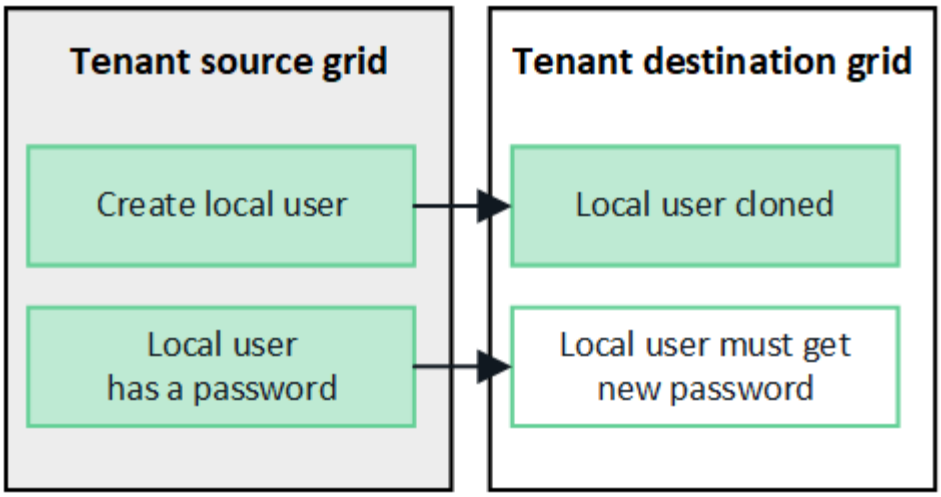



> Gli utenti che selezioni quando crei un gruppo locale sulla griglia di origine non vengono inclusi quando il gruppo viene clonato sulla griglia di destinazione. Per questo motivo, non selezionare utenti quando crei il gruppo. Invece, seleziona il gruppo quando crei gli utenti.

#### Gli utenti locali creati sulla griglia di origine vengono clonati

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

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

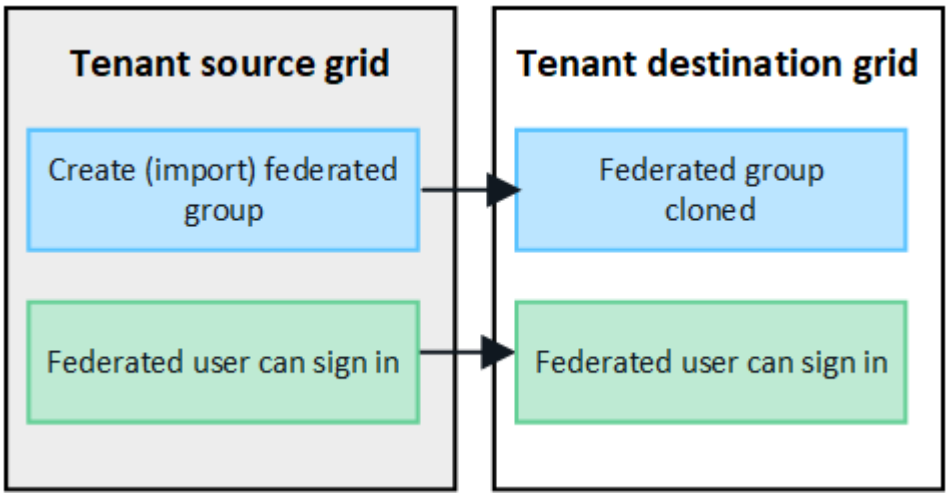



**I gruppi federati creati sulla griglia di origine vengono clonati**

Supponendo che siano stati soddisfatti i requisiti per l'utilizzo della clonazione dell'account con "single sign-on" e "federazione di identità", i gruppi federati che crei (importi) per il tenant sulla grid di origine vengono automaticamente clonati nel tenant sulla grid di destinazione.

Entrambi i gruppi hanno la stessa modalità di accesso, autorizzazioni di gruppo e criteri di gruppo S3.

Dopo che i gruppi federati sono stati creati per il tenant di origine e clonati nel tenant di destinazione, gli utenti federati possono accedere al tenant su entrambe le griglie.

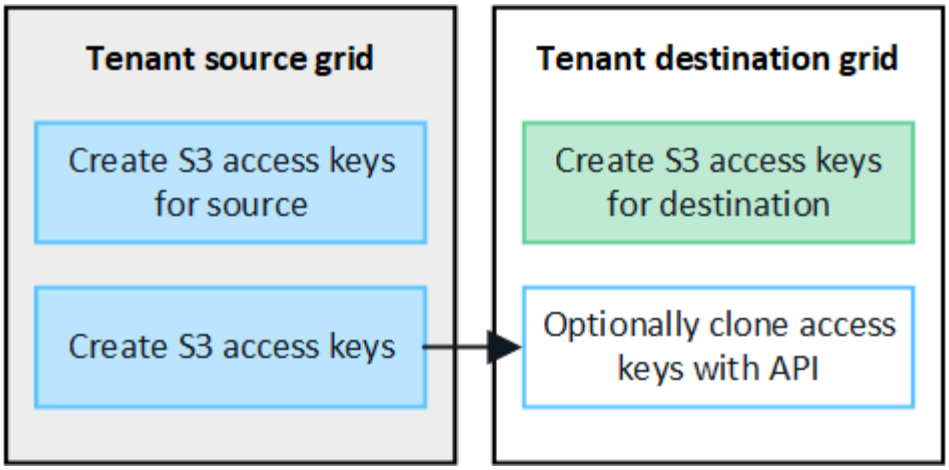



**Le chiavi di accesso S3 possono essere clonate manualmente**

StorageGRID non clona automaticamente le chiavi di accesso S3 perché la sicurezza è migliorata utilizzando chiavi diverse su ogni grid.

Per gestire le chiavi di accesso sulle due griglie, puoi fare una delle seguenti cose:

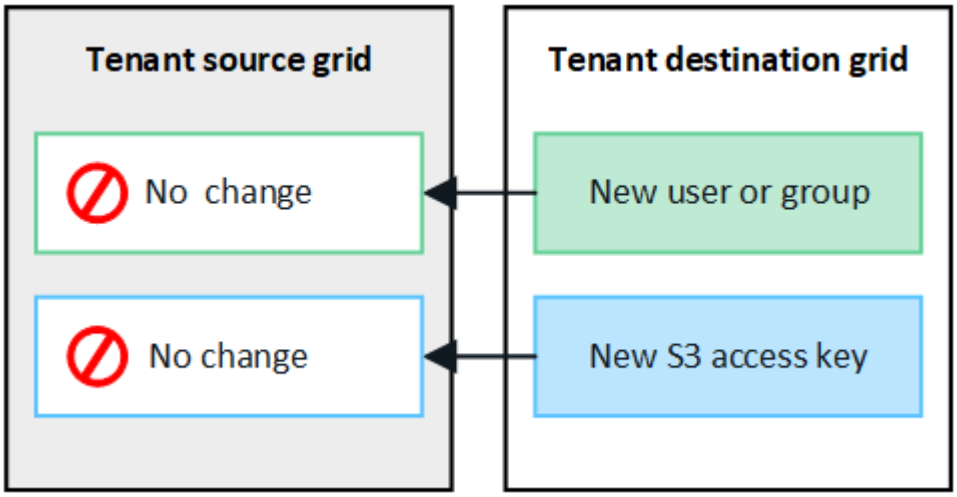
- Se non hai bisogno di usare le stesse chiavi per ogni grid, puoi "crea le tue chiavi di accesso" oppure "creare le chiavi di accesso di un altro utente" su ogni grid.
- Se devi utilizzare le stesse chiavi su entrambe le griglie, puoi creare le chiavi sulla griglia di origine e poi usare l'API di Tenant Manager per "clonare le chiavi" trasferirle manualmente alla destinazione.




Quando cloni le chiavi di accesso S3 per un utente federato, sia l'utente che le chiavi di accesso S3 vengono clonati nella destinazione tenant.

**I gruppi e gli utenti aggiunti alla destinazione grid non vengono clonati**

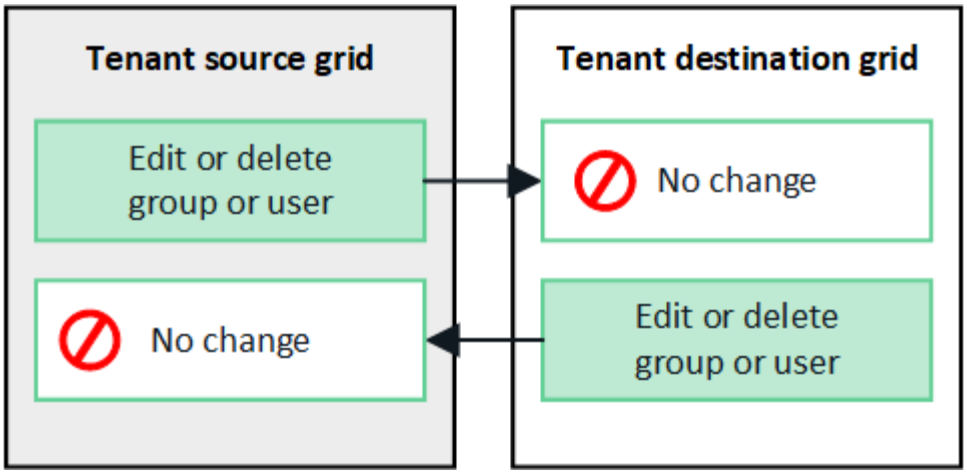
La clonazione avviene solo dalla grid di origine del tenant alla grid di destinazione del tenant. Se crei o importi gruppi e utenti sulla grid di destinazione del tenant, StorageGRID non clonerà questi elementi sulla grid di origine del tenant.




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

La clonazione avviene solo quando crei nuovi gruppi e utenti.

Se modifichi o elimini gruppi, utenti o chiavi di accesso su una delle due griglie, le modifiche non verranno clonate sull'altra griglia.




## Clona le chiavi di accesso S3 tra le grid StorageGRID utilizzando la Tenant Management API

Se il tuo StorageGRID tenant account dispone dell'autorizzazione **Use grid federation connection**, puoi utilizzare la Tenant Management API per clonare manualmente le chiavi di accesso S3 dal tenant sulla grid di origine al tenant sulla grid di destinazione.

### Prima di iniziare

- L'account tenant dispone dell'autorizzazione **Usa la connessione di federazione della griglia**.
- La connessione alla federazione di griglia ha uno stato di connessione **Connesso**.
- Hai effettuato l'accesso al Tenant Manager sulla griglia di origine del tenant utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha il "Gestisci le tue credenziali S3 o i permessi di accesso root".
- Se cloni le chiavi di accesso per un utente locale, l'utente esiste già su entrambe le griglie.

> Quando cloni le chiavi di accesso S3 per un utente federato, sia l'utente che le chiavi di accesso S3 vengono aggiunti alla destinazione tenant.

### Clona le tue chiavi di accesso

Puoi clonare le tue chiavi di accesso se hai bisogno di accedere agli stessi bucket su entrambe le griglie.

### Passaggi

1. Utilizzando il Tenant Manager sulla griglia di origine, "crea le tue chiavi di accesso" e scarica il file `.csv`.
2. Dalla parte superiore di Tenant Manager, seleziona l'icona di aiuto e seleziona **API documentation**.
3. Nella sezione **s3**, seleziona il seguente endpoint:

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

4. ${post_edited_translations.segment}

5. Nella casella di testo **body**, sostituisci le voci di esempio per **accessKey** e **secretAccessKey** con i valori del file **.csv** che hai scaricato.

   Assicurati di mantenere le virgolette doppie attorno a ciascuna stringa.


6. Se la chiave sta per scadere, sostituisci la voce di esempio per **expires** con la data e l'ora di scadenza come stringa nel formato data-ora ISO 8601 (per esempio, `2024-02-28T22:46:33-08:00`). Se la chiave non scadrà, inserisci **null** come valore per la voce **expires** (oppure rimuovi la riga **Expires** e la virgola che la precede).
7. Seleziona **Esegui**.
8. Conferma che il codice di risposta del server sia **204**, a indicare che la chiave è stata clonata correttamente nella destinazione grid.

### Clona le chiavi di accesso di un altro utente

Puoi clonare le chiavi di accesso di un altro utente se deve accedere agli stessi bucket su entrambe le griglie.

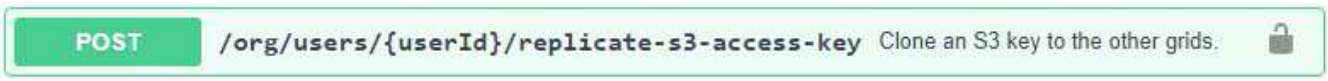
**Passaggi**

1. Utilizzando il Tenant Manager sulla griglia di origine, "crea le chiavi di accesso S3 dell'altro utente" e scarica il file `.csv`.
2. Dalla parte superiore di Tenant Manager, seleziona l'icona di aiuto e seleziona **API documentation**.
3. Ottieni l'ID utente. Ti servirà questo valore per clonare le chiavi di accesso dell'altro utente.
   a. Dalla sezione **utenti**, seleziona il seguente endpoint:

      `GET /org/users`

   b. ${post_edited_translations.segment}
   c. Specifica eventuali parametri che vuoi usare quando cerchi gli utenti.
   d. Seleziona **Esegui**.
   e. Trova l'utente di cui vuoi clonare le chiavi e copia il numero nel campo **id**.
4. Nella sezione **s3**, seleziona il seguente endpoint:

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




5. ${post_edited_translations.segment}
6. Nella casella di testo **userId**, incolla l'ID utente che hai copiato.

7. Nella casella di testo **body**, sostituisci le voci di esempio per **example access key** e **secret access key** con i valori presenti nel file **.csv** per quell'utente.

   ${post_edited_translations.segment}

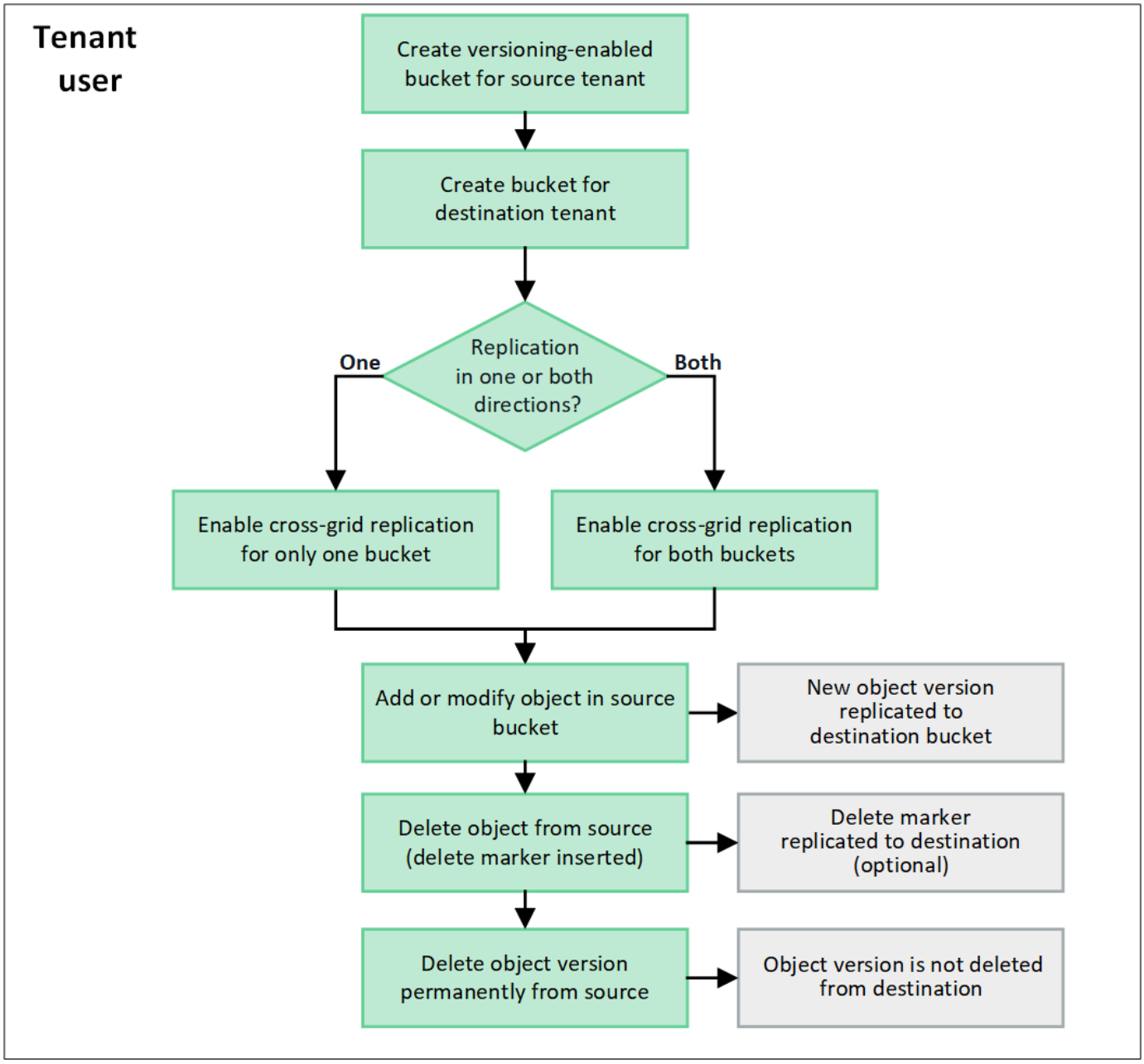
8. Se la chiave sta per scadere, sostituisci la voce di esempio per **expires** con la data e l'ora di scadenza come stringa nel formato data-ora ISO 8601 (per esempio, `2023-02-28T22:46:33-08:00`). Se la chiave non scadrà, inserisci **null** come valore per la voce **expires** (oppure rimuovi la riga **Expires** e la virgola che la precede).
9. Seleziona **Esegui**.
10. Conferma che il codice di risposta del server sia **204**, a indicare che la chiave è stata clonata correttamente nella destinazione grid.

## Gestisci la replica tra griglie in StorageGRID

Se al tuo account tenant è stata assegnata l'autorizzazione **Usa connessione di federazione della griglia** quando è stato creato, puoi utilizzare la replica tra griglie per replicare automaticamente gli oggetti tra i bucket sulla griglia di origine del tenant e i bucket sulla griglia di destinazione del tenant. La replica tra griglie può avvenire in una o in entrambe le direzioni.

### Flusso di lavoro per la replica cross-grid

Il diagramma del flusso di lavoro riassume i passaggi che esegui per configurare la replica cross-grid tra i bucket su due grid. Questi passaggi sono descritti in modo più dettagliato sotto il diagramma.




### Configura la replica cross-grid

Prima di poter utilizzare la replica cross-grid, devi accedere ai corrispondenti account tenant su ciascun grid e creare due bucket. Quindi, puoi abilitare la replica cross-grid su uno o su entrambi i bucket.

#### Prima di iniziare

- Hai verificato i requisiti per la replica cross-grid. Fai riferimento a "${post_edited_translations.segment}".
- Stai usando un "browser web supportato".
- L'account tenant dispone dell'autorizzazione **Utilizza connessione di federazione grid** e su entrambi i grid esistono account tenant identici. Fai riferimento a "Gestisci i tenant autorizzati per la connessione alla federazione di rete".
- L'utente tenant con cui stai effettuando l'accesso esiste già su entrambe le grid e appartiene a un gruppo di utenti che ha il "Permesso di accesso root".
- ${post_edited_translations.segment}

#### ${post_edited_translations.segment}

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

**Passaggi**

1. ${post_edited_translations.segment}
   a. Accedi all'account del tenant utilizzando le credenziali di un utente tenant che esiste su entrambe le griglie.

      ${post_edited_translations.segment}

   b. Segui le istruzioni per "${post_edited_translations.segment}".

      ${post_edited_translations.segment}

   c. Nella scheda **Gestisci impostazioni oggetto**, seleziona **Abilita versioning degli oggetti**.
   d. Se S3 Object Lock è abilitato per il tuo sistema StorageGRID, consulta "${post_edited_translations.segment}".
   e. Seleziona **Create bucket**.
   f. Seleziona **Fine**.
2. ${post_edited_translations.segment}

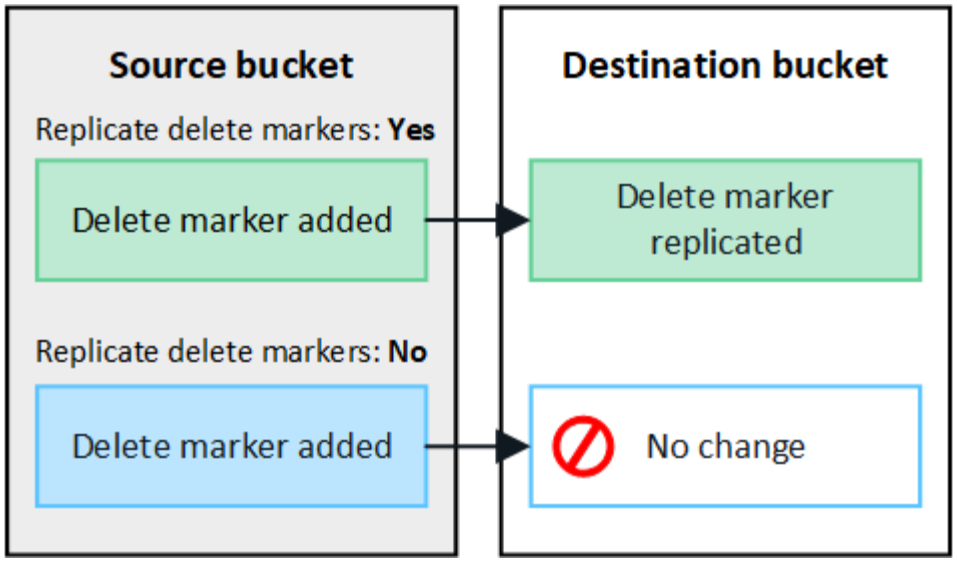
${post_edited_translations.segment}

#### ${post_edited_translations.segment}

Devi eseguire questi passaggi prima di aggiungere qualsiasi oggetto a uno dei due bucket.

**Passaggi**

1. Partendo da una griglia i cui oggetti vuoi replicare, abilita "${post_edited_translations.segment}":
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. Seleziona il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
   d. ${post_edited_translations.segment}
   e. Seleziona **Abilita** e rivedi l'elenco dei requisiti.
   f. Se tutti i requisiti sono stati soddisfatti, seleziona la connessione di federazione di griglia che desideri utilizzare.
   g. ${post_edited_translations.segment}
      - **Sì** (impostazione predefinita): viene aggiunto un indicatore di eliminazione al bucket di origine e replicato nel bucket di destinazione.
      - ${post_edited_translations.segment}




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

Consulta "${post_edited_translations.segment}" per i dettagli.

a. ${post_edited_translations.segment}
   - **Errore** (impostazione predefinita): solo le richieste di replica cross-grid non riuscite sono incluse nell'output di audit.
   - **Normale**: Sono incluse tutte le richieste di replica tra griglie, il che aumenta significativamente il volume dell'output di audit.

b. Rivedi le tue selezioni. Non puoi modificare queste impostazioni a meno che entrambi i bucket non siano vuoti.

c. Seleziona **Abilita e testa**.

   Dopo pochi istanti, viene visualizzato un messaggio di successo. Gli oggetti aggiunti a questo bucket vengono ora replicati automaticamente sull'altro grid. La **replica cross-grid** viene mostrata come funzionalità abilitata nella pagina dei dettagli del bucket.

2. Facoltativamente, vai al bucket corrispondente sull'altra grid e "abilita la replica tra griglie in entrambe le direzioni".

### ${post_edited_translations.segment}

${post_edited_translations.segment}

**Prima di iniziare**

- Stai usando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Permesso di accesso root".

**Passaggi**

1. ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
3. Seleziona il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
4. ${post_edited_translations.segment}
5. Seleziona **Test connessione**.

   Se la connessione è stabile, viene visualizzato un banner di successo. Altrimenti, viene visualizzato un messaggio di errore che tu e l'amministratore della grid potete usare per risolvere il problema. Per dettagli, consulta "Risolvi i problemi relativi agli errori di federazione della griglia".

6. ${post_edited_translations.segment}

### Disabilita la replica tra griglie

Puoi interrompere definitivamente la replica tra griglie se non vuoi più copiare oggetti nell'altra griglia.

${post_edited_translations.segment}

- Disabilitare la replica tra griglie non rimuove gli oggetti già copiati tra le griglie. Ad esempio, gli oggetti in `my-bucket` su Grid 1 che sono stati copiati in `my-bucket` su Grid 2 non vengono rimossi se disabiliti la replica tra griglie per quel bucket. Se vuoi eliminare questi oggetti, devi rimuoverli manualmente.
- Se la replica tra griglie è stata abilitata per ciascuno dei bucket (ovvero, se la replica avviene in entrambe le direzioni), puoi disabilitare la replica tra griglie per uno o entrambi i bucket. Ad esempio, potresti voler disabilitare la replica degli oggetti da `my-bucket` su Grid 1 a `my-bucket` su Grid 2, continuando invece a replicare gli oggetti da `my-bucket` su Grid 2 a `my-bucket` su Grid 1.
- Devi disabilitare la replica tra griglie prima di poter rimuovere l'autorizzazione di un tenant a utilizzare la connessione di federazione della griglia. Consulta "Gestisci i tenant autorizzati".
- Se disabiliti la replica tra griglie per un bucket che contiene oggetti, non potrai riattivare la replica tra griglie a meno che tu non elimini tutti gli oggetti sia dal bucket di origine che da quello di destinazione.

  Non puoi riattivare la replica a meno che entrambi i bucket siano vuoti.

#### Prima di iniziare

- Stai usando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Permesso di accesso root".

#### Passaggi

1. Partendo dalla griglia i cui oggetti non vuoi più replicare, interrompi la replica tra griglie per il bucket:
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. Seleziona il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
   d. ${post_edited_translations.segment}
   e. ${post_edited_translations.segment}
   f. ${post_edited_translations.segment}

      Dopo qualche istante, viene visualizzato un messaggio di conferma. I nuovi oggetti aggiunti a questo bucket non possono più essere replicati automaticamente nell'altra grid. **Cross-grid replication** non viene più visualizzata come funzionalità abilitata nella pagina Buckets.

2. ${post_edited_translations.segment}

## Visualizza le connessioni di federazione della griglia in StorageGRID

Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione grid**, puoi visualizzare le connessioni consentite.

**Prima di iniziare**

- L'account tenant dispone dell'autorizzazione **Usa la connessione di federazione della griglia**.
- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Permesso di accesso root".

**Passaggi**

1. Seleziona **STORAGE (S3)** > **Grid federation connections**.

   ${post_edited_translations.segment}

| Colonna | Descrizione |
| --- | --- |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} |
| ${post_edited_translations.segment} | Per ogni connessione di federazione di griglia, i bucket tenant per cui è abilitata la replica tra griglie. Gli oggetti aggiunti a questi bucket verranno replicati nell'altra griglia della connessione. |
| Ultimo errore | Per ogni connessione di federazione di griglia, l'errore più recente verificatosi, se presente, durante la replica dei dati nell'altra griglia. Vedi ${post_edited_translations.segment}. |

2. Facoltativamente, seleziona un nome bucket da "visualizza i dettagli del bucket".

### Cancella l'ultimo errore

Nella colonna **Ultimo errore** potrebbe comparire un errore per uno di questi motivi:

- La versione dell'oggetto sorgente non è stata trovata.
- ${post_edited_translations.segment}
- Il bucket di destinazione è stato eliminato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- ${post_edited_translations.segment}
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più versionato.

> Questa colonna mostra solo l'ultimo errore di replica tra griglie che si è verificato; gli errori precedenti che potrebbero essersi verificati non verranno visualizzati.

**Passaggi**

1. ${post_edited_translations.segment}

${post_edited_translations.segment}


2. Esegui le azioni consigliate. Ad esempio, se il versioning è stato sospeso sul bucket di destinazione per la replica tra griglie, riattiva il versioning per quel bucket.
3. ${post_edited_translations.segment}
4. Seleziona **Cancella errore**.
5. ${post_edited_translations.segment}
6. Attendi 5-6 minuti e poi inserisci un nuovo oggetto nel bucket. Verifica che il messaggio di errore non si ripresenti.

> Per assicurarti che il messaggio di errore venga eliminato, aspetta almeno 5 minuti dopo l'orario indicato nel messaggio prima di inserire un nuovo oggetto.

7. Per determinare se alcuni oggetti non sono stati replicati a causa di un errore del bucket, vedi "Identifica e riprova le operazioni di replica non riuscite".

# Gestisci gruppi e utenti

## Usa la federazione delle identità in StorageGRID

L'utilizzo della federazione delle identità rende più veloce la configurazione di gruppi e utenti tenant e permette agli utenti tenant di accedere all'account tenant usando le loro credenziali abituali.

### Configura la federazione delle identità per Tenant Manager

Puoi configurare la federazione delle identità per il Tenant Manager se vuoi che i gruppi di tenant e gli utenti siano gestiti in un altro sistema, come Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server.

#### Prima di iniziare

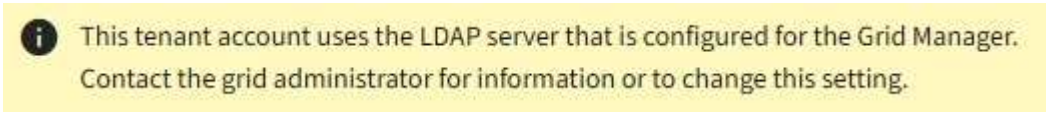
- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Permesso di accesso root".
- Stai utilizzando Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server come provider di identità.

Se vuoi usare un servizio LDAP v3 che non è presente nell'elenco, contatta il supporto tecnico.

- Se vuoi usare OpenLDAP, devi configurare il server OpenLDAP. Vedi Linee guida per la configurazione del server OpenLDAP.
- Se vuoi utilizzare Transport Layer Security (TLS) per le comunicazioni con il LDAP server, il provider di identità deve usare TLS 1.2 o 1.3. Vedi "Algoritmi di crittografia supportati per le connessioni TLS in uscita".

**Informazioni su questa attività**

La possibilità di configurare un servizio di federazione delle identità per il tuo tenant dipende da come è stato configurato il tuo account tenant. Il tuo tenant potrebbe condividere il servizio di federazione delle identità configurato per Grid Manager. Se visualizzi questo messaggio quando accedi alla pagina Identity Federation, non puoi configurare un'origine di identità federata separata per questo tenant.

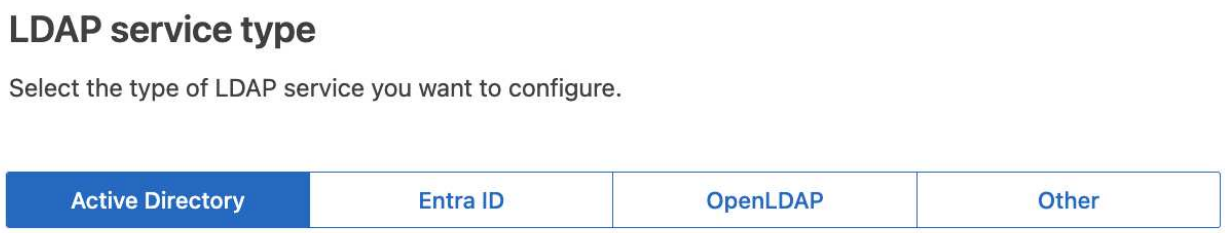



**Inserisci la configurazione**

Quando configuri la federazione delle identità, fornisci i valori di cui StorageGRID ha bisogno per connettersi a un servizio LDAP.

**Passaggi**

1. Seleziona **Gestione accessi** > **Federazione delle identità**.
2. Seleziona **Abilita federazione delle identità**.
3. Nella sezione relativa al tipo di servizio LDAP, seleziona il tipo di servizio LDAP che vuoi configurare.




   Seleziona **Altro** per configurare i valori per un LDAP server che usa Oracle Directory Server.

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. Altrimenti, passa al passaggio successivo.
   - **Nome univoco utente**: Il nome dell'attributo che contiene l'identificativo 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'identificativo 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 a 16 byte o stringa,

dove i trattini vengono ignorati.

- **Nome univoco del gruppo**: il nome dell'attributo che contiene l'identificativo 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 del gruppo**: Il nome dell'attributo che contiene l'identificativo 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 a 16 byte o stringa, dove i trattini vengono ignorati.

5. Per tutti i tipi di servizio LDAP, inserisci le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.
   - **Hostname**: Il fully qualified domain name (FQDN) o l'indirizzo IP del LDAP server.
   - **Porta**: La porta utilizzata per connettersi al LDAP server.

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

   - **Nome utente**: Il full path del distinguished name (DN) dell'utente che si connetterà al LDAP server.

     Per Active Directory, puoi anche specificare il Down-Level Logon Name o lo User Principal Name.

     L'utente specificato deve avere l'autorizzazione per visualizzare l'elenco di 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`
     - **Entra ID**: `accountEnabled` e `userPrincipalName`

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

     Se in futuro cambierai la password, dovrai aggiornarla su questa pagina.

   - **DN di base del gruppo**: il full path del nome distinto (DN) per un sottoalbero LDAP in cui vuoi cercare i gruppi. Nell'esempio di Active Directory (sotto), tutti i gruppi il cui nome distinto è relativo al DN di base (DC=storagegrid,DC=example,DC=com) possono essere usati come gruppi federati.

     ${post_edited_translations.segment}

   - **DN della base utente**: Il full path del nome distinto (DN) di un sottoalbero LDAP in cui vuoi cercare gli utenti.

     I valori del **nome univoco utente** devono essere univoci all'interno del **User Base DN** a cui appartengono.

◦ ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

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

Inserisci **[USERNAME]** esattamente come è scritto.

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

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

7. Se hai selezionato STARTTLS o LDAPS, scegli il certificato utilizzato per proteggere la connessione.
   - **Utilizza il certificato CA del sistema operativo**: Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
   - **Utilizza un certificato CA personalizzato**: Utilizza un certificato di sicurezza personalizzato.

     Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo del certificato CA.

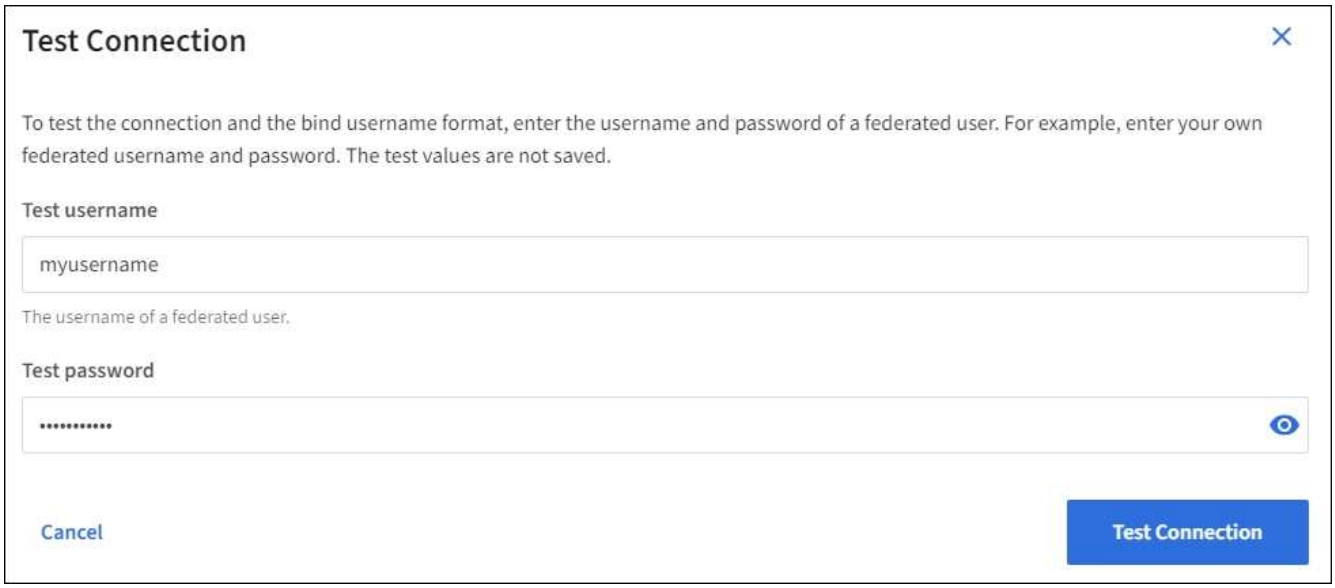
#### Verifica la connessione e salva la configurazione

Dopo aver inserito tutti i valori, devi testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il LDAP server e il formato del nome utente di bind, se ne hai fornito uno.

**Passaggi**

1. Seleziona **Test connessione**.
2. Se non hai fornito un formato per il nome utente bind:
   - Viene visualizzato il messaggio "Test di connessione riuscito" se le impostazioni di connessione sono valide. Seleziona **Salva** per salvare la configurazione.
   - Viene visualizzato il messaggio "Impossibile stabilire la connessione di prova" se le impostazioni di connessione non sono valide. Seleziona **Chiudi**. Quindi, risolvi eventuali problemi e prova nuovamente la connessione.
3. Se hai specificato un formato di nome utente di bind, inserisci il nome utente e la password di un utente federato valido.

Ad esempio, inserisci il tuo nome utente e la tua password. Non includere caratteri speciali nel nome utente, come @ o /.




- Viene visualizzato il messaggio "Test di connessione riuscito" se le impostazioni di connessione sono valide. Seleziona **Salva** per salvare la configurazione.
- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente di bind o il nome utente e la password di test non sono validi. Risolvi eventuali problemi e prova nuovamente la connessione.

### Forza la sincronizzazione con l'origine di identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dalla sorgente di identità. Puoi forzare l'avvio della sincronizzazione se vuoi abilitare o limitare le autorizzazioni degli utenti il più rapidamente possibile.

#### Passaggi

1. Vai alla pagina di federazione delle identità.
2. ${post_edited_translations.segment}

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

   ${post_edited_translations.segment}

### Disabilita la federazione delle identità

Puoi disabilitare 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 delle identità. Tuttavia, tutte le impostazioni che hai configurato vengono mantenute, permettendoti di riattivare facilmente la federazione delle identità in futuro.

#### Informazioni su questa attività

Prima di disabilitare la federazione delle identità, dovresti tenere presente quanto segue:

- Gli utenti federati non potranno accedere.

- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della loro sessione, ma non potranno accedere dopo la scadenza della sessione.
- ${post_edited_translations.segment}
- La casella di controllo **Abilita federazione delle identità** è disabilitata se lo stato del single sign-on (SSO) è **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedi "${post_edited_translations.segment}".

**Passaggi**

1. Vai alla pagina di federazione delle identità.
2. Deseleziona la casella di controllo **Abilita federazione delle identità**.

### Linee guida per la configurazione del server OpenLDAP

Se vuoi usare un server OpenLDAP per la federazione delle identità, devi configurare impostazioni specifiche sul server OpenLDAP.

> Per le origini di identità diverse da Active Directory o Microsoft Entra ID, StorageGRID non bloccherà automaticamente l'accesso S3 per gli utenti disabilitati esternamente. Per bloccare l'accesso S3, elimina tutte le chiavi S3 dell'utente o rimuovi l'utente da tutti i gruppi.

#### Sovrapposizioni Memberof e Refint

Le sovrapposizioni memberof e refint devono essere abilitate. Per ulteriori informazioni, consulta le istruzioni per la manutenzione della membership inversa del gruppo nel "Documentazione di OpenLDAP: Guida dell'amministratore versione 2.4".

#### Indicizzazione

${post_edited_translations.segment}

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

Inoltre, assicurati che i campi menzionati nell'aiuto per Nome utente siano indicizzati per prestazioni ottimali.

Vedi le informazioni sulla manutenzione dell'appartenenza inversa ai gruppi nel "Documentazione di OpenLDAP: Guida dell'amministratore versione 2.4".

## Gestisci i gruppi tenant

### Creare gruppi per un tenant S3 in StorageGRID

${post_edited_translations.segment}

**Prima di iniziare**

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

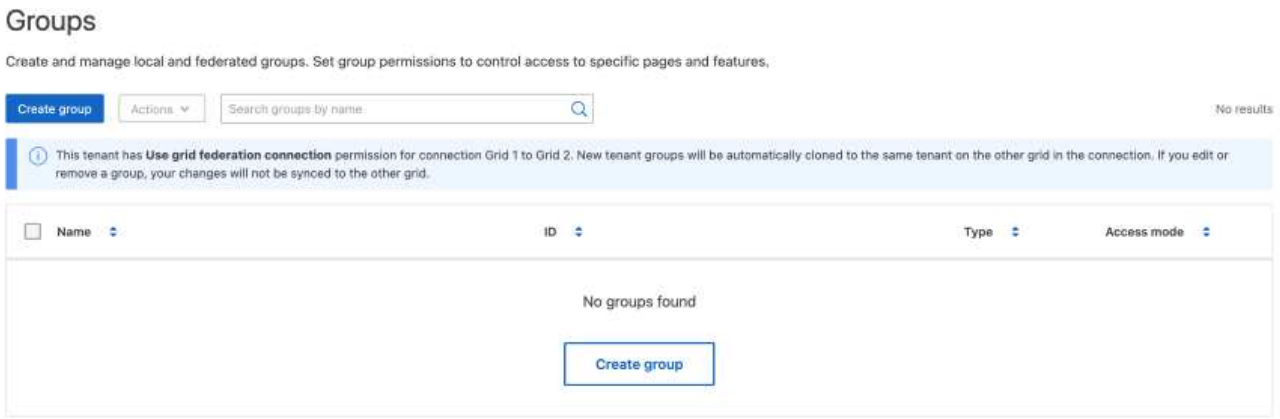
- Se pianifichi di importare un gruppo federato, hai "${post_edited_translations.segment}" e il gruppo federato esiste già nell'origine dell'identità configurata.
- Se il tuo account tenant dispone dell'autorizzazione **Use grid federation connection**, hai esaminato il workflow e le considerazioni per "${post_edited_translations.segment}" e hai effettuato l'accesso alla grid di origine del tenant.

#### Accedi alla procedura guidata Crea gruppo

Come primo passo, accedi alla procedura guidata Crea gruppo.

**Passaggi**

1. ${post_edited_translations.segment}
2. Se il tuo account tenant dispone dell'autorizzazione **Use grid federation connection**, conferma che venga visualizzato un banner blu, a indicare che i nuovi gruppi creati su questa griglia verranno clonati sullo stesso tenant sull'altra griglia della connessione. Se questo banner non viene visualizzato, potresti aver effettuato l'accesso alla griglia di destinazione del tenant.




3. Seleziona **Crea gruppo**.

#### Scegli un tipo di gruppo

Puoi creare un gruppo locale o importare un gruppo federato.

**Passaggi**

1. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
   - **Gruppo locale**: Inserisci sia un nome visualizzato che un nome univoco. Puoi modificare il nome visualizzato in seguito.

     ${post_edited_translations.segment}

   - **Gruppo federato**: Inserisci il nome univoco. Per Active Directory, il nome univoco è il nome associato all'attributo `sAMAccountName`. Per OpenLDAP, il nome univoco è il nome associato all'attributo `uid`.
3. Seleziona **Continue**.

#### Gestisci le autorizzazioni di gruppo

${post_edited_translations.segment}

**Passaggi**

1. Per la **modalità di accesso**, seleziona una delle seguenti opzioni:
   - ${post_edited_translations.segment}
   - **Sola lettura**: gli utenti possono solo visualizzare le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nel Tenant Manager o nella Tenant Management API. Gli utenti locali in sola lettura possono modificare le proprie password.

     Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su Sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Seleziona una o più autorizzazioni per questo gruppo.

   Vedi "Autorizzazioni per la gestione dei tenant".

3. Seleziona **Continue**.

#### Imposta i criteri di gruppo S3

Il criterio di gruppo determina quali autorizzazioni di accesso S3 avranno gli utenti.

**Passaggi**

1. Seleziona il criterio che vuoi usare per questo gruppo.

| Criteri di gruppo | Descrizione |
|---|---|
| Nessun accesso S3 | Predefinito. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non venga concesso tramite una bucket policy. Se scegli 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 selezioni questa opzione, la stringa JSON per un criterio di gruppo di sola lettura appare nella casella di testo. Non puoi modificare questa stringa. |
| Accesso completo | Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando selezioni questa opzione, la stringa JSON per un criterio di gruppo con accesso completo appare nella casella di testo. Non puoi modificare questa stringa. |

| Criteri di gruppo | Descrizione |
| --- | --- |
| Mitigazione del ransomware | Questa policy di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare definitivamente oggetti dai bucket che hanno il versioning degli oggetti abilitato.<br><br>Gli utenti di Tenant Manager che dispongono dell'autorizzazione **Gestisci tutti i bucket** possono ignorare questo criterio di gruppo. Limita l'autorizzazione **Gestisci tutti i bucket** agli utenti attendibili e usa l'autenticazione a più fattori (MFA) dove disponibile. |
| Personalizzato | Agli utenti del gruppo vengono concesse le autorizzazioni che specifichi nella casella di testo. |

2. Se hai selezionato **Personalizzato**, inserisci i criteri di gruppo. Ogni criterio di gruppo ha un limite di dimensione di 5.120 byte. Devi inserire una stringa in formato JSON valido.

   Per informazioni dettagliate sulle policy di gruppo, inclusa la sintassi del linguaggio e gli esempi, vedi "Esempi di criteri di gruppo".

3. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona **Crea gruppo** e **Fine**.

#### Aggiungi utenti (solo gruppi locali)

Puoi salvare il gruppo senza aggiungere utenti oppure, se vuoi, aggiungere eventuali utenti locali già esistenti.

> Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia**, gli utenti che selezioni quando crei un gruppo locale sulla griglia di origine non vengono inclusi quando il gruppo viene clonato sul cluster di destinazione. Per questo motivo, non selezionare utenti quando crei il gruppo. Invece, seleziona il gruppo quando crei gli utenti.

**Passaggi**

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.
2. Seleziona **Crea gruppo** e **Fine**.

   Il gruppo che hai creato appare nell'elenco dei gruppi.

   Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e ti trovi sulla grid di origine del tenant, il nuovo gruppo viene clonato nella grid di destinazione del tenant. **Success** appare come **Stato di clonazione** nella sezione Panoramica della pagina dei dettagli del gruppo.

### Autorizzazioni di gestione del tenant StorageGRID

Prima di creare un gruppo di tenant, considera quali autorizzazioni desideri assegnare a tale gruppo. Le autorizzazioni di gestione del tenant determinano quali attività 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 al Tenant Manager o per utilizzare l'API Tenant Management, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono accedere possono eseguire le seguenti attività:

- Visualizza la dashboard
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su Sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Puoi assegnare le seguenti autorizzazioni a un gruppo.

| Permesso | Descrizione | Dettagli |
|---|---|---|
| Accesso root | Fornisce accesso completo al Tenant Manager e al Tenant Management API. | |
| Gestisci le tue credenziali S3 | ${post_edited_translations.segment} | Gli utenti che non dispongono di questa autorizzazione non vedono l'opzione di menu **STORAGE (S3)** > **My S3 access keys**. |
| Visualizza tutti i bucket | Consente agli utenti di visualizzare tutti i bucket e le configurazioni dei bucket. | Gli utenti che non dispongono dell'autorizzazione "Visualizza tutti i bucket" o "Gestisci tutti i bucket" non vedono l'opzione di menu **Bucket**.<br><br>Questa autorizzazione è sostituita dall'autorizzazione Manage all buckets. Non influisce sulle policy di gruppo o dei bucket S3 utilizzate dai client S3 o dalla Console S3. |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | Gli utenti che non dispongono dell'autorizzazione "Visualizza tutti i bucket" o "Gestisci tutti i bucket" non vedono l'opzione di menu **Bucket**.<br><br>Questa autorizzazione sostituisce l'autorizzazione Visualizza tutti i bucket. Non influisce sulle policy dei bucket o dei gruppi S3 utilizzate dai client S3 o dalla S3 Console. |
| Gestisci gli endpoint | Consente agli utenti di utilizzare il Tenant Manager o l'API di gestione dei tenant per creare o modificare gli endpoint dei servizi della piattaforma, che vengono utilizzati come destinazione per i servizi della piattaforma StorageGRID. | Gli utenti che non dispongono di questa autorizzazione non vedono l'opzione di menu **Endpoint dei servizi della piattaforma**. |

| Permesso | Descrizione | Dettagli |
| --- | --- | --- |
| Usa la scheda Console S3 | ${post_edited_translations.segment} | |

### Gestisci i gruppi tenant di StorageGRID

Gestisci i tuoi gruppi di tenant secondo necessità per visualizzare, modificare o duplicare un gruppo e altro ancora.

#### Prima di iniziare

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

#### Visualizza o modifica gruppo

Puoi visualizzare e modificare le informazioni e i dettagli di base per ogni gruppo.

#### Passaggi

1. ${post_edited_translations.segment}
2. Esamina le informazioni fornite nella pagina Gruppi, che elenca i dati di base di tutti i gruppi locali e federati per questo tenant account.

   ${post_edited_translations.segment}

   - Un messaggio a comparsa indica che se modifichi o rimuovi un gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio banner indica se i gruppi non sono stati clonati nel tenant sulla griglia di destinazione. Puoi riprovare un clone di gruppo che non sono riusciti.
3. Se vuoi cambiare il nome del gruppo:
   a. ${post_edited_translations.segment}
   b. Seleziona **Azioni** > **Modifica nome gruppo**.
   c. ${post_edited_translations.segment}
   d. Seleziona **Salva modifiche.**
4. Se desideri visualizzare maggiori dettagli o apportare ulteriori modifiche, procedi in uno dei seguenti modi:
   - Seleziona il nome del gruppo.
   - Seleziona la casella di controllo relativa al gruppo e seleziona **Azioni** > **Visualizza dettagli del gruppo**.
5. ${post_edited_translations.segment}
   - Nome da visualizzare
   - Nome unico
   - Tipo
   - Modalità di accesso
   - Autorizzazioni

- Policy S3
- Numero di utenti in questo gruppo
- ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}

6. Modifica le impostazioni del gruppo secondo necessità. Consulta "Crea gruppi per un tenant S3" per i dettagli su cosa inserire.
   a. Nella sezione Panoramica, modifica il nome visualizzato selezionando il nome o l'icona di modifica .
   b. Nella scheda **Autorizzazioni di gruppo**, aggiorna le autorizzazioni e seleziona **Salva modifiche**.
   c. ${post_edited_translations.segment}

      Facoltativamente, seleziona un criterio di gruppo S3 diverso oppure inserisci la stringa JSON per un criterio personalizzato, se necessario.

7. ${post_edited_translations.segment}
   a. Seleziona la scheda Utenti.


   b. Seleziona **Aggiungi utenti**.
   c. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

8. ${post_edited_translations.segment}
   a. Seleziona la scheda Utenti.
   b. Seleziona **Rimuovi utenti**.
   c. Seleziona gli utenti che desideri rimuovere e seleziona **Rimuovi utenti**.

      ${post_edited_translations.segment}

9. Conferma di aver selezionato **Salva modifiche** per ogni sezione che hai modificato.

**${post_edited_translations.segment}**

Puoi duplicare un gruppo esistente per creare nuovi gruppi più rapidamente.

${post_edited_translations.segment}

**Passaggi**

1. ${post_edited_translations.segment}
2. Seleziona la casella di controllo per il gruppo che vuoi duplicare.
3. Seleziona **Azioni** > **Duplica gruppo**.
4. Vedi "Crea gruppi per un tenant S3" per i dettagli su cosa inserire.
5. Seleziona **Crea gruppo**.

#### Riprova il clone del gruppo

Per riprovare una clonazione non riuscita:

1. ${post_edited_translations.segment}
2. Seleziona **Azioni** > **Clona gruppi**.
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ogni gruppo che stai clonando.

Per ulteriori informazioni, consulta "${post_edited_translations.segment}".

#### Elimina uno o più gruppi

Puoi eliminare uno o più gruppi. Gli utenti che appartengono solo a un gruppo eliminato non potranno più accedere a Tenant Manager o utilizzare l'account tenant.

> Se il tuo tenant account ha l'autorizzazione **Use grid federation connection** e elimini un gruppo, StorageGRID non eliminerà il gruppo corrispondente sull'altra grid. Se vuoi mantenere queste informazioni sincronizzate, devi eliminare lo stesso gruppo da entrambe le grid.

**Passaggi**

1. ${post_edited_translations.segment}
2. Seleziona la casella di controllo per ogni gruppo che vuoi eliminare.
3. ${post_edited_translations.segment}

   Viene visualizzata una finestra di dialogo di conferma.

4. Seleziona **Elimina gruppo** o **Elimina gruppi**.

#### Configura AssumeRole

**Prima di iniziare**

Devi essere un amministratore per configurare AssumeRole.

**Informazioni su questa attività**

Per configurare AssumeRole, crea il gruppo di destinazione da assumere, se il gruppo non esiste già. Modifica la policy S3 del gruppo per specificare le azioni consentite per assumere questo gruppo. Modifica la policy di attendibilità S3 del gruppo per specificare gli utenti attendibili autorizzati ad assumere il gruppo con l'API AssumeRole.

Le credenziali di sicurezza temporanee create assumendo questo gruppo sono valide per una durata limitata. La sessione dura da 15 minuti a 12 ore e la sessione predefinita è di 1 ora. Quando rimuovi l'utente dalla policy di attendibilità S3 del gruppo, l'utente non può più assumere questo gruppo.

**Passaggi**

1. ${post_edited_translations.segment}
2. Fai clic sul nome del gruppo.
3. Seleziona la scheda **S3 trust policy**.
4. Aggiungi la tua policy di attendibilità S3, incluso un elenco di utenti che possono eseguire AssumeRole.
5. Seleziona **Salva modifiche**.
6. Seleziona la scheda **Criteri di gruppo S3**.
7. Modifica la policy S3 per specificare solo le azioni S3 necessarie per gli utenti attendibili aggiunti alla S3 trust policy di questo gruppo.
8. Seleziona **Salva modifiche**.

**Esempio di policy di trust S3 AssumeRole**

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

Al termine della configurazione, gli utenti elencati nella policy di attendibilità di S3 possono eseguire AssumeRole e ricevere le credenziali. Le autorizzazioni finali sono determinate dalla policy di gruppo, dalla policy del bucket e dalla policy di sessione. Per ulteriori informazioni, consulta "Usa le policy di accesso".

## Gestisci utenti tenant di StorageGRID

Puoi creare utenti locali e assegnarli a gruppi locali per determinare a quali funzionalità questi utenti possono accedere. Puoi anche importare utenti federati. Il Tenant Manager include un utente locale predefinito, chiamato "root". Anche se puoi aggiungere e rimuovere utenti locali, non puoi rimuovere l'utente root.

${post_edited_translations.segment}

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Tu appartieni a un gruppo di utenti che ha il "Permesso di accesso root".
- Se il tuo account tenant dispone dell'autorizzazione **Use grid federation connection**, hai esaminato il

workflow e le considerazioni per "${post_edited_translations.segment}" e hai effettuato l'accesso alla grid di origine del tenant.

## Crea un utente locale

Puoi creare un utente locale e assegnarlo a uno o più gruppi locali per controllare le sue autorizzazioni di accesso.

Gli utenti S3 che non appartengono ad alcun gruppo non dispongono di autorizzazioni di gestione né di criteri di gruppo S3 applicati a loro. Questi utenti potrebbero avere accesso ai bucket S3 concesso tramite un criterio di bucket.

#### Accedi alla procedura guidata di creazione utente

### Passaggi

1. Seleziona **Gestione accessi** > **Utenti**.

   Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia**, un banner blu indica che questa è la grid di origine del tenant. Tutti gli utenti locali che crei su questa grid verranno clonati nell'altra grid della connessione.


2. Seleziona **Crea utente**.

#### ${post_edited_translations.segment}

### Passaggi

1. ${post_edited_translations.segment}

| Campo | Descrizione |
| --- | --- |
| Nome e cognome | ${post_edited_translations.segment} |
| Nome utente | Il nome che questo utente utilizzerà per accedere. I nomi utente devono essere univoci e non possono essere cambiati.<br><br>**Nota**: Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione grid**, si verificherà un errore di clonazione se lo stesso **Username** esiste già per il tenant sulla destinazione grid. |

| Campo | Descrizione |
| --- | --- |
| Password e Conferma password | La password che l'utente userà inizialmente per accedere. |
| Nega l'accesso | Seleziona **Sì** per impedire a questo utente di accedere all'account del tenant, anche se potrebbe ancora appartenere a uno o più gruppi.<br><br>${post_edited_translations.segment} |

2. Seleziona **Continue**.

#### Assegna ai gruppi

**Passaggi**

1. Assegna l'utente a uno o più gruppi locali per determinare quali attività può svolgere.

   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 ad alcun gruppo non avranno permessi di gestione. I permessi sono cumulativi. Gli utenti avranno tutti i permessi per tutti i gruppi a cui appartengono. Vedi "Autorizzazioni per la gestione dei tenant".

2. Seleziona **Crea utente**.

   Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e ti trovi sulla griglia di origine del tenant, il nuovo utente locale viene clonato nella griglia di destinazione del tenant. **Riuscito** appare come **Stato di clonazione** nella sezione Panoramica della pagina dei dettagli dell'utente.

3. ${post_edited_translations.segment}

### ${post_edited_translations.segment}

**Passaggi**

1. Seleziona **Gestione accessi** > **Utenti**.
2. ${post_edited_translations.segment}

   Se il tenant account dispone dell'autorizzazione **Utilizza la connessione di federazione della griglia** e stai visualizzando l'utente sulla griglia di origine del tenant:

   - Un messaggio a comparsa indica che se modifichi o rimuovi un utente, le modifiche non verranno sincronizzate con l'altra grid.
   - Se necessario, un messaggio banner indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. Puoi ${post_edited_translations.segment}.

3. ${post_edited_translations.segment}
   a. Seleziona la casella di controllo per l'utente.
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. Seleziona **Salva modifiche.**

4. Se desideri visualizzare maggiori dettagli o apportare ulteriori modifiche, procedi in uno dei seguenti modi:
   - Seleziona il nome utente.
   - ${post_edited_translations.segment}
5. Esamina la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
   - Nome e cognome
   - Nome utente
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Modalità di accesso
   - ${post_edited_translations.segment}
   - Campi aggiuntivi se il tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e stai visualizzando l'utente sulla griglia di origine del tenant:
     - ${post_edited_translations.segment}
     - Un banner blu indica che, se modifichi questo utente, le modifiche non verranno sincronizzate con l'altra grid.
6. Modifica le impostazioni utente secondo necessità. Consulta ${post_edited_translations.segment} per dettagli su cosa inserire.
   a. Nella sezione Panoramica, modifica il nome completo selezionando il nome o l'icona di modifica .

      ${post_edited_translations.segment}

   b. Nella scheda **Password**, modifica la password dell'utente e seleziona **Salva modifiche**.
   c. ${post_edited_translations.segment}
   d. Nella scheda **Chiavi di accesso**, seleziona **Crea chiave** e segui le istruzioni per "${post_edited_translations.segment}".
   e. Nella scheda **Gruppi**, seleziona **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai gruppi. Quindi, seleziona **Salva modifiche**.
7. Conferma di aver selezionato **Salva modifiche** per ogni sezione che hai modificato.

### Importa utenti federati

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

#### Passaggi

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

   Per inserire più voci, aggiungi ogni UUID o nome utente su una nuova riga.

4. Seleziona **Import**.

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

   a. ${post_edited_translations.segment}

b. ${post_edited_translations.segment}

${post_edited_translations.segment}

### Duplica utente locale

Puoi duplicare un utente locale per creare un nuovo utente più rapidamente.

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

**Passaggi**

1. Seleziona **Gestione accessi** > **Utenti**.
2. ${post_edited_translations.segment}
3. Seleziona **Azioni** > **Duplica utente**.
4. Vedi ${post_edited_translations.segment} per i dettagli su cosa inserire.
5. Seleziona **Crea utente**.

### ${post_edited_translations.segment}

Per riprovare una clonazione non riuscita:

1. Seleziona ciascun utente che riporta la dicitura *(Cloning failed)* sotto il nome utente.
2. ${post_edited_translations.segment}
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ogni utente che stai clonando.

Per ulteriori informazioni, consulta "${post_edited_translations.segment}".

### Elimina uno o più utenti locali

Puoi eliminare definitivamente uno o più utenti locali che non hanno più bisogno di accedere all'account tenant di StorageGRID.

> Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione grid** e elimini un utente locale, StorageGRID non eliminerà l'utente corrispondente sull'altra grid. Se hai bisogno di mantenere sincronizzate queste informazioni, devi eliminare lo stesso utente da entrambe le grid.

> Devi usare l'origine di identità federata per eliminare gli utenti federati.

**Passaggi**

1. Seleziona **Gestione accessi** > **Utenti**.
2. ${post_edited_translations.segment}
3. Seleziona **Azioni** > **Elimina utente** oppure **Azioni** > **Elimina utenti**.

   Viene visualizzata una finestra di dialogo di conferma.

4. ${post_edited_translations.segment}

# ${post_edited_translations.segment}

## Gestisci le chiavi di accesso S3 in StorageGRID

Ogni utente di un tenant account S3 deve avere una chiave di accesso per archiviare e recuperare oggetti nel sistema StorageGRID. Una chiave di accesso è composta da un access key ID e da una secret access key.

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- Gli utenti che dispongono dell'autorizzazione **Root access** possono gestire le chiavi di accesso per l'account root S3 e per tutti gli altri utenti. Le chiavi di accesso root forniscono accesso completo a tutti i bucket e agli oggetti per il tenant, a meno che non sia esplicitamente disabilitato da una bucket policy.

StorageGRID supporta l'autenticazione Signature Version 2 e Signature Version 4. L'accesso tra account non è consentito a meno che non sia esplicitamente abilitato da una bucket policy.

## Crea le tue chiavi di accesso S3 in StorageGRID

Se utilizzi un tenant S3 e hai l'autorizzazione appropriata, puoi creare le tue chiavi di accesso S3. Devi avere una chiave di accesso per accedere ai tuoi bucket e oggetti.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha il "Gestisci le tue credenziali S3 o i permessi di accesso root".

**Informazioni su questa attività**

Puoi creare una o più chiavi di accesso S3 che ti permettono di creare e gestire bucket per il tuo tenant account. Dopo aver creato una nuova chiave di accesso, aggiorna l'applicazione con il nuovo access key ID e la secret access key. Per sicurezza, non creare più chiavi del necessario ed elimina quelle che non usi. Se hai solo una chiave e sta per scadere, crea una nuova chiave prima che la vecchia scada, poi elimina quella vecchia.

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

- Imposta una data di scadenza per le tue chiavi per limitare l'accesso a un determinato periodo di tempo. Impostare una scadenza breve può aiutarti a ridurre il rischio se il tuo access key ID e la tua secret access key vengono accidentalmente esposti. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio per la sicurezza nel tuo ambiente è basso e non hai bisogno di creare periodicamente nuove chiavi, non devi impostare una data di scadenza per le tue chiavi. Se in seguito decidi di creare nuove chiavi, elimina manualmente le vecchie chiavi.

> È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account nel Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota le chiavi di accesso regolarmente, rimuovi le chiavi inutilizzate dal tuo account e non condividerle mai con altri utenti.

**Passaggi**

1. ${post_edited_translations.segment}

   Viene visualizzata la pagina "Le mie chiavi di accesso" e vengono elencate tutte le chiavi di accesso esistenti.

2. ${post_edited_translations.segment}
3. Esegui una delle seguenti operazioni:
   - Seleziona **Non impostare una data di scadenza** per creare una chiave che non scadrà. (Predefinito)
   - Seleziona **Imposta una data di scadenza** e imposta la data e l'ora di scadenza.

     La data di scadenza può essere al massimo di cinque anni dalla data odierna. L'orario di scadenza può essere di minimo un minuto dall'ora attuale.

4. Seleziona **Crea access key**.

   Viene visualizzata la finestra di dialogo "Chiave di accesso per il download", che elenca l'ID della chiave di accesso e la chiave di accesso segreta.

5. Copia l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro, oppure seleziona **Download .csv** per salvare un file foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   Non chiudere questa finestra di dialogo finché non hai copiato o scaricato queste informazioni. Non potrai copiare o scaricare le chiavi dopo la chiusura della finestra di dialogo.

6. Seleziona **Fine**.

   La nuova chiave è elencata nella pagina My access keys.

7. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione di federazione della griglia**, puoi facoltativamente utilizzare l'API di gestione dei tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedi "${post_edited_translations.segment}".

## Visualizza le tue chiavi di accesso S3 in StorageGRID

Se stai utilizzando un tenant S3 e hai le "${post_edited_translations.segment}", puoi visualizzare un elenco delle tue chiavi di accesso S3. Puoi ordinare l'elenco per data di scadenza, così puoi vedere quali chiavi scadranno presto. Se necessario, puoi "crea nuove chiavi" o "elimina chiavi" quelle che non usi più.

È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account nel Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota le chiavi di accesso regolarmente, rimuovi le chiavi inutilizzate dal tuo account e non condividerle mai con altri utenti.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Fai parte di un gruppo di utenti che ha il privilegio "Gestisci le tue credenziali S3" "${post_edited_translations.segment}".

**Passaggi**

1. ${post_edited_translations.segment}
2. Dalla pagina Le mie chiavi di accesso, ordina le chiavi di accesso esistenti per **Expiration time** o **Access key ID**.
3. Se necessario, crea nuove chiavi o elimina quelle che non usi più.

   Se crei nuove chiavi prima della scadenza di quelle esistenti, puoi iniziare a utilizzarle senza perdere temporaneamente l'accesso agli oggetti dell'account.

   Le chiavi scadute vengono rimosse automaticamente.

## Elimina le tue chiavi di accesso S3 in StorageGRID

Se utilizzi un tenant S3 e hai le autorizzazioni appropriate, puoi eliminare le tue chiavi di accesso S3. Dopo che una chiave di accesso è stata eliminata, non può più essere utilizzata per accedere agli oggetti e ai bucket nel tenant account.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Hai il "Gestisci le tue autorizzazioni delle credenziali S3".

> È possibile accedere ai bucket e agli oggetti S3 appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account nel Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota le chiavi di accesso regolarmente, rimuovi le chiavi inutilizzate dal tuo account e non condividerle mai con altri utenti.

**Passaggi**

1. ${post_edited_translations.segment}
2. Dalla pagina My access keys, seleziona la casella di controllo per ogni chiave di accesso che vuoi rimuovere.
3. Seleziona il tasto **Delete**.
4. Nella finestra di dialogo di conferma, seleziona **Elimina chiave**.

   ${post_edited_translations.segment}

## Crea le chiavi di accesso S3 di un altro utente in StorageGRID

${post_edited_translations.segment}

**Prima di iniziare**

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

**Informazioni su questa attività**

Puoi creare una o più chiavi di accesso S3 per altri utenti così possono creare e gestire bucket per il loro account tenant. Dopo che hai creato una nuova chiave di accesso, aggiorna l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per sicurezza, non creare più chiavi di quante ne servano all'utente ed elimina quelle che non vengono usate. Se hai solo una chiave e sta per scadere, crea una nuova chiave prima che la vecchia scada, poi elimina quella vecchia.

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

- Imposta un tempo di scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. L'impostazione di un tempo di scadenza breve può aiutare 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 per la sicurezza nel tuo ambiente è basso e non hai bisogno di creare periodicamente nuove chiavi, non è necessario impostare un tempo di scadenza per le chiavi. Se in seguito decidi di creare nuove chiavi, elimina manualmente le vecchie chiavi.

> È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente nel Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi le chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

**Passaggi**

1. Seleziona **Gestione accessi** > **Utenti**.
2. Seleziona l'utente di cui vuoi gestire le chiavi di accesso S3.

   Viene visualizzata la pagina dei dettagli dell'utente.

3. ${post_edited_translations.segment}
4. Esegui una delle seguenti operazioni:
   - Seleziona **Non impostare una data di scadenza** per creare una chiave che non scade. (Predefinito)
   - Seleziona **Imposta una data di scadenza** e imposta la data e l'ora di scadenza.

     > La data di scadenza può essere al massimo di cinque anni dalla data odierna. L'orario di scadenza può essere di minimo un minuto dall'ora attuale.

5. Seleziona **Crea access key**.

   Viene visualizzata la finestra di dialogo "Chiave di accesso per il download", che elenca l'ID della chiave di accesso e la chiave di accesso segreta.

6. Copia l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro, oppure seleziona **Download .csv** per salvare un file foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   > Non chiudere questa finestra di dialogo finché non hai copiato o scaricato queste informazioni. Non potrai copiare o scaricare le chiavi dopo la chiusura della finestra di dialogo.

7. Seleziona **Fine**.

   ${post_edited_translations.segment}

8. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione di federazione della griglia**, puoi facoltativamente utilizzare l'API di gestione dei tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedi "${post_edited_translations.segment}".

## Visualizza le chiavi di accesso S3 di un altro utente in StorageGRID

Se utilizzi un tenant S3 e hai le autorizzazioni appropriate, puoi visualizzare le chiavi di accesso S3 di un altro utente. Puoi ordinare l'elenco in base alla data di scadenza così puoi vedere quali chiavi scadranno presto. Se serve, puoi creare nuove chiavi ed eliminare quelle che non sono più in uso.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".

> È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente nel Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi le chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

**Passaggi**

1. Seleziona **Gestione accessi** > **Utenti**.
2. Dalla pagina Utenti, seleziona l'utente di cui vuoi vedere le chiavi di accesso S3.
3. Dalla pagina Dettagli utente, seleziona **Chiavi di accesso**.
4. Ordina le chiavi per **Expiration time** o **Access key ID**.
5. Se necessario, crea nuove chiavi ed elimina manualmente quelle che non sono più in uso.

   Se crei nuove chiavi prima che quelle esistenti scadano, l'utente può iniziare a usare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti nell'account.

   Le chiavi scadute vengono rimosse automaticamente.

**Informazioni correlate**

- "Crea le chiavi di accesso S3 di un altro utente"
- "Elimina le chiavi di accesso S3 di un altro utente"

## Elimina le chiavi di accesso S3 di un altro utente in StorageGRID

Se utilizzi un tenant S3 e hai le autorizzazioni appropriate, puoi eliminare le chiavi di accesso S3 di un altro utente. Dopo che una chiave di accesso è stata eliminata, non può più essere utilizzata per accedere agli oggetti e ai bucket nell'account del tenant.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".

> È possibile accedere ai bucket e agli oggetti S3 appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente nel Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruota regolarmente le chiavi di accesso, rimuovi le chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

**Passaggi**

1. Seleziona **Gestione accessi** > **Utenti**.
2. Dalla pagina Utenti, seleziona l'utente di cui vuoi gestire le chiavi di accesso S3.
3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. Nella finestra di dialogo di conferma, seleziona **Elimina chiave**.

${post_edited_translations.segment}

# ${post_edited_translations.segment}

## Crea un bucket S3 di StorageGRID

Puoi usare Tenant Manager per creare bucket S3 per i dati degli oggetti.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Fai parte di un gruppo di utenti che dispone dell'accesso Root o della possibilità di gestire tutti i bucket "${post_edited_translations.segment}". Queste autorizzazioni hanno la precedenza sulle impostazioni di autorizzazione definite nei criteri di gruppo o di bucket.

> Le autorizzazioni per impostare o modificare le proprietà di S3 Object Lock di bucket o oggetti possono essere concesse da "criterio del bucket o criterio di gruppo".

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

> Ciascuna grid può avere un massimo di 100.000 bucket, inclusi "${post_edited_translations.segment}".

**Accedi al wizard**

**Passaggi**

1. ${post_edited_translations.segment}
2. Seleziona **Create bucket**.

### Inserisci i dettagli

**Passaggi**

1. ${post_edited_translations.segment}

| Campo | Descrizione |
| --- | --- |
| Nome bucket | ${post_edited_translations.segment}<br>• Deve essere univoco in ogni sistema StorageGRID (non solo all'interno dell'account del tenant).<br>• Deve essere conforme al DNS.<br>• Devi inserire almeno 3 e non più di 63 caratteri.<br>• ${post_edited_translations.segment}<br>• Le richieste di tipo virtual hosted non devono contenere punti. I punti causeranno problemi con la verifica del certificato wildcard del server.<br>Per ulteriori informazioni, consultare il "${post_edited_translations.segment}".<br>${post_edited_translations.segment} |
| Regione | La regione del bucket.<br>Il tuo amministratore StorageGRID gestisce le aree geografiche disponibili. L'area geografica di un bucket può influire sulla policy di protezione dei dati applicata agli oggetti. Per impostazione predefinita, tutti i bucket vengono creati nell'area geografica `us-east-1`. Se l'area geografica predefinita è configurata su un'area diversa da `us-east-1`, quest'altra area viene inizialmente selezionata nel menu a discesa.<br>${post_edited_translations.segment} |

2. Seleziona **Continue**.

### Gestisci le impostazioni

**Passaggi**

1. Facoltativamente, puoi abilitare il versioning degli oggetti per il bucket.

   Abilita il versioning degli oggetti se desideri archiviare ogni versione di ciascun oggetto in questo bucket. Puoi quindi recuperare le versioni precedenti di un oggetto secondo necessità.

   Devi abilitare il versioning degli oggetti se:

   - ${post_edited_translations.segment}
   - Vuoi creare un "bucket branch" da questo bucket.

2. Se l'impostazione globale S3 Object Lock è abilitata, puoi abilitare facoltativamente S3 Object Lock per il bucket per archiviare oggetti utilizzando un modello WORM (write-once-read-many).

   Abilita S3 Object Lock per un bucket solo se devi conservare gli oggetti per un periodo di tempo stabilito, ad esempio per soddisfare determinati requisiti normativi. S3 Object Lock è un'impostazione permanente

che ti aiuta a evitare che gli oggetti vengano eliminati o sovrascritti per un periodo di tempo stabilito o a tempo indeterminato.

> Una volta attivata l'impostazione S3 Object Lock per un bucket, non puoi disattivarla. Chiunque abbia le autorizzazioni corrette può aggiungere oggetti a questo bucket che non possono essere modificati. Potresti non riuscire a eliminare questi oggetti o il bucket stesso.

Se abiliti il blocco degli oggetti S3 per un bucket, la gestione delle versioni del bucket viene abilitata automaticamente.

3. Se hai selezionato **Abilita S3 Object Lock**, puoi facoltativamente abilitare **Default retention** per questo bucket.

> L'amministratore della grid deve darti l'autorizzazione per "usare funzionalità specifiche di S3 Object Lock".

Quando la **conservazione predefinita** è abilitata, i nuovi oggetti aggiunti al bucket verranno protetti automaticamente dall'eliminazione o dalla sovrascrittura. L'impostazione di **conservazione predefinita** non si applica agli oggetti che hanno i propri periodi di conservazione.

a. ${post_edited_translations.segment}

| Modalità di conservazione predefinita | Descrizione |
|---|---|
| Governance | • Gli utenti con l' `s3:BypassGovernanceRetention`autorizzazione possono usare l' `x-amz-bypass-governance-retention: true`intestazione della richiesta per bypassare le impostazioni di conservazione.<br>• Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione prevista.<br>• Questi utenti possono aumentare, diminuire o rimuovere la retain-until-date di un oggetto. |
| Conformità | • L'oggetto non può essere eliminato fino al raggiungimento della sua retain-until-date.<br>• La data di conservazione dell'oggetto può essere aumentata, ma non può essere diminuita.<br>• La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.<br><br>**Nota**: L'amministratore della grid deve consentirti di utilizzare la modalità di conformità. |

b. Se l'opzione **Conservazione predefinita** è abilitata, specifica il **periodo di conservazione predefinito** per il bucket.

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

Un *periodo di conservazione massimo*, che può variare da 1 giorno a 100 anni, viene impostato quando l'amministratore della griglia crea il tenant. Quando imposti un *periodo di conservazione predefinito*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedi all'amministratore della griglia 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 questo bucket. Questo valore rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).

   Se non imposti alcun limite, la capacità di questo bucket è illimitata. Consulta "${post_edited_translations.segment}" per maggiori informazioni.

5. Facoltativamente, seleziona **Abilita limite al numero di oggetti**.

   Il limite di oggetti rappresenta il numero massimo di oggetti che questo bucket può contenere. Questo valore rappresenta una quantità logica (numero di oggetti). Se non viene impostato alcun limite, il numero di oggetti è illimitato.

6. Seleziona **Create bucket**.

   ${post_edited_translations.segment}

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

Puoi anche "${post_edited_translations.segment}" se necessario.

## Visualizza i dettagli del bucket S3 in StorageGRID

Puoi visualizzare i bucket nel tuo tenant account.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che dispone delle "Autorizzazione di accesso root, gestisci tutti i bucket o visualizza tutti i bucket". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o di bucket.

**Passaggi**

1. ${post_edited_translations.segment}

   Viene visualizzata la pagina Buckets.

2. Esamina la tabella riassuntiva per ciascun bucket.

   Se necessario, puoi ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco avanti e indietro.

   I valori visualizzati relativi a Conteggio oggetti, Spazio utilizzato e Utilizzo sono stime. Queste stime sono influenzate dal momento dell'ingestione, dalla connettività di rete e dallo stato dei nodi. Se per i bucket è abilitato il versioning, le versioni degli oggetti eliminati sono incluse nel conteggio degli oggetti.

**Nome**

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

**Funzionalità abilitate**

Elenco delle funzionalità abilitate per il bucket.

**Blocco oggetto S3**

${post_edited_translations.segment}

Questa colonna viene visualizzata solo se il blocco degli oggetti S3 è abilitato per la griglia. Questa colonna mostra anche le informazioni per eventuali bucket Compliant legacy.

**Regione**

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

**Conteggio oggetti**

Il numero di oggetti in questo bucket. Se per i bucket è abilitato il versioning, in questo valore sono incluse anche le versioni degli oggetti non correnti.

Quando aggiungi o elimini oggetti, questo valore potrebbe non aggiornarsi 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 con erasure coding o per i metadati degli oggetti.

Questo valore può impiegare fino a 10 minuti per aggiornarsi.

**Utilizzo**

La percentuale utilizzata rispetto al limite di capacità del bucket, se impostato.

Il valore di utilizzo si basa su stime interne e potrebbe essere superato in alcuni casi. Ad esempio, StorageGRID verifica il limite di capacità (se impostato) quando un tenant inizia a caricare oggetti e rifiuta nuovi caricamenti 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 vengono eliminati oggetti, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti in questo bucket finché l'utilizzo del limite di capacità non viene ricalcolato. I calcoli possono richiedere 10 minuti o più.

Questo valore indica la dimensione logica, non la dimensione fisica necessaria per memorizzare gli oggetti e i loro metadati.

**Capacità**

Se impostato, il limite di capacità per il bucket.

**Data di creazione**

Data e ora di creazione del bucket. Questa colonna è nascosta per impostazione predefinita.

3. Per visualizzare i dettagli relativi a uno specifico bucket, seleziona il nome del bucket dalla tabella.
   a. ${post_edited_translations.segment}
   b. Visualizza le barre di utilizzo del limite di capacità e del limite di conteggio degli oggetti. Se l'utilizzo è al 100% o vicino al 100%, valuta se aumentare il limite o eliminare alcuni oggetti.

c. Se necessario, seleziona **Elimina oggetti nel bucket** e **Elimina bucket**.

> Presta molta attenzione agli avvisi che compaiono quando selezioni ciascuna di queste opzioni. Per ulteriori informazioni, consulta:
>
> - "Elimina tutti gli oggetti in un bucket"
> - "Elimina un bucket" (il bucket deve essere vuoto)

d. Visualizza o modifica le impostazioni del bucket in ciascuna delle schede secondo necessità.

- **Console S3**: Visualizza gli oggetti per il bucket. Per ulteriori informazioni, consulta "Usa la console S3".
- **Opzioni del bucket**: Visualizza o modifica le impostazioni delle opzioni. Alcune impostazioni, come S3 Object Lock, non possono essere modificate dopo la creazione del bucket.
  - "Gestisci la coerenza dei bucket"
  - "Aggiornamenti dell'ora dell'ultimo accesso"
  - "Limite di capacità"
  - "Limite del numero di oggetti"
  - "Versioning degli oggetti"
  - "Blocco oggetto S3"
  - "Conservazione predefinita del bucket"
  - "${post_edited_translations.segment}" (se consentito per il tenant)
- **Servizi della piattaforma**: "Gestisci i servizi della piattaforma" (se consentiti per il tenant)
- **Accesso al bucket**: Visualizza o modifica le impostazioni delle opzioni. Devi disporre di autorizzazioni di accesso specifiche.
  - Configura "CORS per bucket e oggetti" in modo che il bucket e gli oggetti nel bucket siano accessibili alle applicazioni web di altri domini.
  - "Controlla l'accesso degli utenti" per un bucket S3 e gli oggetti in quel bucket.
- **Rami**: Visualizza l'elenco dei bucket dei rami per il bucket. "Crea un nuovo bucket di branch o gestisci i bucket di branch".

## Scopri i bucket di ramo di StorageGRID

Un bucket di ramo fornisce accesso agli oggetti in un bucket come esistevano in un determinato momento.

Crei un bucket di diramazione da un bucket esistente. Dopo che hai creato un bucket di diramazione, il bucket originale da cui è stato creato viene chiamato *bucket di base*. Inoltre, puoi creare un bucket di diramazione da un altro bucket di diramazione.

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

- "Blocco oggetto S3"
- "Replicazione cross-grid" per bucket di base
- "Politiche dei bucket" per i bucket versionati per eliminare le vecchie versioni degli oggetti

Nota le seguenti caratteristiche dei bucket di ramificazione:

- Puoi accedere agli oggetti nei bucket di filiale usando "Console S3 per scaricare oggetti".
- Quando i client accedono agli oggetti in un bucket di una filiale, "politiche di accesso"sono le policy del bucket della filiale, piuttosto che quelle del bucket di base, a determinare se l'accesso viene concesso o negato.
- Gli oggetti creati in un bucket di base vengono valutati in base a come "Regole ILM" si applicano al bucket di base. Gli oggetti creati in un bucket di diramazione vengono valutati in base a come le regole ILM si applicano al bucket di diramazione.
- La replica tra griglie non è supportata per i bucket di branch.
- I servizi della piattaforma non sono supportati per i bucket branch.

**Esempi di utilizzo del bucket branch**

- Puoi usare un bucket di diramazione per rimuovere oggetti danneggiati creando un bucket di diramazione da un momento precedente al verificarsi del danneggiamento e poi indirizzando le applicazioni al bucket di diramazione invece che al bucket di base che contiene oggetti danneggiati.
- Stai salvando dati in un bucket versionato. C'è stata una vulnerabilità accidentale che ha causato l'ingestione di molti oggetti indesiderati dopo il tempo *T*. Puoi creare un bucket di diramazione per il valore del tempo Before, *T*, e reindirizzare le operazioni dei client a quel bucket di diramazione. Così, solo gli oggetti ingeriti prima del tempo Before *T* sono esposti ai client.

**Operazioni sugli oggetti nei bucket di branch**

- Un'operazione PUT su un bucket branch crea un oggetto nel branch.
- Un'operazione GET su un bucket di branch recupera un oggetto dal branch. Se l'oggetto non esiste nel bucket di branch, viene recuperato dal bucket di base.
- L'eliminazione degli oggetti dai bucket branch avviene come segue:

| Operazione | Target | Risultato | Visibilità degli oggetti nel bucket di base | Visibilità degli oggetti nel bucket del branch |
|---|---|---|---|---|
| Elimina senza ID versione | Bucket di base | Il marcatore di eliminazione viene creato solo per il bucket di base | HEAD/GET restituisce Oggetto non esiste, ma puoi comunque accedere a versioni specifiche | HEAD/GET restituisce Oggetto esiste e puoi ancora accedere a versioni specifiche<br><br>Il marcatore di eliminazione sarebbe stato creato dopo il bucket del ramo `beforeTime`. |
| Elimina con ID versione | Bucket di base | La versione specifica dell'oggetto viene eliminata sia per il bucket base che per il bucket branch. | HEAD/GET restituisce La versione dell'oggetto non esiste | HEAD/GET restituisce La versione dell'oggetto non esiste |

| Operazione | Target | Risultato | Visibilità degli oggetti nel bucket di base | Visibilità degli oggetti nel bucket del branch |
|---|---|---|---|---|
| Elimina senza ID versione | Bucket del branch | Il marcatore di eliminazione viene creato solo per il bucket branch | HEAD/GET restituisce l'oggetto (l'oggetto base del bucket non viene modificato) | HEAD/GET restituisce Oggetto inesistente |
| Elimina con ID versione | Bucket del branch | La versione specifica dell'oggetto viene eliminata solo per il bucket branch | HEAD/GET restituisce una versione specifica dell'oggetto (l'oggetto del bucket di base non è interessato) | HEAD/GET restituisce La versione dell'oggetto non esiste |

Consultare anche "Come vengono eliminati gli oggetti versionati di S3".

## Gestisci i bucket di filiale di StorageGRID

Utilizza il 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 l'autorizzazione per tutti i bucket". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o di bucket.
- Il bucket di base da cui vuoi creare un ramo ha "versioning abilitato".
- Sei il proprietario del bucket di base.

**Informazioni su questa attività**

Nota le seguenti informazioni sui bucket di ramo:

- Le autorizzazioni per impostare le proprietà di blocco degli oggetti S3 di bucket o oggetti possono essere concesse da "criterio del bucket o criterio di gruppo".
- ${post_edited_translations.segment}

> Dopo che hai configurato e creato un bucket di filiale, non puoi più modificarne la configurazione.

**${post_edited_translations.segment}**

**Passaggi**

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

### Inserisci i dettagli

**Passaggi**

1. ${post_edited_translations.segment}

| Campo | Descrizione |
| --- | --- |
| Nome del bucket del branch | ${post_edited_translations.segment}<br>• Deve essere univoco in ogni sistema StorageGRID (non solo all'interno dell'account del tenant).<br>• Deve essere conforme al DNS.<br>• Devi inserire almeno 3 e non più di 63 caratteri.<br>• ${post_edited_translations.segment}<br>• Le richieste di tipo virtual hosted non devono contenere punti. I punti causeranno problemi con la verifica del certificato wildcard del server.<br>Per ulteriori informazioni, consultare il "${post_edited_translations.segment}".<br>**Nota**: Non puoi cambiare il nome dopo aver creato il bucket del ramo. |
| Regione (non puoi modificarla per i bucket di branch) | La regione del bucket del branch.<br>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 | L'orario limite per cui le versioni degli oggetti create nel bucket di base sono accessibili dal bucket di diramazione. Il bucket di diramazione fornisce accesso alle versioni degli oggetti create prima dell'orario limite.<br>Prima di time deve essere una data e un'ora trascorse. Non può essere una data futura. |
| Tipo di bucket branch | • **Lettura/scrittura**: Puoi aggiungere o eliminare oggetti o versioni di oggetti nel bucket del branch.<br>• **Sola lettura**: Non puoi modificare gli oggetti nel bucket del branch.<br>**Nota**: puoi impostare il tipo di bucket branch su sola lettura solo se il bucket branch è vuoto. Se il tipo di un bucket branch esistente è impostato su lettura-scrittura e non vi hai ancora scritto, puoi modificare il tipo in sola lettura. |

2. Seleziona **Continue**.

### Gestisci le impostazioni dell'oggetto (facoltativo)

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

**Passaggi**

1. Se l'impostazione globale di S3 Object Lock è abilitata, puoi abilitare facoltativamente S3 Object Lock anche per il bucket della filiale. Per abilitare S3 Object Lock, il bucket della filiale deve essere un bucket di lettura/scrittura.

   Abilita S3 Object Lock per un bucket di filiale solo se devi conservare gli oggetti per un periodo di tempo determinato, ad esempio per soddisfare specifici requisiti normativi. S3 Object Lock è un'impostazione permanente che ti aiuta a impedire che gli oggetti vengano eliminati o sovrascritti per un periodo di tempo determinato o a tempo indeterminato.

   > Una volta abilitata l'impostazione Blocco oggetti S3 per un bucket, non può essere disabilitata. Chiunque disponga delle autorizzazioni corrette può aggiungere oggetti al bucket del branch che non possono essere modificati. Potresti non riuscire a eliminare questi oggetti o il bucket del branch stesso.

2. Se hai selezionato **Abilita blocco oggetto S3**, puoi facoltativamente abilitare **periodo di conservazione predefinito** per il bucket del ramo.

   > L'amministratore della grid deve darti l'autorizzazione per "usare funzionalità specifiche di S3 Object Lock".

   Quando l'impostazione **Conservazione predefinita** è abilitata, 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 il proprio periodo di conservazione.

   a. Se è abilitata l'opzione **Conservazione predefinita**, specifica una **Modalità di conservazione predefinita** per il bucket del ramo.

| Modalità di conservazione predefinita | Descrizione |
|---|---|
| Governance | • Gli utenti con l' `s3:BypassGovernanceRetention`autorizzazione possono usare l' `x-amz-bypass-governance-retention: true`intestazione della richiesta per bypassare le impostazioni di conservazione.<br>• Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione prevista.<br>• Questi utenti possono aumentare, diminuire o rimuovere la retain-until-date di un oggetto. |
| Conformità | • L'oggetto non può essere eliminato fino al raggiungimento della sua retain-until-date.<br>• La data di conservazione dell'oggetto può essere aumentata, ma non può essere diminuita.<br>• La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.<br>**Nota**: L'amministratore della grid deve consentirti di utilizzare la modalità di conformità. |

   b. Se l'opzione **Conservazione predefinita** è abilitata, specifica il **periodo di conservazione predefinito** per il bucket della filiale.

Il **periodo di conservazione predefinito** indica per quanto tempo devono essere conservati i nuovi oggetti aggiunti al bucket del ramo, a partire dal momento in cui vengono acquisiti. Specifica un valore che sia inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della grid.

Un *periodo di conservazione massimo*, che può variare da 1 giorno a 100 anni, viene impostato quando l'amministratore della griglia crea il tenant. Quando imposti un *periodo di conservazione predefinito*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedi all'amministratore della griglia di aumentare o diminuire il periodo di conservazione massimo.

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

   Il limite di capacità rappresenta la capacità massima disponibile per il bucket di filiale. 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 diramazione è illimitata. Consulta "${post_edited_translations.segment}" 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 al numero di oggetti**.

   Il limite di conteggio degli oggetti rappresenta il numero massimo di oggetti che il bucket del ramo può contenere. Questo valore rappresenta una quantità logica (conteggio degli oggetti). Se non viene impostato alcun limite, il conteggio degli 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. Seleziona **Create bucket**.

   Il bucket del ramo viene creato e aggiunto alla tabella nella pagina Buckets.

6. Facoltativamente, seleziona **Vai alla pagina dei dettagli del bucket** "visualizza i dettagli del branch bucket" e configura ulteriormente.

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

## Applica un tag di policy ILM a un bucket StorageGRID

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

La policy ILM controlla dove vengono memorizzati i dati degli oggetti e se vengono eliminati dopo un determinato periodo di tempo. Il tuo amministratore di grid crea le policy ILM e le assegna ai tag della policy ILM quando si utilizzano più policy attive.

> Evita di riassegnare frequentemente il tag di policy di un bucket. Altrimenti potrebbero verificarsi problemi di prestazioni.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che dispone delle "Autorizzazione di accesso root, gestisci tutti i bucket o visualizza tutti i bucket". Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o di bucket.

**Passaggi**

1. ${post_edited_translations.segment}

   Viene visualizzata la pagina Bucket. Se necessario, puoi ordinare le informazioni in base a qualsiasi colonna oppure puoi scorrere avanti e indietro l'elenco.

2. ${post_edited_translations.segment}

   Puoi anche modificare l'assegnazione del tag della policy ILM per un bucket a cui è già stato assegnato un tag.

   I valori visualizzati per il numero di oggetti e lo spazio utilizzato sono stime. Queste stime sono influenzate dal momento dell'ingestione, dalla connettività di rete e dallo stato dei nodi. Se i bucket hanno il versioning abilitato, le versioni degli oggetti eliminati sono incluse nel conteggio degli oggetti.

3. Nella scheda Opzioni bucket, espandi il menu a fisarmonica Tag policy ILM. Questo menu a fisarmonica viene visualizzato solo se l'amministratore della griglia ha abilitato l'utilizzo di tag policy personalizzati.
4. ${post_edited_translations.segment}

   La modifica del tag della policy ILM per un bucket attiverà una rivalutazione di ILM di tutti gli oggetti nel bucket. Se la nuova policy conserva gli oggetti per un periodo di tempo limitato, gli oggetti più vecchi saranno eliminati.

5. ${post_edited_translations.segment}
6. Seleziona **Salva modifiche**. Un nuovo tag del bucket S3 verrà impostato sul bucket con la chiave `NTAP-SG-ILM-BUCKET-TAG` e il valore del nome del tag del criterio ILM.

   Assicurati che le tue applicazioni S3 non sovrascrivano o eliminino accidentalmente il nuovo tag 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 alla policy ILM predefinita.

   Imposta e modifica i tag della policy ILM usando solo il Tenant Manager o l'API di Tenant Manager, dove il tag della policy ILM viene validato. Non modificare il tag della policy ILM usando l'API S3 PutBucketTagging o l'API S3 DeleteBucketTagging. `NTAP-SG-ILM-BUCKET-TAG`

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

## Gestisci la policy dei bucket di StorageGRID

Puoi controllare l'accesso degli utenti a un bucket S3 e agli oggetti in quel bucket.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha le "Permesso 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 Storage Node e siti sia disponibile. Se due o più Storage Node non sono disponibili in un sito, o se un sito non è disponibile, potrebbe non essere possibile modificare queste impostazioni.

**Passaggi**

1. Seleziona **Buckets**, quindi seleziona il bucket che desideri gestire.
2. Nella pagina dei dettagli del bucket, seleziona **Accesso al bucket** > **Criteri del bucket**.
3. Esegui una delle seguenti operazioni:
   - Inserisci una bucket policy selezionando la casella di controllo **Abilita policy**. Quindi inserisci una stringa valida in formato JSON.

     ${post_edited_translations.segment}

   - Modifica una policy esistente modificando la stringa.
   - ${post_edited_translations.segment}

Per informazioni dettagliate sulle policy dei bucket, inclusa la sintassi del linguaggio ed esempi, vedi "Esempi di policy dei bucket".

## Gestire la coerenza dei bucket di StorageGRID

I valori di coerenza possono essere utilizzati per specificare la disponibilità delle modifiche alle impostazioni del bucket, nonché per bilanciare la disponibilità degli oggetti all'interno di un bucket e la coerenza di tali oggetti tra diversi Storage Node e siti. Puoi modificare i valori di coerenza in modo che siano diversi da quelli predefiniti, così le applicazioni client possono soddisfare le loro esigenze operative.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha le "Gestisci tutti i bucket o autorizzazione di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o di bucket.

### Linee guida sulla coerenza dei bucket

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

### Modifica della coerenza del bucket

Se la coerenza **Read-after-new-write** non soddisfa i requisiti dell'applicazione client, puoi modificarla impostando la coerenza del bucket o utilizzando l' `Consistency-Control`intestazione. L' `Consistency-Control`intestazione ha la precedenza sulla coerenza del bucket.

Quando cambi la consistenza di un bucket, solo gli oggetti ingeriti dopo la modifica sono garantiti di rispettare la nuova impostazione.

**Passaggi**

1. Seleziona **Visualizza bucket** dalla dashboard oppure seleziona **STORAGE (S3)** > **Buckets**.
2. Seleziona il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni del bucket**, seleziona l'**accordion**.
4. Seleziona una coerenza per le operazioni eseguite sugli oggetti in questo bucket.
   - **Tutti**: Garantisce il massimo livello di coerenza. Tutti i nodi ricevono i dati immediatamente, oppure la richiesta fallisce.
   - **Strong-global**: Garantisce la coerenza read-after-write per tutte le richieste dei client su 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** (impostazione predefinita): garantisce la coerenza read-after-write per i nuovi oggetti e la coerenza finale per gli aggiornamenti degli oggetti. Offre elevata disponibilità e garanzie di protezione dei dati. Consigliato nella maggior parte dei casi.
   - **Disponibile**: Fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, usalo solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.
5. Seleziona **Salva modifiche**.

**${post_edited_translations.segment}**

${post_edited_translations.segment}

Le seguenti impostazioni del bucket utilizzano la coerenza **forte** per impostazione predefinita. Se due o più Storage Node non sono disponibili in un sito, o se un sito non è disponibile, eventuali modifiche a queste impostazioni potrebbero non essere disponibili.

- "${post_edited_translations.segment}"
- "Ultimo accesso"
- "Ciclo di vita del bucket"
- "Criteri del bucket"
- "${post_edited_translations.segment}"
- "Versioning del bucket"
- "Blocco oggetto S3"
- "Crittografia del bucket"

Il valore di coerenza per il versioning dei bucket, il blocco degli oggetti S3 e la crittografia dei bucket non può essere impostato su un valore che non sia fortemente coerente.

Le seguenti impostazioni dei bucket non utilizzano la coerenza forte e presentano una maggiore disponibilità

alle modifiche. Le modifiche a queste impostazioni potrebbero richiedere del tempo prima di avere effetto.

- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"
- Modifica la coerenza del bucket

> Se la coerenza predefinita utilizzata durante la modifica delle impostazioni del bucket non soddisfa i requisiti dell'applicazione client, puoi modificare la coerenza utilizzando l'intestazione `Consistency-Control` per "${post_edited_translations.segment}" o utilizzando le opzioni `reducedConsistency` o `force` in "API di gestione tenant".

## Abilita o disabilita gli aggiornamenti dell'ora dell'ultimo accesso in StorageGRID

Quando gli amministratori grid creano le regole di gestione del ciclo di vita delle informazioni (ILM) per un sistema StorageGRID, possono facoltativamente specificare che l'ora dell'ultimo accesso di un oggetto venga utilizzata per determinare se spostare tale oggetto in una posizione di storage diversa. Se utilizzi un tenant S3, puoi sfruttare queste regole abilitando gli aggiornamenti dell'ora dell'ultimo 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 accesso** come filtro avanzato o come tempo di riferimento. Puoi ignorare queste istruzioni se il tuo sistema StorageGRID non include una regola di questo tipo. Vedi "Usa l'ora dell'ultimo accesso nelle regole ILM" per i dettagli.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha le "Gestisci tutti i bucket o autorizzazione di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o di bucket.

### Informazioni su questa attività

**Ora dell'ultimo accesso** è una delle opzioni disponibili per l'istruzione di posizionamento **Ora di riferimento** per una regola ILM. L'impostazione dell'Ora di riferimento per una regola su Ora dell'ultimo accesso consente agli amministratori della griglia di specificare che gli oggetti vengano collocati in determinate posizioni di storage in base a quando sono stati recuperati l'ultima volta (letti o visualizzati).

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Per impostazione predefinita, gli aggiornamenti all'ora dell'ultimo accesso sono disabilitati. Se il tuo sistema StorageGRID include una regola ILM che utilizza l'opzione **Ora dell'ultimo accesso** e desideri che questa opzione si applichi agli oggetti in questo bucket, devi abilitare gli aggiornamenti all'ora dell'ultimo accesso per i bucket S3 specificati in tale regola.

> L'aggiornamento dell'ora dell'ultimo accesso quando un oggetto viene recuperato può ridurre le prestazioni di StorageGRID, soprattutto per gli oggetti di piccole dimensioni.

${post_edited_translations.segment}

- Aggiorna gli oggetti con nuovi timestamp
- ${post_edited_translations.segment}

${post_edited_translations.segment}

| Tipo di richiesta | Comportamento se l'impostazione dell'ultimo accesso è disabilitata (impostazione predefinita) | | Comportamento se il tempo di ultimo accesso è abilitato | |
|---|---|---|---|---|
| | Ultima data di accesso aggiornata? | Oggetto aggiunto alla coda di valutazione ILM? | Ultima data di accesso aggiornata? | 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 recupero di un oggetto, del relativo access control list o dei relativi metadati | No | No | Sì | Sì |
| Richiesta di aggiornamento dei metadati di un oggetto | Sì | Sì | Sì | Sì |
| Richiesta di elencare oggetti o versioni di oggetti | No | No | No | No |
| Richiesta di copiare un oggetto da un bucket a un altro | • No, per la copia sorgente<br>• Sì, per la copia di destinazione | • No, per la copia sorgente<br>• Sì, per la copia di destinazione | • Sì, per la copia di origine<br>• Sì, per la copia di destinazione | • Sì, per la copia di origine<br>• Sì, per la copia di destinazione |
| Richiesta di completamento di un caricamento in più parti | Sì, per l'oggetto assemblato | Sì, per l'oggetto assemblato | Sì, per l'oggetto assemblato | Sì, per l'oggetto assemblato |

**Passaggi**

1. ${post_edited_translations.segment}

2. Seleziona il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona l'accordion **Aggiornamenti dell'ora dell'ultimo accesso**.
4. Attiva o disattiva l'aggiornamento dell'ora dell'ultimo accesso.
5. Seleziona **Salva modifiche**.

## Modifica la versione degli oggetti per un bucket S3 in StorageGRID

Se usi un tenant S3, puoi modificare lo stato di versioning per i bucket S3.

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha le "Gestisci tutti i bucket o autorizzazione di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o di bucket.
- Hai verificato che il numero richiesto di Storage Node e siti sia disponibile. Se due o più Storage Node non sono disponibili in un sito, o se un sito non è disponibile, potrebbe non essere possibile modificare queste impostazioni.

**Informazioni su questa attività**

Puoi abilitare o sospendere il versioning degli oggetti per un bucket. Dopo che hai abilitato il versioning per un bucket, non può più tornare a uno stato senza versioning. Tuttavia, puoi sospendere il versioning per il bucket.

- Disabilitato: il versioning non è mai stato abilitato
- Abilitato: la gestione delle versioni è abilitata
- Sospeso: la gestione delle versioni era precedentemente abilitata ed è sospesa

Per ulteriori informazioni, consulta quanto segue:

- "Versioning degli oggetti"
- "Regole e politiche ILM per gli oggetti versionati S3 (Esempio 4)"
- "Come vengono eliminati gli oggetti"

**Passaggi**

1. ${post_edited_translations.segment}
2. Seleziona il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la sezione **Versionamento oggetti**.
4. Seleziona uno stato di versioning per gli oggetti in questo bucket.

   Il versioning degli oggetti deve rimanere abilitato per un bucket utilizzato per la replica cross-grid. Se è abilitato S3 Object Lock o la conformità legacy, le opzioni di **Object versioning** sono disabilitate.

| Opzione | Descrizione |
| --- | --- |
| Abilita il versioning | Abilita il versioning degli oggetti se desideri archiviare ogni versione di ciascun oggetto in questo bucket. Puoi quindi recuperare le versioni precedenti di un oggetto secondo necessità.<br><br>Gli oggetti già presenti nel bucket verranno versionati quando vengono modificati da un utente. |
| Sospendi il versioning | Sospendi il controllo delle versioni degli oggetti se non vuoi più che vengano create nuove versioni degli oggetti. Puoi comunque recuperare le versioni degli oggetti esistenti. |

5. Seleziona **Salva modifiche**.

## Utilizza S3 Object Lock per conservare gli oggetti in StorageGRID

Puoi usare S3 Object Lock se i bucket e gli oggetti devono rispettare i requisiti normativi per la conservazione.

L'amministratore della griglia deve darti il permesso di usare funzionalità specifiche di S3 Object Lock.

### Che cos'è S3 Object Lock?

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

Quando l'impostazione globale S3 Object Lock è abilitata per un sistema StorageGRID, un tenant account S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock abilitato, il versioning del bucket è obbligatorio e viene abilitato automaticamente.

**Un bucket senza S3 Object Lock** può contenere solo oggetti per i quali non sono specificate impostazioni di conservazione. Nessun oggetto ingerito avrà impostazioni di conservazione.

Un bucket con S3 Object Lock può contenere oggetti con o senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

**Un bucket con S3 Object Lock e periodo di conservazione predefinito configurato** può avere oggetti caricati con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, perché l'impostazione di conservazione non è stata configurata a livello di oggetto.

In pratica, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurato il periodo di conservazione predefinito. Gli oggetti esistenti senza impostazioni di conservazione rimangono invariati.

#### Modalità di retention

La funzionalità S3 Object Lock di StorageGRID supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità sono equivalenti alle modalità di conservazione di Amazon S3.

- In modalità conformità:

    - L’oggetto non può essere eliminato fino al raggiungimento della sua retain-until-date.
    - La data di conservazione dell’oggetto 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 determinate impostazioni di conservazione.
    - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione prevista.
    - Questi utenti possono aumentare, diminuire o rimuovere la retain-until-date di un oggetto.

#### Impostazioni di conservazione per le versioni degli oggetti

Se crei un bucket con la funzionalità S3 Object Lock abilitata, puoi usare l’applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione**: conformità o governance.
- **Retain-until-date**: Se la retain-until-date di una versione dell’oggetto è nel futuro, l’oggetto può essere recuperato, ma non può essere eliminato.
- **Blocco legale**: L’applicazione di un blocco legale a una versione di un oggetto blocca immediatamente quell’oggetto. Ad esempio, potresti dover applicare un blocco legale a un oggetto che è collegato a un’indagine o a una controversia legale. Un blocco legale non ha una data di scadenza, ma rimane in vigore finché non viene esplicitamente rimosso. I blocchi legali sono indipendenti dalla retain-until-date.

> Se un oggetto è soggetto a un blocco legale, nessuno può eliminare l’oggetto, indipendentemente dalla sua modalità di conservazione.

Per i dettagli sulle impostazioni dell’oggetto, vedi "Utilizza l’API REST S3 per configurare S3 Object Lock".

#### Impostazione di conservazione predefinita per i bucket

Se crei un bucket con S3 Object Lock abilitato, puoi facoltativamente specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita**: conformità o governance.
- **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 hanno le proprie impostazioni di conservazione. Gli oggetti esistenti nel bucket non vengono influenzati quando aggiungi o modifichi queste impostazioni predefinite.

Vedi "Crea un bucket S3" e "Aggiorna la conservazione predefinita del blocco oggetto S3".

### Attività di blocco oggetto S3

I seguenti elenchi per gli amministratori della griglia e gli utenti tenant contengono le high-level attività per l’utilizzo della funzionalità S3 Object Lock.

**Amministratore della grid**

- Abilita l'impostazione globale di S3 Object Lock per l'intero sistema StorageGRID.
- Assicurati che le policy di information lifecycle management (ILM) siano *conformi*; cioè che soddisfino i "requisiti dei bucket con S3 Object Lock abilitato".
- Se necessario, consenti a un tenant di utilizzare Compliance come modalità di conservazione. Altrimenti, è consentita solo la modalità Governance.
- Se necessario, imposta un periodo massimo di conservazione per un tenant.

**Utente tenant**

- Esamina le considerazioni relative a bucket e oggetti con S3 Object Lock.
- Se necessario, contatta l'amministratore della grid per abilitare l'impostazione globale S3 Object Lock e impostare le autorizzazioni.
- Crea bucket con S3 Object Lock abilitato.
- Facoltativamente, puoi configurare le impostazioni di conservazione predefinite per un bucket:
  - Modalità di conservazione predefinita: Governance o Compliance, se consentita dall'amministratore della grid.
  - Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall'amministratore della griglia.
- Utilizza l'applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica per ciascun oggetto:
  - Modalità di conservazione. Governance o Compliance, se consentito dall'amministratore del grid.
  - Data di conservazione: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall'amministratore della griglia.

**Requisiti per i bucket con S3 Object Lock abilitato**

- Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID, puoi usare il Tenant Manager, la Tenant Management API o la S3 REST API per creare bucket con S3 Object Lock abilitato.
- Se intendi utilizzare S3 Object Lock, devi abilitarlo quando crei il bucket. Non puoi abilitare S3 Object Lock per un bucket esistente.
- Quando il blocco degli oggetti S3 è abilitato per un bucket, StorageGRID abilita automaticamente il versioning per quel bucket. Non puoi disabilitare il blocco degli oggetti S3 o sospendere il versioning per il bucket.
- Facoltativamente, puoi specificare una modalità di conservazione predefinita e un periodo di conservazione per ogni bucket utilizzando il Tenant Manager, la Tenant Management API o la S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non hanno proprie impostazioni di conservazione. Puoi ignorare queste impostazioni predefinite specificando una modalità di conservazione e una retain-until-date per ogni versione dell'oggetto quando viene caricata.
- La configurazione del ciclo di vita dei bucket è supportata per i bucket con S3 Object Lock abilitato.
- CloudMirror replication non è supportata per i bucket con S3 Object Lock abilitato.

**Requisiti per gli oggetti nei bucket con S3 Object Lock abilitato**

- Per proteggere una versione di un oggetto, puoi specificare le impostazioni di conservazione predefinite per il bucket oppure puoi specificare le impostazioni di conservazione per ogni versione dell'oggetto. Le

impostazioni di conservazione a livello di oggetto possono essere specificate usando l'applicazione client S3 o l'S3 REST API.

- Le impostazioni di conservazione si applicano alle singole versioni degli oggetti. Una versione di un oggetto può avere sia una data di conservazione che un'impostazione di legal hold, una sola delle due oppure nessuna delle due. Specificare una data di conservazione o un'impostazione di legal hold per un oggetto protegge solo la versione specificata nella richiesta. Puoi creare nuove versioni dell'oggetto, mentre la versione precedente dell'oggetto rimane bloccata.

#### Ciclo di vita degli oggetti nei bucket con S3 Object Lock abilitato

Ogni oggetto salvato in un bucket con S3 Object Lock abilitato attraversa queste fasi:

1. **Ingestione oggetto**

   Quando una versione di un oggetto viene aggiunta a un bucket che ha S3 Object Lock abilitato, le impostazioni di conservazione vengono applicate come segue:

   - Se per l'oggetto sono specificate delle impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Le impostazioni predefinite del bucket vengono ignorate.
   - Se non vengono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se esistono.
   - Se non vengono 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, sia l'oggetto che tutti i metadati S3 definiti dall'utente sono protetti.

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 di copie degli oggetti e le posizioni di archiviazione sono determinati dalle regole conformi nelle policy ILM attive. Se un oggetto protetto può essere eliminato prima che venga raggiunta la sua retain-until-date dipende dalla sua modalità di conservazione.

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

#### Posso ancora gestire i bucket Compliant precedenti?

La funzionalità S3 Object Lock sostituisce la funzionalità Compliance che era disponibile nelle versioni precedenti di StorageGRID. Se hai creato bucket conformi utilizzando una versione precedente di StorageGRID, puoi continuare a gestire le impostazioni di questi bucket; tuttavia, non puoi più creare nuovi bucket conformi. Per le istruzioni, consulta "NetApp Knowledge Base: Come gestire i bucket Compliant legacy in StorageGRID 11.5".

## Aggiorna la conservazione predefinita di S3 Object Lock in StorageGRID

Se hai abilitato S3 Object Lock durante la creazione del bucket, puoi modificare il bucket per cambiare le impostazioni di conservazione predefinite. Puoi abilitare (o disabilitare) la conservazione predefinita e impostare una modalità di conservazione e un periodo di conservazione.

#### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha le "Gestisci tutti i bucket o autorizzazione di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o di bucket.
- Il blocco degli oggetti S3 è abilitato a livello globale per il tuo sistema StorageGRID e hai abilitato il blocco degli oggetti S3 quando hai creato il bucket. Vedi "Usa S3 Object Lock per conservare gli oggetti".

**Passaggi**

1. ${post_edited_translations.segment}
2. Seleziona il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona l'accordion **Blocco oggetto S3**.
4. Facoltativamente, puoi abilitare o disabilitare la **conservazione predefinita** per questo bucket.

   Le modifiche a questa impostazione non si applicano agli oggetti già presenti nel bucket né agli oggetti che potrebbero avere il proprio periodo di conservazione.

5. ${post_edited_translations.segment}

| Modalità di conservazione predefinita | Descrizione |
|---|---|
| Governance | • Gli utenti con l' `s3:BypassGovernanceRetention`autorizzazione possono usare l' `x-amz-bypass-governance-retention: true`intestazione della richiesta per bypassare le impostazioni di conservazione.<br>• Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione prevista.<br>• Questi utenti possono aumentare, diminuire o rimuovere la retain-until-date di un oggetto. |
| Conformità | • L'oggetto non può essere eliminato fino al raggiungimento della sua retain-until-date.<br>• La data di conservazione dell'oggetto può essere aumentata, ma non può essere diminuita.<br>• La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.<br>**Nota**: L'amministratore della grid deve consentirti di utilizzare la modalità di conformità. |

6. Se l'opzione **Conservazione predefinita** è abilitata, specifica il **periodo di conservazione predefinito** per il bucket.

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

Un *periodo di conservazione massimo*, che può variare da 1 giorno a 100 anni, viene impostato quando l'amministratore della griglia crea il tenant. Quando imposti un *periodo di conservazione predefinito*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedi all'amministratore della griglia di aumentare o diminuire il periodo di conservazione massimo.

7. Seleziona **Salva modifiche**.

## Configura CORS per i bucket S3 in StorageGRID

Puoi configurare la condivisione delle risorse tra origini diverse (CORS) per un bucket S3 se vuoi che quel bucket e gli oggetti in esso siano accessibili alle applicazioni web di altri domini.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Per le richieste di configurazione GET CORS, appartieni a un gruppo di utenti che dispone delle autorizzazioni "Autorizzazione Gestisci tutti i bucket o Visualizza tutti i bucket". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o di bucket.
- Per le richieste di configurazione PUT CORS, appartieni a un gruppo di utenti che dispone dell'autorizzazione "Gestisci l'autorizzazione per tutti i bucket". Questa autorizzazione sovrascrive le impostazioni di autorizzazione definite nei criteri di gruppo o di bucket.
- Il "Permesso di accesso root" fornisce accesso a tutte le richieste di configurazione CORS.

### Informazioni su questa attività

La condivisione di risorse tra origini diverse (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, supponi di utilizzare un bucket S3 denominato `Images` per archiviare immagini. Configurando CORS per il bucket `Images`, puoi consentire la visualizzazione delle immagini contenute in quel bucket sul sito web `http://www.example.com`.

### Abilita CORS per un bucket

### Passaggi

1. Utilizza un editor di testo per creare il file XML necessario. Questo esempio mostra l'XML utilizzato per abilitare CORS per un bucket S3. Nello specifico:
    - Consente a qualsiasi dominio di inviare richieste GET al bucket
    - Consente solo al `http://www.example.com`dominio di inviare richieste GET, POST e DELETE
    - Sono consentite tutte le intestazioni di richiesta

```
<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 sulla configurazione XML CORS, vedi "Amazon Web Services (AWS) Documentazione: Guida utente di Amazon Simple Storage Service".

2. Seleziona **Visualizza bucket** dalla dashboard oppure seleziona **STORAGE (S3)** > **Buckets**.
3. Seleziona il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Dalla scheda **Accesso al bucket**, seleziona la sezione **Condivisione delle risorse tra origini diverse (CORS)**.
5. Seleziona la casella di controllo **Abilita CORS**.
6. Incolla la configurazione XML CORS nella casella di testo.
7. Seleziona **Salva modifiche**.

### Modifica l'impostazione CORS

#### Passaggi

1. Aggiorna il file XML di configurazione CORS nella casella di testo oppure seleziona **Clear** per ricominciare.
2. Seleziona **Salva modifiche**.

### Disabilita l'impostazione CORS

#### Passaggi

1. Deseleziona la casella di controllo **Abilita CORS**.
2. Seleziona **Salva modifiche**.

#### Informazioni correlate

"Configura StorageGRID CORS per un'interfaccia di gestione"

# Eliminare oggetti da un bucket S3 di StorageGRID

${post_edited_translations.segment}

### Considerazioni e requisiti

Prima di eseguire questi passaggi, tieni presente quanto segue:

- Quando elimini gli oggetti in un bucket, StorageGRID rimuove in modo permanente tutti gli oggetti e tutte le versioni degli oggetti in ciascun bucket selezionato da tutti i nodi e siti del tuo sistema StorageGRID. StorageGRID rimuove anche tutti i metadati degli oggetti correlati. Non potrai recuperare queste informazioni.
- ${post_edited_translations.segment}
- Se un bucket ha "Blocco oggetto S3 abilitato", potrebbe rimanere nello stato **Eliminazione oggetti: sola lettura** per *anni*.

> Un bucket che utilizza S3 Object Lock rimarrà nello stato **Eliminazione oggetti: sola lettura** fino al raggiungimento della data di conservazione per tutti gli oggetti e alla rimozione di eventuali blocchi legali.

- Durante l'eliminazione degli oggetti, lo stato del bucket è **Eliminazione oggetti: sola lettura**. In questo stato, non puoi aggiungere nuovi oggetti al bucket.
- Una volta eliminati tutti gli oggetti, il bucket rimane in stato di sola lettura. Puoi fare una delle seguenti cose:
  - Riporta il bucket in modalità di scrittura e riutilizzalo per nuovi oggetti
  - Elimina il bucket
  - ${post_edited_translations.segment}
- Se per un bucket è abilitato il versioning degli oggetti, i delete marker creati in StorageGRID 11.8 o versioni successive possono essere rimossi utilizzando le operazioni Delete objects in bucket.
- Se per un bucket è abilitato il versioning degli oggetti, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11.7 o versioni precedenti. Consulta le informazioni sull'eliminazione degli oggetti in un bucket in "Come vengono eliminati gli oggetti versionati di S3".
- Se utilizzi "replicazione cross-grid", tieni presente quanto segue:
  - ${post_edited_translations.segment}
  - Se selezioni questa opzione per il bucket di origine, verrà attivato l'avviso **Errore di replica tra griglie** se aggiungi oggetti al bucket di destinazione sull'altra griglia. Se non puoi garantire che nessuno aggiunga oggetti al bucket sull'altra griglia, "${post_edited_translations.segment}" per quel bucket prima di eliminare tutti gli oggetti del bucket.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha l'autorizzazione "Permesso di accesso root". Questa autorizzazione sovrascrive le impostazioni delle autorizzazioni definite nelle policy di gruppo o di bucket.

### Passaggi

1. ${post_edited_translations.segment}

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

2. ${post_edited_translations.segment}

**Menu azioni**

a. Seleziona la casella di controllo per ogni bucket da cui desideri eliminare gli oggetti.

b. Seleziona **Azioni** > **Elimina oggetti nel bucket**.

**Pagina dei dettagli**

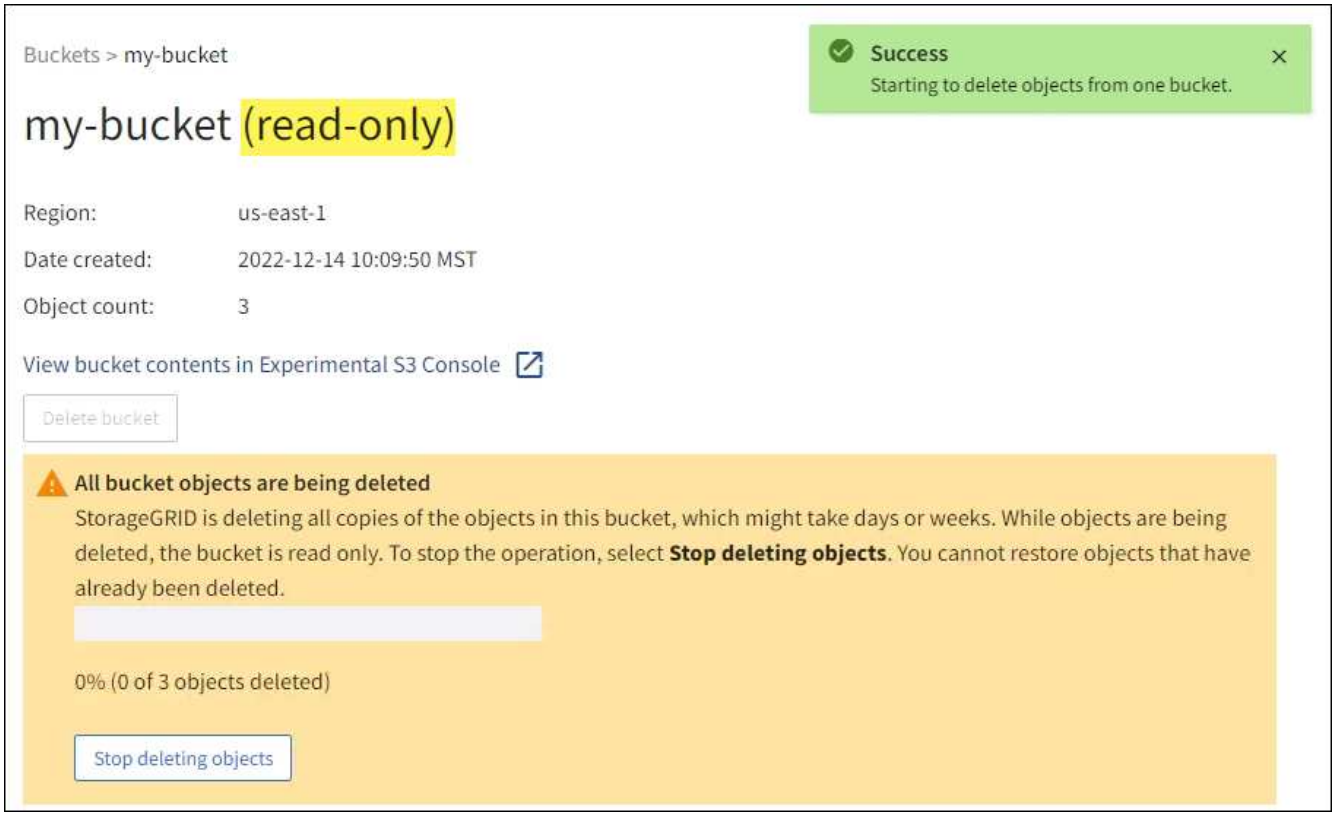
a. Seleziona il nome di un bucket per visualizzarne i dettagli.

b. Seleziona **Elimina oggetti nel bucket**.

3. Quando viene visualizzata la finestra di dialogo di conferma, rivedi i dettagli, inserisci **Yes** e seleziona **OK**.
4. Attendi l'avvio dell'operazione di eliminazione.

   Dopo qualche minuto:

   - Nella pagina dei dettagli del bucket viene visualizzato un banner di stato giallo. La barra di avanzamento indica quale % di oggetti è stata eliminata.
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

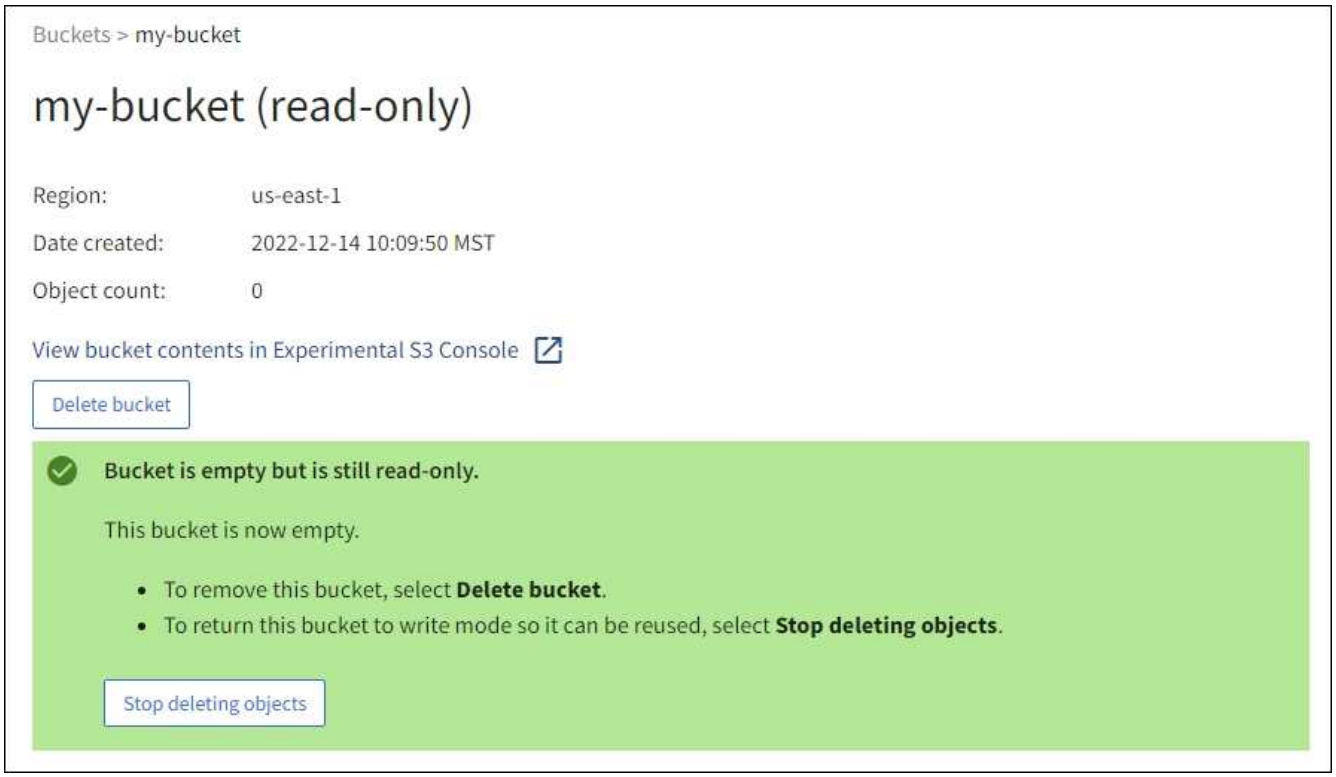



5. Se necessario, durante l'esecuzione dell'operazione, seleziona **Interrompi eliminazione oggetti** per arrestare il processo. Quindi, facoltativamente, seleziona **Elimina oggetti nel bucket** per riprendere il processo.

   ${post_edited_translations.segment}

6. Attendi il completamento dell'operazione.

   ${post_edited_translations.segment}




7. Esegui una delle seguenti operazioni:
   - Esci dalla pagina per mantenere il bucket in modalità di sola lettura. Ad esempio, potresti mantenere un bucket vuoto in modalità di sola lettura per riservare il nome per usi futuri.
   - Elimina il bucket. Puoi selezionare **Elimina bucket** per eliminare un singolo bucket o tornare alla pagina Bucket e selezionare **Azioni** > **Elimina** bucket per rimuovere più di un bucket.

     > Se non riesci a eliminare un bucket con controllo delle versioni dopo che tutti gli oggetti sono stati eliminati, potrebbero essere rimasti dei marker di eliminazione. Per eliminare il bucket, devi rimuovere tutti i marker di eliminazione rimanenti.

   - Riporta il bucket in modalità di scrittura e, facoltativamente, riutilizzalo per nuovi oggetti. Puoi selezionare **Interrompi l'eliminazione degli oggetti** per un singolo bucket oppure tornare alla pagina Buckets e selezionare **Azione** > **Interrompi l'eliminazione degli oggetti** per più di un bucket.

## Eliminare un bucket S3 di StorageGRID

${post_edited_translations.segment}

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Appartieni a un gruppo di utenti che ha le "Gestisci tutti i bucket o autorizzazione di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o di bucket.
- I bucket che vuoi eliminare sono vuoti. Se i bucket che vuoi eliminare *non* sono vuoti, "eliminare oggetti dal bucket".

**Informazioni su questa attività**

Queste istruzioni descrivono come eliminare un bucket S3 utilizzando il Tenant Manager. Puoi anche eliminare i bucket S3 utilizzando il "API di gestione tenant" o il "${post_edited_translations.segment}".

Non puoi eliminare un bucket S3 se contiene oggetti, versioni di oggetti non correnti o marcatori di eliminazione. Per informazioni su come vengono eliminati gli oggetti S3 con versione, consulta "Come vengono eliminati gli oggetti".

**Passaggi**

1. ${post_edited_translations.segment}

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

2. ${post_edited_translations.segment}

   **Menu azioni**

   a. ${post_edited_translations.segment}

   b. ${post_edited_translations.segment}

   **Pagina dei dettagli**

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

   b. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

   StorageGRID verifica che ogni bucket sia vuoto e quindi elimina ogni bucket. Questa operazione potrebbe richiedere alcuni minuti.

   Se un bucket non è vuoto, viene visualizzato un messaggio di errore. Devi "elimina tutti gli oggetti e tutti i marcatori di eliminazione nel bucket" prima di poter eliminare il bucket.

## Usa la console S3 in StorageGRID

Puoi usare la console S3 per visualizzare e gestire gli oggetti in un bucket S3.

S3 Console ti permette di:

- Caricare, scaricare, rinominare, copiare, spostare ed eliminare oggetti
- Visualizza, ripristina, scarica ed elimina le versioni degli oggetti
- Cerca oggetti tramite prefisso
- Gestisci i tag degli oggetti
- Visualizza metadati oggetto
- Visualizza, crea, rinomina, copia, sposta ed elimina cartelle

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

Se usi S3 Console e le operazioni richiedono troppo tempo (ad esempio minuti o ore), considera:

- Ridurre il numero di oggetti selezionati
- Utilizzo di metodi non grafici (API o CLI) per accedere ai tuoi dati

**Prima di iniziare**

- Hai effettuato l'accesso al Tenant Manager utilizzando un "browser web supportato".
- Se vuoi gestire gli oggetti, devi appartenere a un gruppo di utenti con l'autorizzazione di accesso Root. In alternativa, appartieni a un gruppo di utenti con l'autorizzazione "Usa la scheda Console S3" e l'autorizzazione "Visualizza tutti i bucket" oppure "Gestisci tutti i bucket". Vedi "Autorizzazioni per la gestione dei tenant".
- È stata configurata una policy S3 Group o Bucket per l'utente. Vedi "Usa le policy di accesso per bucket e gruppi".
- Conosci l'ID della chiave di accesso dell'utente e la chiave di accesso segreta. Facoltativamente, hai un `.csv` file contenente queste informazioni. Vedi il "istruzioni per la creazione di chiavi di accesso".

**Passaggi**

1. Seleziona **Storage** > **Buckets** > ***bucket name***.
2. Seleziona la scheda Console S3.
3. Incolla l'ID della chiave di accesso e la chiave di accesso segreta nei campi. Altrimenti, seleziona **Carica chiavi di accesso** e seleziona il tuo `.csv` file.
4. Seleziona **Accedi**.
5. Viene visualizzata la tabella degli oggetti bucket. Puoi gestire gli oggetti come preferisci.

**Informazioni aggiuntive**

- **Ricerca per prefisso**: La funzione di ricerca per prefisso cerca solo 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 per `folder1/folder2/somefile-` restituirebbe oggetti che si trovano all'interno della `folder1/folder2/` cartella e che iniziano con la parola `somefile-`.
- **Trascina e rilascia**: Puoi trascinare e rilasciare i file dal gestore file del tuo computer alla S3 Console. Tuttavia, non puoi caricare cartelle.
- **Operazioni sulle cartelle**: Quando sposti, copi o rinomini una cartella, tutti gli oggetti al suo interno vengono aggiornati uno alla volta, il che potrebbe richiedere tempo.
- **Cancellazione permanente quando il versioning del bucket è disabilitato**: Quando sovrascrivi o elimini un oggetto in un bucket con il versioning disabilitato, l'operazione è permanente. Vedi "Modifica la gestione delle versioni degli oggetti per un bucket".

# Gestisci i servizi della piattaforma S3

# servizi della piattaforma S3

## Scopri i servizi della piattaforma per StorageGRID

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

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

### Panoramica dei servizi della piattaforma

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

Poiché la posizione di destinazione per i servizi della piattaforma è in genere esterna alla tua distribuzione StorageGRID, i servizi della piattaforma ti offrono la potenza e la flessibilità derivanti dall'utilizzo di risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi per i tuoi dati.

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

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

### ${post_edited_translations.segment}

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

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

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

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

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

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

**${post_edited_translations.segment}**

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

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

#### Considerazioni sull'utilizzo del servizio di replica CloudMirror

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

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

**Scopri il servizio di replica CloudMirror di StorageGRID**

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

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

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

**CloudMirror e ILM**

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

#### CloudMirror e replicazione cross-grid

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

#### CloudMirror e bucket S3

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

**bucket esistenti**

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

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

**Bucket di destinazione multipli**

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

**Bucket con versione o senza versione**

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

#### ${post_edited_translations.segment}

**Comportamento di eliminazione**

È uguale al comportamento di eliminazione del servizio Amazon S3, Cross-Region Replication (CRR). L'eliminazione di un oggetto in un bucket di origine non elimina mai un oggetto replicato nella destinazione. Se sia il bucket di origine che quello di destinazione sono dotati di controllo delle versioni, il marcatore di eliminazione viene replicato. Se il bucket di destinazione non è dotato di controllo delle versioni, l'eliminazione di un oggetto nel bucket di origine non replica il marcatore di eliminazione nel bucket di destinazione né elimina l'oggetto di destinazione.

**${post_edited_translations.segment}**

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

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

**${post_edited_translations.segment}**

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

### Scopri le notifiche degli eventi di StorageGRID per i bucket S3

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

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

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

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

${post_edited_translations.segment}

- Sono supportati i seguenti tipi di evento:
  - s3:ObjectCreated:
  - s3:ObjectCreated:Put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copy
  - s3:ObjectCreated:CompleteMultipartUpload
  - s3:ObjectRemoved:
  - s3:ObjectRemoved:Delete
  - s3:ObjectRemoved:DeleteMarkerCreated
  - s3:ObjectRestore:Post
- ${post_edited_translations.segment}

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

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

### Scopri il servizio di integrazione della ricerca StorageGRID

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

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

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

${post_edited_translations.segment}

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

#### Integrazione della ricerca e bucket S3

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

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

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

#### ${post_edited_translations.segment}

${post_edited_translations.segment}

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

policy ILM della griglia.

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

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

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

#### ${post_edited_translations.segment}

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

## Gestisci gli endpoint dei servizi della piattaforma

### Configura gli endpoint dei servizi della piattaforma in StorageGRID

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

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

#### Che cos'è un endpoint dei servizi di piattaforma?

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

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

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

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

secondo topic di Amazon SNS.

#### Endpoint per la replica CloudMirror

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

#### Endpoint per le notifiche

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

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

#### Endpoint per il servizio di integrazione della ricerca

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

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

**Informazioni correlate**

"${post_edited_translations.segment}"

### Specificare un URN per un endpoint dei servizi della piattaforma StorageGRID

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

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

#### Elementi URN

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

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

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

${post_edited_translations.segment}

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

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

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

${post_edited_translations.segment}

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

#### ${post_edited_translations.segment}

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

- Replicazione CloudMirror:

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

- Notifiche:

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

- Integrazione della ricerca:

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

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

**${post_edited_translations.segment}**

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

- Replicazione CloudMirror:

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

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

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

- Notifiche:

  ${post_edited_translations.segment}

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

  Specifica un endpoint Kafka:

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

  Specifica un endpoint webhook:

```
urn:mysite:webhook:optional:optional:webhook-name
```

- Integrazione della ricerca:

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

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

### Creare un endpoint dei servizi della piattaforma StorageGRID

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

**Prima di iniziare**

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

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

  - Nome univoco della risorsa (URN)

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

  - Credenziali di autenticazione (se richieste):

**Endpoint di integrazione della ricerca**

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

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

**endpoint di replica CloudMirror**

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

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

**Endpoint Amazon SNS**

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

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

**Endpoint Kafka**

Per gli endpoint Kafka, puoi utilizzare le seguenti credenziali:

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

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

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

**Passaggi**

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

   Il tipo di servizio della piattaforma supportato dall'endpoint viene visualizzato accanto al nome dell'endpoint quando questo è elencato nella pagina Endpoints, quindi non devi includere questa informazione nel nome.

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

   Usa uno dei seguenti formati:

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

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

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

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

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

In questo esempio, `s3.example.com` rappresenta la voce DNS per il VIP (virtual IP) del gruppo HA (alta disponibilità) di StorageGRID, e `10443` rappresenta la porta definita nell'endpoint del load balancer.

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

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

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

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

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

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

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

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

**Endpoint di integrazione della ricerca**

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

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

| Tipo di autenticazione | Descrizione | Credenziali |
|---|---|---|
| Anonimo | Consente accesso anonimo alla destinazione. Funziona solo per gli endpoint con la sicurezza disabilitata. | Nessuna autenticazione. |
| Chiave di accesso | Utilizza credenziali in stile AWS per autenticare le connessioni con la destinazione. | • ID chiave di accesso<br>• Chiave di accesso segreta |
| HTTP di base | Utilizza un nome utente e una password per autenticare le connessioni alla destinazione. | • Nome utente<br>• Password |

**endpoint di replica CloudMirror**

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

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

| Tipo di autenticazione | Descrizione | Credenziali |
|---|---|---|
| Anonimo | Consente accesso anonimo alla destinazione. Funziona solo per gli endpoint con la sicurezza disabilitata. | Nessuna autenticazione. |
| Chiave di accesso | Utilizza credenziali in stile AWS per autenticare le connessioni con la destinazione. | • ID chiave di accesso<br>• Chiave di accesso segreta |
| CAP (C2S Access Portal) | Utilizza certificati e chiavi per autenticare le connessioni alla destinazione. | • URL delle credenziali temporanee<br>• Certificato CA del server (caricamento file PEM)<br>• Certificato client (caricamento file PEM)<br>• Chiave privata del client (caricamento file PEM, formato crittografato OpenSSL o formato chiave privata non crittografata)<br>• Frase di accesso della chiave privata del client (facoltativa) |

**Endpoint Amazon SNS**

Inserisci o carica le credenziali per un endpoint Amazon SNS.

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

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

**Endpoint Kafka**

Inserisci o carica le credenziali per un endpoint Kafka.

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

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

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

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

**La maggior parte degli endpoint**

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

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

**Solo endpoint Webhook**

Verifica la connessione TLS per gli endpoint webhook.

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

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

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

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

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

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

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

**Informazioni correlate**

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

### Verifica la connessione per un endpoint dei servizi della piattaforma StorageGRID

## ${post_edited_translations.segment}

**Prima di iniziare**

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

**Informazioni su questa attività**

${post_edited_translations.segment}

**Passaggi**

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

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}

   Viene visualizzata la pagina dei dettagli dell'endpoint.

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

### Modifica un endpoint dei servizi della piattaforma in StorageGRID

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

#### Prima di iniziare

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

#### Passaggi

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

   ${post_edited_translations.segment}

2. Seleziona l'endpoint che desideri modificare.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

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

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

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

        ${post_edited_translations.segment}

   d. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
    - Se l'endpoint è raggiungibile utilizzando le credenziali specificate, viene visualizzato un messaggio di successo. La connessione all'endpoint viene verificata da un nodo in ciascun sito.

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

### Eliminare un endpoint dei servizi della piattaforma StorageGRID

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

#### Prima di iniziare

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

#### Passaggi

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

   ${post_edited_translations.segment}

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

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

3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

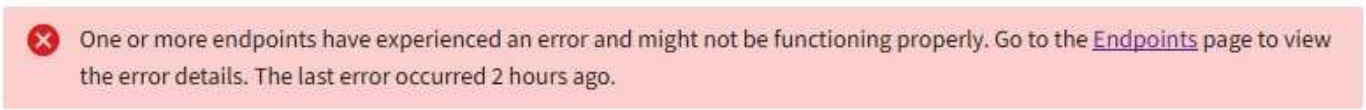
4. ${post_edited_translations.segment}

### Risoluzione dei problemi relativi agli endpoint dei servizi della piattaforma StorageGRID

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

#### ${post_edited_translations.segment}

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




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

**Passaggi**

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

#### ${post_edited_translations.segment}

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

**Passaggi**

1. ${post_edited_translations.segment}

   Viene visualizzata la pagina dei dettagli dell'endpoint.

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

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

#### Risolvere gli errori degli endpoint

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

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

**Passaggi**

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

#### ${post_edited_translations.segment}

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

**Informazioni correlate**

- "${post_edited_translations.segment}"

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

## Configura la replica CloudMirror in StorageGRID

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

**Prima di iniziare**

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

**Informazioni su questa attività**

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

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

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

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

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

**Passaggi**

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

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

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

2. ${post_edited_translations.segment}
3. Seleziona il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

7. Verifica che la replica sia configurata correttamente:
   a. Aggiungi un oggetto al bucket di origine che soddisfi i requisiti per la replica come specificato nella

configurazione di replica.

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

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

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

**Informazioni correlate**

"Crea un endpoint per i servizi della piattaforma"

## Configura le notifiche degli eventi in StorageGRID

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

**Prima di iniziare**

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

**Informazioni su questa attività**

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

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

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

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

**Passaggi**

1. Abilita le notifiche per il tuo bucket di origine:
   - Utilizza un editor di testo per creare il file XML di configurazione delle notifiche necessario per abilitare le notifiche degli eventi, come specificato nell'API di notifica S3.
   - Durante la configurazione del file XML, usa l'URN di un endpoint di notifiche eventi come topic di destinazione.

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

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

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

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

   b. Conferma che una notifica sia stata recapitata all'argomento Amazon SNS di destinazione, all'argomento Kafka di destinazione o all'endpoint webhook di destinazione.

      Ad esempio, se il tuo topic di destinazione è ospitato su Amazon SNS, puoi configurare il servizio per

ricevere un'email quando la notifica viene recapitata.

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

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

**Informazioni correlate**

- "Comprendi le notifiche per i bucket"
- "${post_edited_translations.segment}"

- "Crea un endpoint per i servizi della piattaforma"

## Configura il servizio di integrazione della ricerca in StorageGRID

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

**Prima di iniziare**

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

**Informazioni su questa attività**

Dopo che hai configurato il servizio di integrazione della ricerca per un bucket di origine, la creazione di un oggetto o l'aggiornamento dei metadati o dei tag di un oggetto fa sì che i metadati dell'oggetto vengano inviati all'endpoint di destinazione.

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

**Passaggi**

1. Abilita l'integrazione della ricerca per un bucket:
    - Utilizza un editor di testo per creare il file XML di notifica dei metadati necessario per abilitare l'integrazione con la ricerca.
    - Durante la configurazione dell'XML, usa l'URN di un endpoint di integrazione della ricerca come destinazione.

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

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

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

Elementi nel file XML di configurazione della notifica dei metadati:

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

| Nome | Descrizione | Richiesto |
| --- | --- | --- |
| Urn | URN della destinazione a cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà:<br>• `es`deve essere il terzo elemento.<br>• L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel formato `domain-name/myindex/mytype`.<br>Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma:<br>• `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br>L'endpoint deve essere configurato prima dell'invio del file XML di configurazione, altrimenti la configurazione fallirà con un errore 404.<br>L'URN è incluso nell'elemento Destinazione. | Sì |

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

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

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

**Dopo aver finito**

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

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

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

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

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

**Esempio: configurazione della notifica dei metadati con due regole**

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

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

### Formato di notifica dei metadati

Quando abiliti il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato alla destinazione ogni volta che i metadati o i tag di un oggetto vengono aggiunti, aggiornati o eliminati.

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

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

#### Campi inclusi nel documento JSON

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

**Informazioni su bucket e oggetto**

`bucket`: Nome del bucket

`key`: Nome della chiave dell'oggetto

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

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

**Metadati di sistema**

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

`md5`: Hash dell'oggetto

**Metadati utente**

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

`key:value`

### Etichette

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

```
key:value
```

#### Come visualizzare i risultati in Elasticsearch

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

## Informazioni sul copyright



## Informazioni sul marchio commerciale