



## **Utilizzare un account tenant**

StorageGRID software

NetApp

December 03, 2025

# Sommario

Utilizzare un account tenant .....	1
Utilizzare un account tenant .....	1
Che cos'è un conto inquilino .....	1
Come creare un account tenant .....	1
Come accedere e uscire .....	2
Sign in a Tenant Manager .....	2
Esci da Tenant Manager .....	6
Comprendere la dashboard di Tenant Manager .....	7
Informazioni sull'account dell'inquilino .....	8
Utilizzo di spazio di archiviazione e quote .....	8
Avvisi sull'utilizzo delle quote .....	9
Limite di utilizzo della capacità .....	10
Errori di endpoint .....	10
API di gestione degli inquilini .....	10
Comprendere l'API di gestione degli inquilini .....	10
Versionamento dell'API di gestione degli inquilini .....	13
Protezione contro la falsificazione delle richieste tra siti (CSRF) .....	14
Utilizzare connessioni di federazione di rete .....	15
Clona gruppi tenant e utenti .....	15
Clona le chiavi di accesso S3 utilizzando l'API .....	20
Gestire la replicazione tra griglie .....	22
Visualizza le connessioni della federazione di griglia .....	27
Gestisci gruppi e utenti .....	28
Utilizzare la federazione delle identità .....	28
Gestire gruppi di tenant .....	34
Gestisci gli utenti locali .....	44
Gestisci le chiavi di accesso S3 .....	48
Gestisci le chiavi di accesso S3 .....	48
Crea le tue chiavi di accesso S3 .....	48
Visualizza le tue chiavi di accesso S3 .....	50
Elimina le tue chiavi di accesso S3 .....	50
Crea le chiavi di accesso S3 di un altro utente .....	51
Visualizza le chiavi di accesso S3 di un altro utente .....	52
Elimina le chiavi di accesso S3 di un altro utente .....	53
Gestisci i bucket S3 .....	53
Crea un bucket S3 .....	54
Visualizza i dettagli del bucket .....	57
Applicare un tag di policy ILM a un bucket .....	59
Gestisci i criteri del bucket .....	60
Gestire la coerenza del bucket .....	60
Abilita o disabilita gli aggiornamenti dell'ultimo orario di accesso .....	62
Modificare il controllo delle versioni degli oggetti per un bucket .....	64
Utilizzare S3 Object Lock per conservare gli oggetti .....	65

Aggiorna la conservazione predefinita del blocco degli oggetti S3 . . . . .	69
Configurare la condivisione delle risorse tra origini (CORS) . . . . .	70
Elimina gli oggetti nel bucket . . . . .	72
Elimina bucket S3 . . . . .	75
Utilizzare la console S3 . . . . .	76
Gestire i servizi della piattaforma S3 . . . . .	77
Servizi della piattaforma S3 . . . . .	78
Gestire gli endpoint dei servizi della piattaforma . . . . .	85
Configurare la replica di CloudMirror . . . . .	98
Configurare le notifiche degli eventi . . . . .	100
Configurare il servizio di integrazione della ricerca . . . . .	104

# Utilizzare un account tenant

## Utilizzare un account tenant

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

### Che cos'è un conto inquilino?

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

Gli account tenant possono essere utilizzati per separare gli oggetti archiviati da entità diverse. Ad esempio, è possibile utilizzare più account tenant per uno qualsiasi di questi casi d'uso:

- **Caso d'uso aziendale:** se il sistema StorageGRID viene utilizzato all'interno di un'azienda, l'archiviazione degli oggetti della griglia potrebbe essere segregata dai diversi reparti dell'organizzazione. Ad esempio, potrebbero esserci account tenant per il reparto marketing, il reparto assistenza clienti, il reparto risorse umane e così via.



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

- **Caso d'uso del fornitore di servizi:** se il sistema StorageGRID viene utilizzato da un fornitore di servizi, l'archiviazione degli oggetti della griglia potrebbe essere segregata dalle diverse entità che affittano l'archiviazione. Ad esempio, potrebbero esserci conti inquilino per la Società A, la Società B, la Società C e così via.

### Come creare un account tenant

Gli account degli inquilini vengono creati da un "[Amministratore della griglia StorageGRID che utilizza Grid Manager](#)" . Quando si crea un account tenant, l'amministratore della griglia specifica quanto segue:

- Informazioni di base, tra cui il nome del tenant, il tipo di client (S3) e la quota di archiviazione facoltativa.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine identità, utilizzare S3 Select o utilizzare una connessione di federazione di griglia.
- L'accesso root iniziale per il tenant, a seconda 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.

### Configurare i tenant S3

Dopo un "[L'account tenant S3 è stato creato](#)" , puoi accedere al Tenant Manager per eseguire attività come le seguenti:

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

- Gestisci gruppi e utenti
- Utilizzare la federazione di griglia per la clonazione degli account e la replica tra griglie
- Gestisci le chiavi di accesso S3
- Crea e gestisci bucket S3
- Utilizzare i servizi della piattaforma S3
- Utilizzare S3 Select
- Monitorare l'utilizzo dello spazio di archiviazione



Sebbene sia possibile creare e gestire bucket S3 con Tenant Manager, è necessario utilizzare un "[Cliente S3](#)" O "[Consolle S3](#)" per ingerire e gestire oggetti.

## Come accedere e uscire

### Sign in a Tenant Manager

Si accede 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.
- Hai un URL per accedere a Tenant Manager, fornito dall'amministratore della tua griglia. 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 nome di dominio completo (FQDN), l'indirizzo IP di un nodo di amministrazione o l'indirizzo IP virtuale di un gruppo HA di nodi di amministrazione. Potrebbe includere anche un numero di porta, l'ID dell'account tenant a 20 cifre o entrambi.

- Se l'URL non include l'ID account di 20 cifre del tenant, si dispone di questo ID account.
- Stai utilizzando un "[browser web supportato](#)" .
- I cookie sono abilitati nel tuo browser web.
- Appartieni a un gruppo di utenti che ha "[autorizzazioni di accesso specifiche](#)" .

#### Passi

1. Lanciare un "[browser web supportato](#)" .
2. Nella barra degli indirizzi del browser, inserisci l'URL per accedere a Tenant Manager.
3. Se viene visualizzato un avviso di sicurezza, installare il certificato utilizzando la procedura guidata di installazione del browser.

#### 4. Sign in a Tenant Manager.

La schermata di accesso visualizzata dipende dall'URL immesso e dal fatto che sia stato configurato l'accesso singolo (SSO) per StorageGRID.

## Non si utilizza SSO

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

- La pagina di accesso di Grid Manager. Selezionare il link **Accesso tenant**.



The screenshot shows the login interface for the NetApp StorageGRID Grid Manager. At the top, the NetApp StorageGRID logo is displayed. Below it, the title "Grid Manager" is centered. The interface includes two input fields: "Username" and "Password", each with a placeholder character ("|"). A blue "Sign in" button is positioned below the password field. At the bottom, there are three links: "Tenant sign in" (which is highlighted with a green rectangular border), "NetApp support", and "NetApp.com".

- La pagina di accesso del Tenant Manager. Il campo **Account** potrebbe essere già compilato, come mostrato di seguito.



# Tenant Manager

## Recent

## Account

## Username

## Password

**Sign in**

[NetApp support](#) | [NetApp.com](#)

- i. Se l'ID account di 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account del tenant se appare nell'elenco degli account recenti oppure immettere l'ID account.
- ii. Inserisci il tuo nome utente e la tua password.
- iii. Seleziona \* Sign in\*.

Viene visualizzata la dashboard del Tenant Manager.

- iv. Se hai ricevuto una password iniziale da qualcun altro, seleziona **username > Cambia password** per proteggere il tuo account.

## Utilizzo di SSO

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

- La pagina SSO della tua organizzazione. Per esempio:

Sign in with your organizational account

**Sign in**

Inserisci le tue credenziali SSO standard e seleziona \* Sign in\*.

- Pagina di accesso SSO del Tenant Manager.

**NetApp StorageGRID®**

# Tenant Manager

**Recent**

**Account**

**Sign in**

[NetApp support | NetApp.com](#)

- i. Se l'ID account di 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account del tenant se appare nell'elenco degli account recenti oppure immettere l'ID account.
- ii. Seleziona \* Sign in\*.
- iii. Sign in con le tue credenziali SSO standard alla pagina di accesso SSO della tua organizzazione.

Viene visualizzata la dashboard del Tenant Manager.

## Esci da Tenant Manager

Una volta terminato di lavorare con Tenant Manager, è necessario disconnettersi per

impedire agli utenti non autorizzati di accedere al sistema StorageGRID. In base alle impostazioni dei cookie del browser, la chiusura del browser potrebbe non comportare la disconnessione dal sistema.

#### Passi

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



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

- Se SSO non è in uso:

Hai effettuato la disconnessione dal nodo di amministrazione. Viene visualizzata la pagina di accesso del 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 l'uscita da tutti i nodi amministrativi a cui stavi accedendo. Viene visualizzata la pagina Sign in a StorageGRID. Il nome dell'account tenant a cui hai appena avuto accesso è elencato come predefinito nel menu a discesa **Account recenti** e viene visualizzato l'**ID account** del tenant.



Se l'SSO è abilitato e hai effettuato l'accesso anche a Grid Manager, devi anche disconnetterti da Grid Manager per uscire dall'SSO.

## Comprendere la dashboard di Tenant Manager

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



I valori dello spazio utilizzato sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo.

Una volta caricati gli oggetti, la dashboard apparirà come nell'esempio seguente:

# Dashboard

**16** Buckets  
[View buckets](#)

**2** Platform services endpoints  
[View endpoints](#)

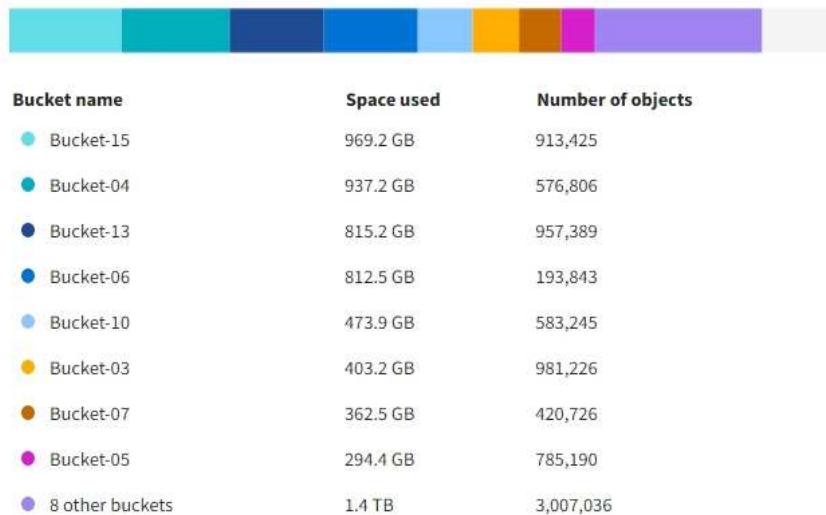
**0** Groups  
[View groups](#)

**1** User  
[View users](#)

## Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



## Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

## Tenant details [?](#)

Name:	Tenant02
ID:	3341 1240 0546 8283 2208
<input checked="" type="checkbox"/> Platform services enabled	
<input checked="" type="checkbox"/> Can use own identity source	
<input checked="" type="checkbox"/> S3 Select enabled	

## Informazioni sull'account dell'inquilino

Nella parte superiore della dashboard viene visualizzato il numero di bucket o contenitori, gruppi e utenti configurati. Visualizza anche il numero di endpoint dei servizi della piattaforma, se ne sono stati configurati. Selezionare i link per visualizzare i dettagli.

A seconda del "permessi di gestione degli inquilini" di cui disponi e le opzioni che hai configurato, il resto della dashboard visualizza varie combinazioni di linee guida, utilizzo dello storage, informazioni sugli oggetti e dettagli sui tenant.

## Utilizzo di spazio di archiviazione e quote

Il pannello Utilizzo dello spazio di archiviazione 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 archiviare copie di tali oggetti e dei relativi metadati.

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



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

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

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



- Per far corrispondere il grafico a barre, un elenco dei bucket o contenitori più grandi, inclusa la quantità totale di dati degli oggetti e il numero di oggetti per ciascun bucket o contenitore.

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 l'inquilino ha più di nove bucket o contenitori, tutti gli altri bucket o contenitori vengono combinati in un'unica voce in fondo all'elenco.



Per modificare le unità per i valori di archiviazione visualizzati in Tenant Manager, selezionare il menu a discesa dell'utente in alto a destra di Tenant Manager, quindi selezionare **Preferenze utente**.

## Avvisi sull'utilizzo delle quote

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

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

Si consiglia di chiedere all'amministratore della rete di aumentare la quota.

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

## Limite di utilizzo della 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 viene impostato alcun limite per un bucket, la sua capacità è illimitata. Tuttavia, se il tuo account tenant ha una quota di archiviazione totale e tale quota viene raggiunta, non potrai acquisire altri oggetti indipendentemente dal limite di capacità rimanente su un bucket.

## Errori di endpoint

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

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

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

## API di gestione degli inquilini

### Comprendere l'API di gestione degli inquilini

È possibile eseguire 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, più rapidamente.

API di gestione degli inquilini:

- Utilizza la piattaforma API open source Swagger. Swagger fornisce un'interfaccia utente intuitiva che consente agli sviluppatori e ai non sviluppatori di interagire con l'API. L'interfaccia utente di Swagger fornisce dettagli e documentazione completi per ogni operazione API.
- Usi "controllo delle versioni per supportare aggiornamenti non distruttivi".

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

1. Sign in a Tenant Manager.
2. Nella parte superiore di Tenant Manager, seleziona l'icona della guida e seleziona **Documentazione API**.

## operazioni API

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

- **account**: Operazioni sull'account del tenant corrente, incluso l'ottenimento di informazioni sull'utilizzo dello spazio di archiviazione.
- **auth**: Operazioni per eseguire l'autenticazione della sessione utente.

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

Per informazioni su come migliorare la sicurezza dell'autenticazione, vedere "["Protezione contro la falsificazione delle richieste tra siti"](#)" .



Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), è necessario eseguire passaggi diversi per l'autenticazione. Vedi il "["Istruzioni per l'utilizzo dell'API di gestione della griglia"](#)" .

- **config**: Operazioni relative alla versione del prodotto e alle versioni dell'API di gestione tenant. È possibile elencare la versione del prodotto e le principali versioni dell'API supportate da tale versione.
- **contenitori**: operazioni su bucket S3 o contenitori Swift.
- **deactivated-features**: 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, le notifiche o l'integrazione della ricerca StorageGRID CloudMirror.
- **grid-federation-connections**: Operazioni sulle connessioni della federazione di griglia e sulla replicazione tra griglie.
- **gruppi**: operazioni per gestire gruppi di tenant locali e per recuperare gruppi di tenant federati da una fonte di identità esterna.
- **identity-source**: Operazioni per configurare una fonte di identità esterna e per sincronizzare manualmente le informazioni sui gruppi federati e sugli utenti.
- **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 gestire le chiavi di accesso S3 per gli utenti 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 tenant.

## Dettagli dell'operazione

Espandendo ogni operazione API, è possibile visualizzare la relativa azione HTTP, l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (quando richiesto) e le possibili risposte.

## groups Operations on groups

GET

/org/groups Lists Tenant User Groups

### Parameters

Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

### Responses

Response content type

application/json

Code	Description
200	

Example Value Model

```
[{"responseTime": "2018-02-01T16:22:31.066Z",  
 "status": "success",  
 "apiVersion": "2.0"}
```

## Inviare richieste API



Tutte le operazioni API eseguite tramite la pagina web Documentazione API sono operazioni live. Fare attenzione a non creare, aggiornare o eliminare per errore dati di configurazione o altri dati.

### Passi

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

4. Seleziona **Provalo**.
5. Fornire tutti i parametri richiesti o modificare il corpo della richiesta come richiesto.
6. Selezionare **Esegui**.
7. Esaminare il codice di risposta per determinare se la richiesta è andata a buon fine.

## Versionamento dell'API di gestione degli inquilini

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

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

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

La versione principale dell'API viene aggiornata quando vengono apportate modifiche che non sono 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 aumentata in base al tipo di modifiche apportate.

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

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



È possibile configurare le versioni supportate. Consultare la sezione **config** della documentazione dell'API Swagger per "[API di gestione della griglia](#)" per maggiori informazioni. Dopo aver aggiornato tutti i client API per utilizzare la versione più recente, è necessario disattivare il supporto per la versione precedente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Obsoleto: vero"
- Il corpo della risposta JSON include "deprecated": true
- Un avviso obsoleto è stato aggiunto a nms.log. Per esempio:

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

## Determina quali versioni API sono supportate nella versione corrente

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

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

## Specificare una versione API per una richiesta

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

```
curl https://[IP-Address]/api/v4/grid/accounts
curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

## Protezione contro la falsificazione delle richieste tra siti (CSRF)

È possibile contribuire a proteggersi dagli attacchi CSRF (Cross-Site Request Forgery) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se abilitarla o meno al momento dell'accesso.

Un aggressore in grado di attivare una richiesta a un sito diverso (ad esempio con un modulo HTTP POST) può far sì che determinate richieste vengano effettuate utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggersi dagli attacchi CSRF utilizzando i token CSRF. Se abilitato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro del corpo POST specifico.

Per abilitare la funzione, impostare csrfToken parametro a `true` durante l'autenticazione. L'impostazione predefinita è `false`.

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

Quando è vero, un `GridCsrfToken` il cookie è impostato con un valore casuale per gli accessi a Grid Manager e `AccountCsrfToken` il cookie viene impostato con un valore casuale per gli accessi al Tenant Manager.

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

- IL `x-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie token CSRF.
- Per gli endpoint che accettano un corpo codificato in formato: A `csrfToken` parametro del corpo della richiesta codificato nel modulo.

Per configurare la protezione CSRF, utilizzare "[API di gestione della griglia](#)" O "[API di gestione degli inquilini](#)".



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

## Utilizzare connessioni di federazione di rete

### Clona gruppi tenant e utenti

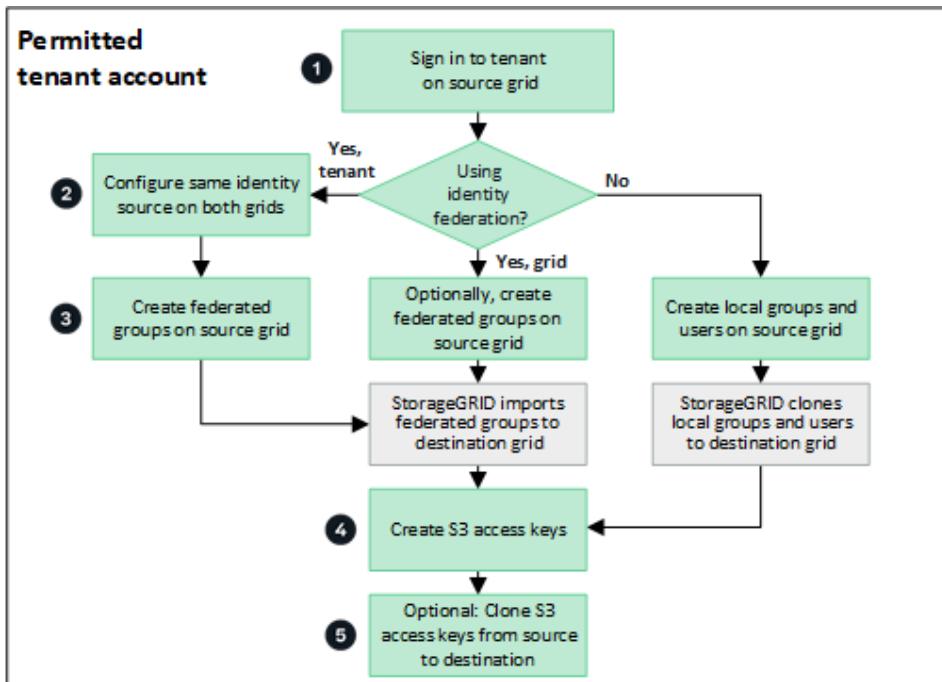
Se un tenant è stato creato o modificato per utilizzare una connessione di federazione della griglia, tale tenant viene replicato da un sistema StorageGRID (il tenant di origine) a un altro sistema StorageGRID (il tenant di replica). Dopo che il tenant è stato replicato, tutti i gruppi e gli utenti aggiunti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

Il sistema StorageGRID in cui il tenant viene creato originariamente è la *griglia sorgente* del tenant. Il sistema StorageGRID in cui viene replicato il tenant è la *griglia di destinazione* del tenant. Entrambi gli account tenant hanno lo stesso ID account, nome, descrizione, quota di archiviazione e autorizzazioni assegnate, ma il tenant di destinazione inizialmente non ha una password utente root. Per i dettagli, vedere "[Che cosa è il clone dell'account](#)" E "[Gestire gli inquilini autorizzati](#)".

La clonazione delle informazioni dell'account dell'inquilino è richiesta per "[replicazione cross-grid](#)" di oggetti secchio. Avere gli stessi gruppi di tenant e utenti su entrambe le griglie garantisce l'accesso ai bucket e agli oggetti corrispondenti su entrambe le griglie.

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

Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, rivedi il diagramma del flusso di lavoro per vedere i passaggi da eseguire per clonare gruppi, utenti e chiavi di accesso S3.



Questi sono i passaggi principali del flusso di lavoro:

1

### Sign in al tenant

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

2

### Facoltativamente, configurare la federazione delle identità

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

3

### Creare gruppi e utenti

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

- Se la federazione delle identità è configurata per l'intero sistema StorageGRID o per il tuo account tenant, ["creare nuovi gruppi di tenant"](#) importando gruppi federati dalla fonte dell'identità.
- Se non si utilizza la federazione delle identità, ["creare nuovi gruppi locali"](#) poi ["creare utenti locali"](#) .

4

### Creare chiavi di accesso S3

Puoi ["creare le tue chiavi di accesso"](#) o a ["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 Tenant Manager per clonarle manualmente sulla griglia di destinazione. Per le istruzioni, vedere "[Clona le chiavi di accesso S3 utilizzando l'API](#)" .

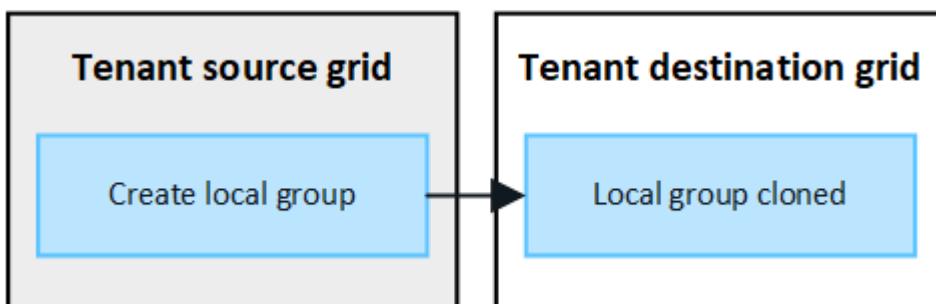
### Come vengono clonati gruppi, utenti e chiavi di accesso S3?

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

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

Dopo che un account tenant è stato creato e replicato nella griglia di destinazione, StorageGRID clona automaticamente tutti i gruppi locali aggiunti 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 la stessa policy di gruppo S3. Per le istruzioni, vedere "[Crea gruppi per il tenant S3](#)" .

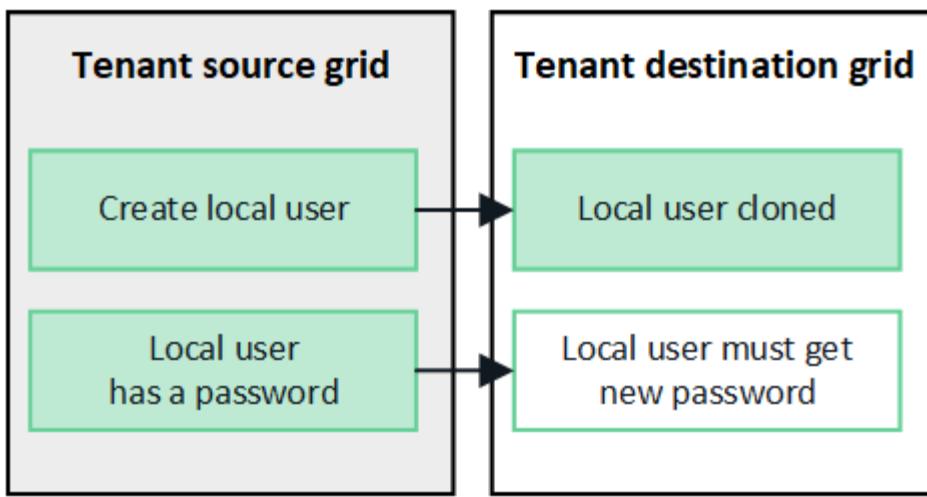


Tutti gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando crei il gruppo. In alternativa, seleziona il gruppo quando crei gli utenti.

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

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

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

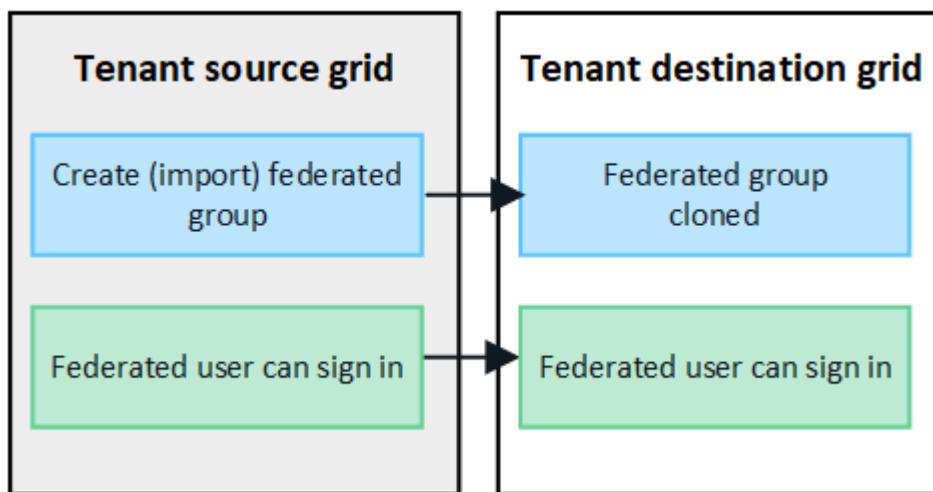


I gruppi federati creati sulla griglia di origine vengono clonati

Supponendo che i requisiti per l'utilizzo del clone dell'account con "[accesso unico](#)" E "[federazione di identità](#)" sono stati soddisfatti, i gruppi federati creati (importati) per il tenant nella griglia di origine vengono automaticamente clonati nel tenant nella griglia di destinazione.

Entrambi i gruppi hanno la stessa modalità di accesso, le stesse autorizzazioni di gruppo e la stessa policy 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.

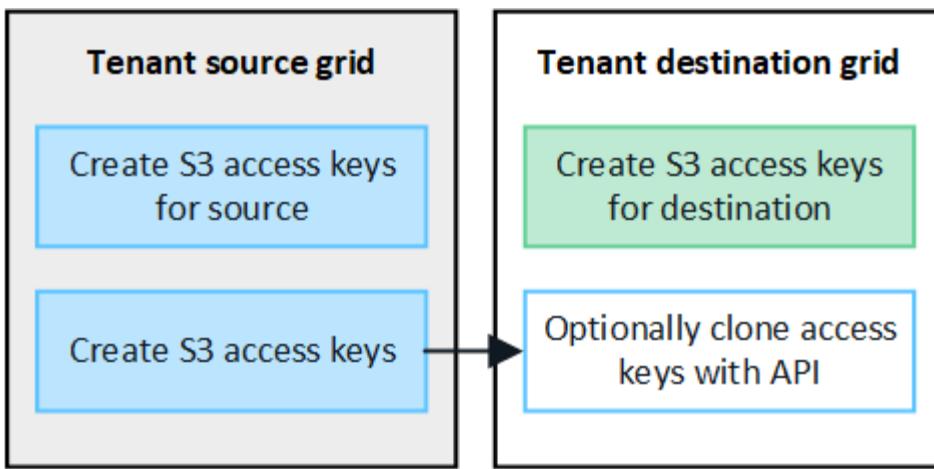


Le chiavi di accesso S3 possono essere clonate manualmente

StorageGRID non clona automaticamente le chiavi di accesso S3 perché la sicurezza è migliorata dalla presenza di chiavi diverse su ogni griglia.

Per gestire le chiavi di accesso sulle due griglie, puoi procedere in uno dei seguenti modi:

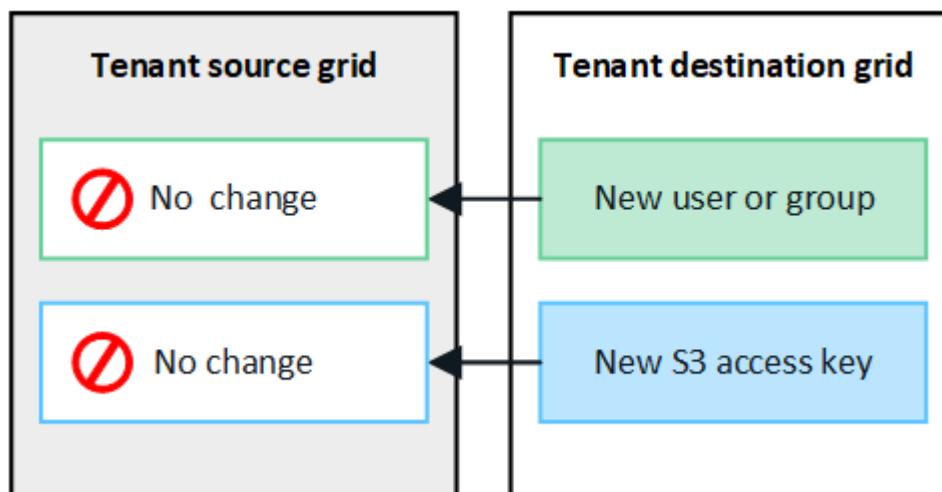
- Se non hai bisogno di usare le stesse chiavi per ogni griglia, puoi "[crea le tue chiavi di accesso](#)" O "[creare le chiavi di accesso di un altro utente](#)" su ogni griglia.
- Se devi utilizzare le stesse chiavi su entrambe le griglie, puoi creare chiavi sulla griglia di origine e quindi utilizzare l'API Tenant Manager per crearle manualmente "[clonare le chiavi](#)" alla griglia di destinazione.



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

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

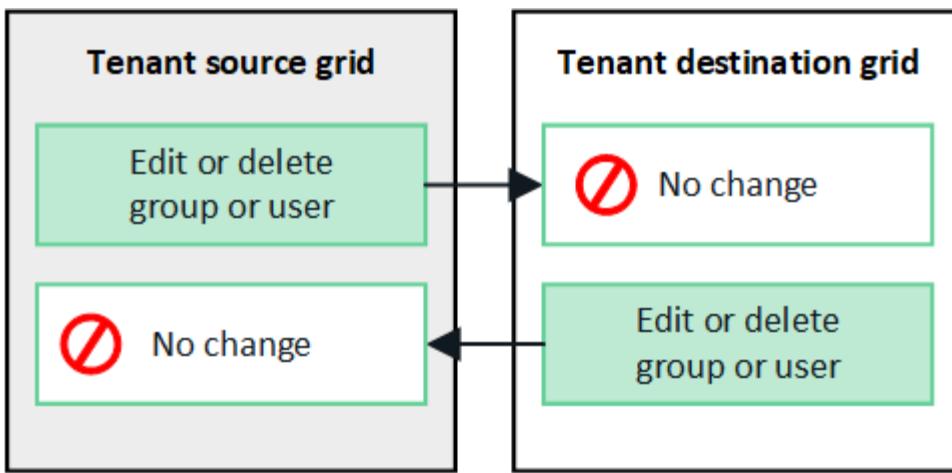
La clonazione avviene solo dalla griglia di origine del tenant alla griglia di destinazione del tenant. Se si creano o si importano gruppi e utenti nella griglia di destinazione del tenant, StorageGRID non clonerà questi elementi nella griglia di origine del tenant.



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

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

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



## Clona le chiavi di accesso S3 utilizzando l'API

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

### Prima di iniziare

- L'account tenant ha l'autorizzazione **Usa connessione federata alla griglia**.
- La connessione della federazione di rete ha uno **Stato di connessione** pari a **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 l'autorizzazione di accesso Root](#)" .
- Se si clonano le chiavi di accesso per un utente locale, l'utente esiste già su entrambe le griglie.



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

### 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.

### Passi

1. Utilizzando Tenant Manager sulla griglia di origine, "[crea le tue chiavi di accesso](#)" e scarica il `.csv` file.
2. Nella parte superiore di Tenant Manager, seleziona l'icona della guida e seleziona **Documentazione API**.
3. Nella sezione **s3**, seleziona il seguente endpoint:

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

**POST**

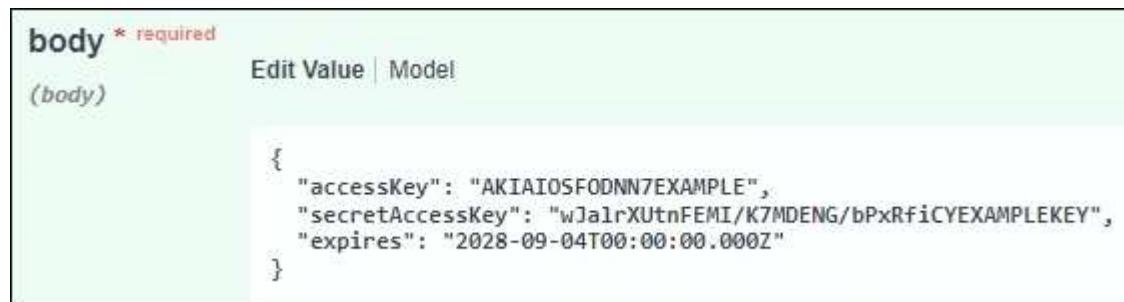
`/org/users/current-user/replicate-s3-access-key` Clone the current user's S3 key to the other grids.



4. Seleziona **Provalo**.

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

Assicuratevi di mantenere le virgolette doppie attorno a ciascuna stringa.



```
body * required
Edit Value | Model
(body)

{
  "accessKey": "AKIAIOSFODNN7EXAMPLE",
  "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "expires": "2028-09-04T00:00:00.000Z"
}
```

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

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

È possibile clonare le chiavi di accesso di un altro utente se quest'ultimo ha bisogno di accedere agli stessi bucket su entrambe le griglie.

#### Passi

1. Utilizzando Tenant Manager sulla griglia di origine, ["creare le chiavi di accesso S3 dell'altro utente"](#) e scarica il **.csv** file.
2. Nella parte superiore di Tenant Manager, seleziona l'icona della guida e seleziona **Documentazione API**.
3. Ottieni l'ID utente. Questo valore ti servirà per clonare le chiavi di accesso dell'altro utente.
  - a. Dalla sezione **utenti**, seleziona il seguente endpoint:  

```
GET /org/users
```
  - b. Seleziona **Provalo**.
  - c. Specificare i parametri che si desidera utilizzare durante la ricerca degli utenti.
  - d. Selezionare **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. Seleziona **Provalo**.
6. Nella casella di testo **userId**, incolla l'ID utente che hai copiato.
7. Nella casella di testo **corpo**, sostituire le voci di esempio per **chiave di accesso di esempio** e **chiave di accesso segreta** con i valori del file **.csv** per quell'utente.

Assicuratevi di mantenere le virgolette doppie attorno alla stringa.

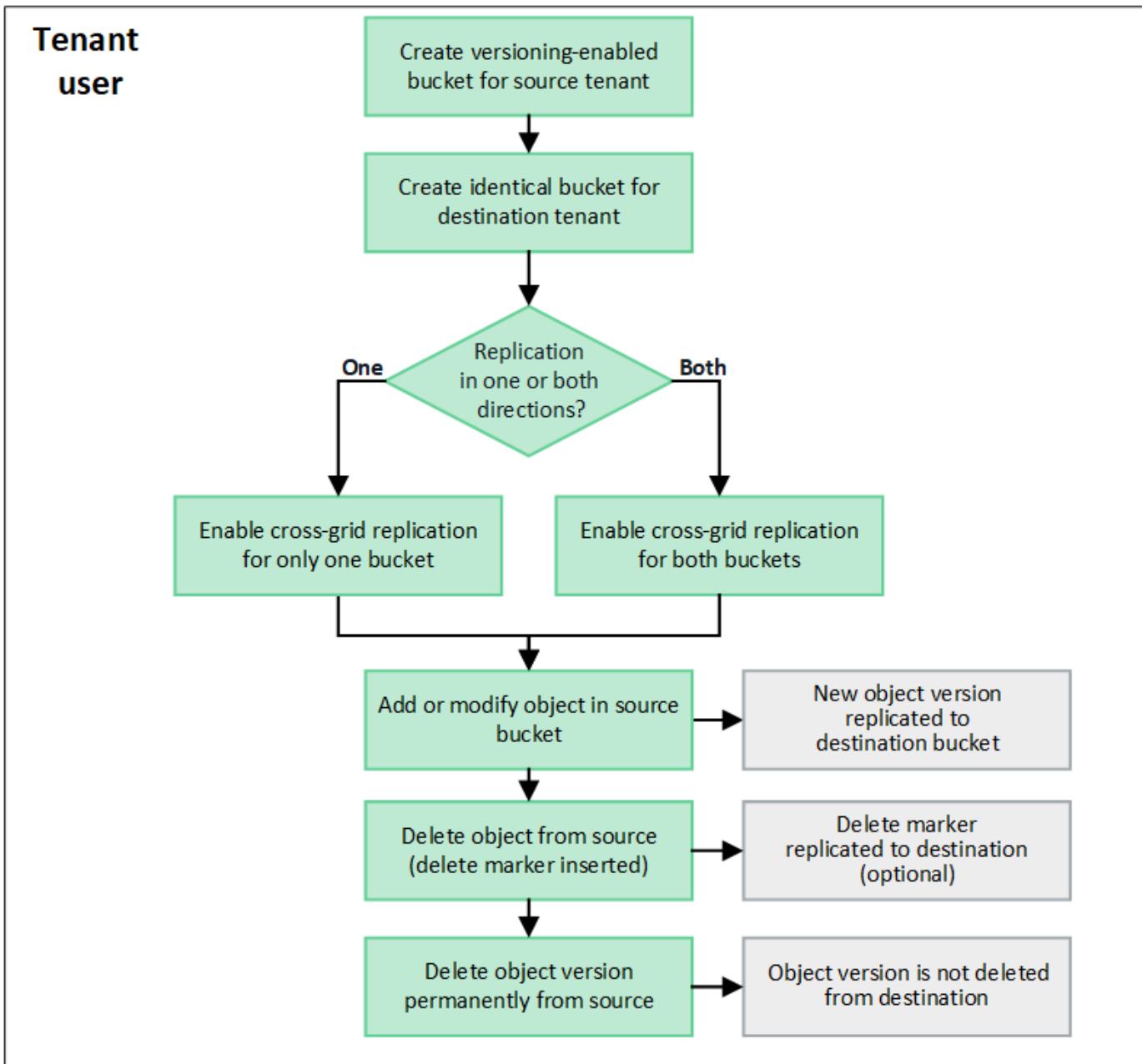
8. Se la chiave scadrà, sostituire la voce di esempio per **expires** con la data e l'ora di scadenza come stringa nel formato data-ora ISO 8601 (ad esempio, 2023-02-28T22:46:33-08:00 ). Se la chiave non scade, immettere **null** come valore per la voce **expires** (oppure rimuovere la riga **Expires**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

## Gestire la replicazione tra griglie

Se al momento della creazione dell'account tenant è stata assegnata l'autorizzazione **Usa connessione federazione griglia**, è possibile 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 replicazione tra griglie può avvenire in una o entrambe le direzioni.

### Flusso di lavoro per la replicazione tra griglie

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



## Configurare la replicazione tra griglie

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

### Prima di iniziare

- Hai esaminato i requisiti per la replicazione tra griglie. Vedere "[Che cosa è la replicazione cross-grid](#)" .
- Stai utilizzando un "[browser web supportato](#)" .
- L'account tenant ha l'autorizzazione **Usa connessione federata di griglia** e su entrambe le griglie esistono account tenant identici. Vedere "[Gestire gli inquilini autorizzati per la connessione alla federazione di rete](#)" .
- L'utente tenant con cui effettuerai l'accesso esiste già su entrambe le griglie e appartiene a un gruppo di utenti che ha "[Permesso di accesso root](#)" .

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

### Crea due bucket identici

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

#### Passi

1. Partendo da una delle due griglie nella connessione di federazione delle griglie, crea un nuovo bucket:
  - a. Sign in all'account tenant utilizzando le credenziali di un utente tenant presente su entrambe le griglie.

 Se non riesci ad accedere alla griglia di destinazione del tenant come utente locale, verifica che l'utente root dell'account tenant abbia impostato una password per il tuo account utente.
  - b. Seguire le istruzioni per "[creare un bucket S3](#)" .
  - c. Nella scheda **Gestisci impostazioni oggetto**, seleziona **Abilita controllo delle versioni degli oggetti**.
  - d. Se S3 Object Lock è abilitato per il sistema StorageGRID, non abilitare S3 Object Lock per il bucket.
  - e. Seleziona **Crea bucket**.
  - f. Selezionare **Fine**.
2. Ripetere questi passaggi per creare un bucket identico per lo stesso account tenant sull'altra griglia nella connessione di federazione della griglia.



A seconda delle necessità, ogni bucket può utilizzare una regione diversa.

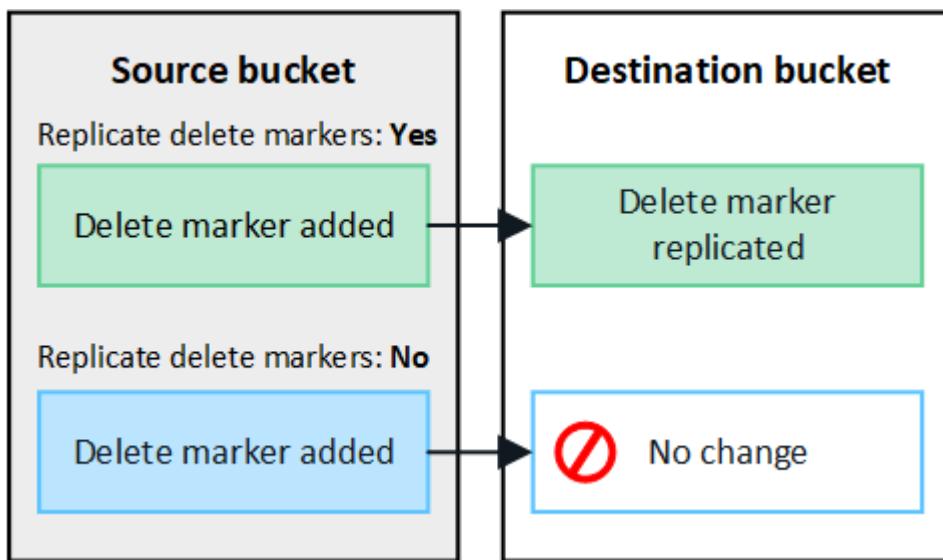
### Abilita la replicazione tra griglie

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

#### Passi

1. Partendo da una griglia di cui vuoi replicare gli oggetti, abilita "[replicazione cross-grid in una direzione](#)" :
  - a. Sign in all'account tenant per il bucket.
  - b. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
  - c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
  - d. Selezionare la scheda **Replica tra griglie**.
  - e. Selezionare **Abilita** e rivedere l'elenco dei requisiti.
  - f. Se tutti i requisiti sono stati soddisfatti, selezionare la connessione di federazione di rete che si desidera utilizzare.
  - g. Facoltativamente, modifica l'impostazione di **Replica marcatori di eliminazione** per determinare cosa accade sulla griglia di destinazione se un client S3 invia una richiesta di eliminazione alla griglia di origine che non include un ID versione:
    - **Sì** (predefinito): un marcitore di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione.
    - **No**: un marcitore di eliminazione viene aggiunto al bucket di origine ma non viene replicato nel

bucket di destinazione.



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

Vedere "[Che cosa è la replicazione cross-grid](#)" per i dettagli.

- Facoltativamente, modificare l'impostazione della categoria di controllo **Replica tra griglie** per gestire il volume dei messaggi di controllo:
  - Errore** (predefinito): nell'output di controllo vengono incluse solo le richieste di replica tra griglie non riuscite.
  - Normale**: vengono incluse tutte le richieste di replica tra griglie, il che aumenta significativamente il volume dell'output di audit.
- Rivedi le tue selezioni. Non è possibile modificare queste impostazioni a meno che entrambi i bucket non siano vuoti.
- Seleziona **Abilita e prova**.

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

- Facoltativamente, vai al bucket corrispondente sull'altra griglia e "[abilitare la replicazione cross-grid in entrambe le direzioni](#)".

### Test di replicazione tra griglie

Se la replica tra griglie è abilitata per un bucket, potrebbe essere necessario verificare che la connessione e la replica tra griglie funzionino correttamente e che i bucket di origine e di destinazione soddisfino ancora tutti i requisiti (ad esempio, che il controllo delle versioni sia ancora abilitato).

#### Prima di iniziare

- Stai utilizzando un "[browser web supportato](#)".

- Appartieni a un gruppo di utenti che ha il "Permesso di accesso root".

## Passi

1. Sign in all'account tenant per il bucket.
2. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
3. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
4. Selezionare la scheda **Replica tra griglie**.
5. Selezionare **Test connessione**.

Se la connessione è funzionante, viene visualizzato un banner di conferma. In caso contrario, verrà visualizzato un messaggio di errore che tu e l'amministratore della griglia potrete utilizzare per risolvere il problema. Per maggiori dettagli, vedere "["Risolvere gli errori di federazione della griglia"](#)".

6. Se la replica tra griglie è configurata per verificarsi in entrambe le direzioni, andare al bucket corrispondente sull'altra griglia e selezionare **Test connessione** per verificare che la replica tra griglie funzioni nell'altra direzione.

## Disabilita la replicazione tra griglie

È possibile interrompere definitivamente la replica tra griglie se non si desidera più copiare oggetti nell'altra griglia.

Prima di disattivare la replica tra griglie, tenere presente quanto segue:

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



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

## Prima di iniziare

- Stai utilizzando un "[browser web supportato](#)".
- Appartieni a un gruppo di utenti che ha il "Permesso di accesso root".

## Passi

1. A partire dalla griglia i cui oggetti non vuoi più replicare, interrompi la replica tra griglie per il bucket:
  - a. Sign in all'account tenant per il bucket.
  - b. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.

- c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
- d. Selezionare la scheda **Replica tra griglie**.
- e. Selezionare **Disabilita replicazione**.
- f. Se sei sicuro di voler disabilitare la replica tra griglie per questo bucket, digita **Sì** nella casella di testo e seleziona **Disabilita**.

Dopo qualche istante, verrà visualizzato un messaggio di conferma dell'operazione. I nuovi oggetti aggiunti a questo bucket non possono più essere replicati automaticamente nell'altra griglia. La **replica tra griglie** non è più visualizzata come funzionalità abilitata nella pagina Bucket.

2. Se la replica tra griglie è stata configurata per essere eseguita in entrambe le direzioni, passare al bucket corrispondente sull'altra griglia e interrompere la replica tra griglie nell'altra direzione.

## Visualizza le connessioni della federazione di griglia

Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federata alla griglia**, puoi visualizzare le connessioni consentite.

### Prima di iniziare

- L'account tenant ha l'autorizzazione **Usa connessione federata alla griglia**.
- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Permesso di accesso root](#)" .

### Passi

1. Selezionare **STORAGE (S3) > Connessioni federazione di rete**.

Viene visualizzata la pagina di connessione della federazione Grid, che include una tabella che riassume le seguenti informazioni:

Colonna	Descrizione
Nome della connessione	Le connessioni della federazione di rete che questo tenant è autorizzato a utilizzare.
Bucket con replicazione cross-grid	Per ogni connessione di federazione di griglia, i bucket tenant che hanno abilitato la replica tra griglie. Gli oggetti aggiunti a questi bucket verranno replicati nell'altra griglia nella connessione.
Ultimo errore	Per ogni connessione di federazione di griglia, l'errore più recente verificatosi, se presente, durante la replica dei dati sull'altra griglia. Vedere <a href="#">Cancella l'ultimo errore</a> .

2. Facoltativamente, seleziona un nome bucket per "[visualizza i dettagli del bucket](#)" .

### Cancella l'ultimo errore

Potrebbe apparire un errore nella colonna **Ultimo errore** per uno dei seguenti motivi:

- La versione dell'oggetto sorgente non è stata trovata.

- Il bucket di origine non è stato trovato.
- Il bucket di destinazione è stato eliminato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il controllo delle versioni del bucket di destinazione è sospeso.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più sottoposto a controllo di versione.



Questa colonna mostra solo l'ultimo errore di replicazione tra griglie verificatosi; gli errori precedenti che potrebbero essersi verificati non verranno mostrati.

## Passi

1. Se nella colonna **Ultimo errore** viene visualizzato un messaggio, visualizzarne il testo.

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

The screenshot shows a table titled 'Grid federation connections' with the following columns and data:

Connection name	Buckets with cross-grid replication	Last error
Grid 1-Grid 2	my-cgr-bucket	<p>2022-12-07 16:02:20 MST</p> <p>Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)</p>

2. Eseguire tutte le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso sul bucket di destinazione per la replica tra griglie, riattivare il controllo delle versioni per quel bucket.
3. Selezionare la connessione dalla tabella.
4. Seleziona **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Aspetta 5-6 minuti e poi ingerisci un nuovo oggetto nel secchio. Verificare che il messaggio di errore non venga più visualizzato.



Per garantire che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo il timestamp nel messaggio prima di acquisire un nuovo oggetto.

7. Per determinare se la replica di alcuni oggetti non è riuscita a causa dell'errore del bucket, vedere "[Identificare e riprovare le operazioni di replicazione non riuscite](#)".

## Gestisci gruppi e utenti

### Utilizzare la federazione delle identità

L'utilizzo della federazione delle identità velocizza la configurazione di gruppi e utenti

tenant e consente agli utenti tenant di accedere all'account tenant utilizzando credenziali familiari.

## Configurare la federazione delle identità per Tenant Manager

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

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Permesso di accesso root](#)" .
- Stai utilizzando Active Directory, Azure AD, OpenLDAP o Oracle Directory Server come provider di identità.



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

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

### Informazioni su questo compito

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



This tenant account uses the LDAP server that is configured for the Grid Manager.

Contact the grid administrator for information or to change this setting.

### Inserisci la configurazione

Quando si configura la federazione delle identità, si forniscono i valori necessari a StorageGRID per connettersi a un servizio LDAP.

### Passi

1. Selezionare **GESTIONE ACCESSI > Federazione identità**.
2. Selezionare **Abilita federazione delle identità**.
3. Nella sezione **Tipo di servizio LDAP**, seleziona il tipo di servizio LDAP che desideri configurare.

## LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

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

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. procedere al passaggio successivo.

- **Nome univoco utente:** il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `uid` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
- **UUID utente:** il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun utente per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
- **Nome univoco del gruppo:** il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `cn` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
- **UUID gruppo:** il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.

5. Per tutti i tipi di servizio LDAP, immettere le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.

- **Nome host:** nome di dominio completo (FQDN) o indirizzo IP del server LDAP.
- **Porta:** la porta utilizzata per connettersi al server LDAP.



La porta predefinita per STARTTLS è 389, mentre la porta predefinita per LDAPS è 636. Tuttavia, puoi utilizzare qualsiasi porta, a patto che il firewall sia configurato correttamente.

- **Nome utente:** percorso completo del nome distinto (DN) dell'utente che si connetterà al server LDAP.

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

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

- `sAMAccountName` `O` `uid`
- `objectGUID`, `entryUUID` , O `nsuniqueid`
- `cn`

- `memberOf`O`isMemberOf`
  - **Directory attiva:** `objectSid`, `primaryGroupID`, `userAccountControl`, `E` `userPrincipalName`
  - **Azzurro:** `accountEnabled` `E` `userPrincipalName`
  - **Password:** la password associata al nome utente.
-  Se in futuro dovessi cambiare la password, dovrà aggiornarla in questa pagina.
- **DN base gruppo:** percorso completo del nome distinto (DN) per un sottoalbero LDAP in cui si desidera 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 utilizzati come gruppi federati.
-  I valori **Nome univoco del gruppo** devono essere univoci all'interno del **DN di base del gruppo** a cui appartengono.
- **DN base utente:** percorso completo del nome distinto (DN) di un sottoalbero LDAP in cui si desidera cercare gli utenti.



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

- **Formato nome utente associato** (facoltativo): il modello di nome utente predefinito che StorageGRID dovrebbe utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il **formato nome utente di associazione** perché può consentire agli utenti di accedere se StorageGRID non è in grado di assocarsi all'account di servizio.

Inserisci uno di questi modelli:

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

Includi **[USERNAME]** esattamente come scritto.

## 6. Nella sezione Transport Layer Security (TLS), seleziona un'impostazione di sicurezza.

- **Usa STARTTLS:** usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Azure.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Azure.
- **Non utilizzare TLS:** il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Azure.



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

## 7. Se hai selezionato STARTTLS o LDAPS, scegli il certificato utilizzato per proteggere la connessione.

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.
- **Utilizza 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 Certificato CA.

#### Testare la connessione e salvare la configurazione

Dopo aver immesso tutti i valori, è necessario testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente associato, se ne è stato fornito uno.

#### Passi

1. Selezionare **Test connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
  - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.
  - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risovi eventuali problemi e verifica nuovamente la connessione.
3. Se hai fornito un formato di nome utente vincolato, 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 /.

**Test Connection**

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

**Test username**

The username of a federated user.

**Test password**

- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.
- Se le impostazioni di connessione, il formato del nome utente associato o il nome utente e la password di prova non sono validi, viene visualizzato un messaggio di errore. Risovi eventuali problemi e verifica nuovamente la connessione.

## Forza la sincronizzazione con la fonte dell'identità

Il sistema StorageGRID sincronizza periodicamente i gruppi federati e gli utenti dalla fonte di identità. È possibile forzare l'avvio della sincronizzazione se si desidera abilitare o limitare le autorizzazioni utente il più rapidamente possibile.

### Passi

1. Vai alla pagina Federazione delle identità.
2. Seleziona **Sincronizza server** nella parte superiore della pagina.

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



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

## Disabilitare la federazione delle identità

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

### Informazioni su questo compito

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

- Gli utenti federati non potranno effettuare l'accesso.
- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno effettuare l'accesso dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non verrà eseguita e non verranno generati avvisi per gli account che non sono stati sincronizzati.
- La casella di controllo **Abilita federazione delle identità** è disabilitata se l'accesso Single Sign-On (SSO) è impostato su **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere "["Disabilitare l'accesso singolo"](#)".

### Passi

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

## Linee guida per la configurazione del server OpenLDAP

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



Per le origini identità diverse da ActiveDirectory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare tutte le chiavi S3 dell'utente o rimuovere l'utente da tutti i gruppi.

## Sovrapposizioni di membri e raffinazione

Le sovrapposizioni memberof e refint dovrebbero essere abilitate. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in <http://www.openldap.org/doc/admin24/index.html>["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"] .

## Indicizzazione

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

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

Inoltre, assicurati che i campi menzionati nella guida per Nome utente siano indicizzati per prestazioni ottimali.

Consultare le informazioni sul mantenimento dell'appartenenza al gruppo inverso in <http://www.openldap.org/doc/admin24/index.html>["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"] .

## Gestire gruppi di tenant

### Creare gruppi per un tenant S3

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

#### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Permesso di accesso root](#)" .
- Se si prevede di importare un gruppo federato, è necessario "[federazione di identità configurata](#)" e il gruppo federato esiste già nell'origine identità configurata.
- Se il tuo account tenant ha l'autorizzazione **Usa connessione federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni per "[clonazione di gruppi di tenant e utenti](#)" e hai effettuato l'accesso alla griglia di origine del tenant.

#### Accedi alla procedura guidata Crea gruppo

Come primo passo, accedi alla procedura guidata Crea gruppo.

#### Passi

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
2. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, verifica che venga visualizzato un banner blu, che indica che i nuovi gruppi creati su questa griglia verranno clonati nello stesso tenant sull'altra griglia nella connessione. Se questo banner non viene visualizzato, è possibile che tu abbia effettuato l'accesso alla griglia di destinazione del tenant.

# Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

0 groups

Create group

Actions ▾

**i** This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant groups will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

### 3. Seleziona **Crea gruppo**.

#### Scegli un tipo di gruppo

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

#### Passi

1. Selezionare la scheda **Gruppo locale** per creare un gruppo locale oppure selezionare la scheda **Gruppo federato** per importare un gruppo dall'origine identità configurata in precedenza.

Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), gli utenti appartenenti a gruppi locali non potranno accedere a Tenant Manager, sebbene possano utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni del gruppo.

2. Inserisci il nome del gruppo.

- **Gruppo locale:** immettere sia un nome visualizzato che un nome univoco. Potrai modificare il nome visualizzato in un secondo momento.



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

- **Gruppo federato:** immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

3. Selezionare **Continua**.

#### Gestisci i permessi del gruppo

Le autorizzazioni di gruppo controllano quali attività gli utenti possono eseguire in Tenant Manager e nell'API Tenant Management.

#### Passi

1. Per **Modalità di accesso**, seleziona una delle seguenti opzioni:

- **Lettura-scrittura** (predefinito): gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.

- **Sola lettura:** gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Tenant Manager o Tenant Management API. Gli utenti locali con privilegi di 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.

Vedere ["Autorizzazioni di gestione degli inquilini"](#).

## 3. Selezionare **Continua**.

### Imposta i criteri di gruppo S3

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

#### Passi

##### 1. Seleziona il criterio che vuoi utilizzare 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 un criterio bucket. Se si seleziona questa opzione, per impostazione predefinita solo l'utente root avrà accesso alle risorse S3.
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 oggetti e leggere dati, metadati e tag degli oggetti. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Non puoi modificare questa stringa.
Accesso completo	Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo con accesso completo. Non puoi modificare questa stringa.
Mitigazione del ransomware	<p>Questo criterio di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare definitivamente gli oggetti dai bucket in cui è abilitato il controllo delle versioni degli oggetti.</p> <p>Gli utenti Tenant Manager che dispongono dell'autorizzazione <b>Gestisci tutti i bucket</b> possono ignorare questo criterio di gruppo. Limitare l'autorizzazione Gestisci tutti i bucket agli utenti attendibili e utilizzare l'autenticazione a più fattori (MFA) laddove disponibile.</p>
Costume	Agli utenti del gruppo vengono concesse le autorizzazioni specificate 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. È necessario immettere una stringa valida in formato JSON.

Per informazioni dettagliate sui criteri di gruppo, inclusa la sintassi del linguaggio e gli esempi, vedere "[Criteri di gruppo di esempio](#)".

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)

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

 Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, tutti gli utenti selezionati quando si crea un gruppo locale sulla griglia di origine non verranno inclusi quando il gruppo viene clonato sulla griglia di destinazione. Per questo motivo, non selezionare gli utenti quando crei il gruppo. In alternativa, seleziona il gruppo quando crei gli utenti.

#### Passi

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 account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ti trovi sulla griglia di origine del tenant, il nuovo gruppo viene clonato nella griglia di destinazione del tenant.

**Successo** appare come **Stato di clonazione** nella sezione Panoramica della pagina dei dettagli del gruppo.

#### Creare gruppi per un tenant Swift

È possibile gestire le autorizzazioni di accesso per un account tenant Swift importando gruppi federati o creando gruppi locali. Almeno un gruppo deve disporre dell'autorizzazione di amministratore Swift, necessaria per gestire i contenitori e gli oggetti per un account tenant Swift.

 Il supporto per le applicazioni client Swift è stato deprecato e verrà rimosso in una versione futura.

#### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)".
- Appartieni a un gruppo di utenti che ha il "[Permesso di accesso root](#)".
- Se si prevede di importare un gruppo federato, è necessario "[federazione di identità configurata](#)" e il gruppo federato esiste già nell'origine identità configurata.

#### Accedi alla procedura guidata Crea gruppo

#### Passi

Come primo passo, accedi alla procedura guidata Crea gruppo.

1. Selezionare **GESTIONE ACCESSI > Gruppi**.

2. Seleziona **Crea gruppo**.

#### Scegli un tipo di gruppo

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

#### Passi

1. Selezionare la scheda **Gruppo locale** per creare un gruppo locale oppure selezionare la scheda **Gruppo federato** per importare un gruppo dall'origine identità configurata in precedenza.

Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), gli utenti appartenenti a gruppi locali non potranno accedere a Tenant Manager, sebbene possano utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni del gruppo.

2. Inserisci il nome del gruppo.

- **Gruppo locale**: immettere sia un nome visualizzato che un nome univoco. Potrai modificare il nome visualizzato in un secondo momento.
- **Gruppo federato**: immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

3. Selezionare **Continua**.

#### Gestisci i permessi del gruppo

Le autorizzazioni di gruppo controllano quali attività gli utenti possono eseguire in Tenant Manager e nell'API Tenant Management.

#### Passi

1. Per **Modalità di accesso**, seleziona una delle seguenti opzioni:

- **Lettura-scrittura** (predefinito): gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
- **Sola lettura**: gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Tenant Manager o Tenant Management API. Gli utenti locali con privilegi di 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. Selezionare la casella di controllo **Accesso root** se gli utenti del gruppo devono accedere a Tenant Manager o all'API Tenant Management.

3. Selezionare **Continua**.

#### Imposta i criteri di gruppo Swift

Gli utenti Swift necessitano dell'autorizzazione di amministratore per autenticarsi nella Swift REST API per creare contenitori e acquisire oggetti.

1. Selezionare la casella di controllo **Amministratore Swift** se gli utenti del gruppo devono utilizzare l'API REST Swift per gestire contenitori e oggetti.

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

#### Aggiungi utenti (solo gruppi locali)

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

#### Passi

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.

Se non hai ancora creato utenti locali, puoi aggiungere questo gruppo all'utente nella pagina Utenti. Vedere "[Gestisci gli utenti locali](#)" .

2. Seleziona **Crea gruppo e Fine**.

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

#### Autorizzazioni di gestione degli inquilini

Prima di creare un gruppo di tenant, valuta quali autorizzazioni vuoi assegnare a quel gruppo. Le autorizzazioni di gestione degli inquilini determinano quali attività gli utenti possono eseguire utilizzando Tenant Manager o Tenant Management API. Un utente può appartenere a uno o più gruppi. Le autorizzazioni sono cumulative se un utente appartiene a più gruppi.

Per accedere a Tenant Manager o utilizzare l'API Tenant Management, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono effettuare l'accesso possono eseguire le seguenti attività:

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

Per tutte le autorizzazioni, l'impostazione Modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni oppure se possono solo visualizzare le impostazioni e le funzionalità correlate.



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.

È possibile assegnare le seguenti autorizzazioni a un gruppo. Si noti che i tenant S3 e i tenant Swift hanno autorizzazioni di gruppo diverse.

Permesso	Descrizione	Dettagli
Accesso root	Fornisce accesso completo al Tenant Manager e all'API Tenant Management.	Gli utenti Swift devono disporre dell'autorizzazione di accesso Root per accedere all'account tenant.

Permesso	Descrizione	Dettagli
Amministratore	Solo per inquilini Swift. Fornisce l'accesso completo ai contenitori e agli oggetti Swift per questo account tenant	Gli utenti Swift devono disporre dell'autorizzazione di amministratore Swift per eseguire qualsiasi operazione con la Swift REST API.
Gestisci le tue credenziali S3	Consente agli utenti di creare e rimuovere le proprie chiavi di accesso S3.	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu <b>ARCHIVIAZIONE (S3) &gt; Le mie chiavi di accesso S3</b> .
Visualizza tutti i bucket	<p><b>Tenant S3:</b> consente agli utenti di visualizzare tutti i bucket e le relative configurazioni.</p> <p><b>Tenant Swift:</b> consente agli utenti Swift di visualizzare tutti i container e le configurazioni dei container utilizzando l'API di gestione dei tenant.</p>	<p>Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu <b>Bucket</b>.</p> <p>Questa autorizzazione è sostituita dall'autorizzazione Gestisci tutti i bucket. Non influisce sui criteri di gruppo o sui bucket S3 utilizzati dai client S3 o dalla console S3.</p> <p>È possibile assegnare questa autorizzazione solo ai gruppi Swift dall'API di gestione tenant. Non è possibile assegnare questa autorizzazione ai gruppi Swift tramite Tenant Manager.</p>
Gestisci tutti i bucket	<p><b>Tenant S3:</b> consente agli utenti di utilizzare Tenant Manager e l'API Tenant Management per creare ed eliminare bucket S3 e gestire le impostazioni per tutti i bucket S3 nell'account tenant, indipendentemente dal bucket S3 o dai criteri di gruppo.</p> <p><b>Tenant Swift:</b> consente agli utenti Swift di controllare la coerenza dei contenitori Swift utilizzando l'API di gestione dei tenant.</p>	<p>Gli utenti che non dispongono dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket non visualizzano l'opzione di menu <b>Bucket</b>.</p> <p>Questa autorizzazione sostituisce l'autorizzazione Visualizza tutti i bucket. Non influisce sui criteri di gruppo o sui bucket S3 utilizzati dai client S3 o dalla console S3.</p> <p>È possibile assegnare questa autorizzazione solo ai gruppi Swift dall'API di gestione tenant. Non è possibile assegnare questa autorizzazione ai gruppi Swift tramite Tenant Manager.</p>
Gestisci gli endpoint	Consente agli utenti di utilizzare Tenant Manager o l'API Tenant Management per creare o modificare gli endpoint dei servizi della piattaforma, utilizzati come destinazione per i servizi della piattaforma StorageGRID .	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu <b>Endpoint dei servizi della piattaforma</b> .

Permesso	Descrizione	Dettagli
Utilizzare la scheda Console S3	Se combinato con l'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket, consente agli utenti di visualizzare e gestire gli oggetti dalla scheda Console S3 nella pagina dei dettagli di un bucket.	

## Gestisci gruppi

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

### Prima di iniziare

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

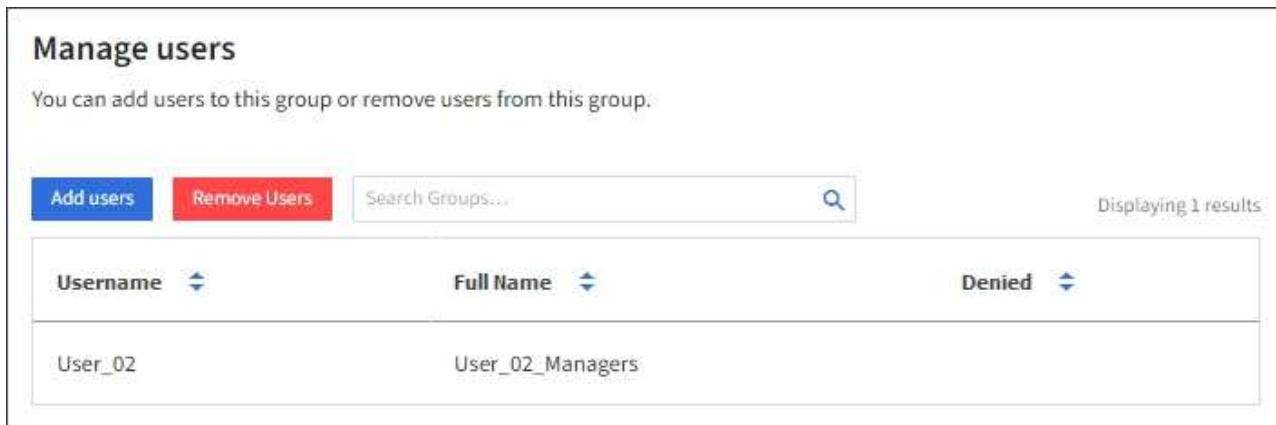
### Visualizza o modifica il gruppo

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

### Passi

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
  2. Esaminare le informazioni fornite nella pagina Gruppi, che elenca le informazioni di base per tutti i gruppi locali e federati per questo account tenant.
- Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si stanno visualizzando i gruppi sulla griglia di origine del tenant:
- Un messaggio banner 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 ha fallito.
3. Se vuoi cambiare il nome del gruppo:
    - a. Selezionare la casella di controllo per il gruppo.
    - b. Seleziona **Azioni > Modifica nome gruppo**.
    - c. Inserisci il nuovo nome.
    - d. Seleziona **Salva modifiche**.
  4. Se desideri visualizzare maggiori dettagli o apportare modifiche aggiuntive, procedi in uno dei seguenti modi:
    - Selezionare il nome del gruppo.
    - Seleziona la casella di controllo per il gruppo e seleziona **Azioni > Visualizza dettagli gruppo**.
  5. Esaminare la sezione Panoramica, che mostra le seguenti informazioni per ciascun gruppo:
    - Nome da visualizzare
    - Nome univoco
    - Tipo

- Modalità di accesso
  - Permessi
  - Politica S3
  - Numero di utenti in questo gruppo
  - Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando il gruppo sulla griglia di origine del tenant:
    - Stato della clonazione, **Riuscito** o **Fallito**
    - Un banner blu che indica che se modifichi o elimini questo gruppo, le tue modifiche non verranno sincronizzate con l'altra griglia.
6. Modificare le impostazioni del gruppo secondo necessità. Vedere "[Creare gruppi per un tenant S3](#)" E "[Creare gruppi per un tenant Swift](#)" per i dettagli su cosa inserire.
- Nella sezione Panoramica, modifica il nome visualizzato selezionando il nome o l'icona di modifica .
  - Nella scheda **Autorizzazioni gruppo**, aggiorna le autorizzazioni e seleziona **Salva modifiche**.
  - Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.
    - Se si sta modificando un gruppo S3, è possibile selezionare facoltativamente un criterio di gruppo S3 diverso oppure immettere la stringa JSON per un criterio personalizzato, a seconda delle necessità.
    - Se stai modificando un gruppo Swift, seleziona o deselectiona facoltativamente la casella di controllo **Amministratore Swift**.
7. Per aggiungere uno o più utenti locali esistenti al gruppo:
- Selezionare la scheda Utenti.



Username	Full Name	Denied
User_02	User_02_Managers	Denied

- Seleziona **Aggiungi utenti**.
- Seleziona gli utenti esistenti che desideri aggiungere e seleziona **Aggiungi utenti**.

In alto a destra appare un messaggio di conferma.

8. Per rimuovere gli utenti locali dal gruppo:
- Selezionare la scheda Utenti.
  - Seleziona **Rimuovi utenti**.
  - Seleziona gli utenti che vuoi rimuovere e seleziona **Rimuovi utenti**.

In alto a destra appare un messaggio di conferma.

9. Conferma di aver selezionato **Salva modifiche** per ogni sezione modificata.

### Gruppo duplicato

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



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

### Passi

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
2. Seleziona la casella di controllo relativa al gruppo che desideri duplicare.
3. Selezionare **Azioni > Duplica gruppo**.
4. Vedere "[Creare gruppi per un tenant S3](#)" O "[Creare gruppi per un tenant Swift](#)" per i dettagli su cosa inserire.
5. Seleziona **Crea gruppo**.

### Riprova a clonare il gruppo

Per riprovare una clonazione non riuscita:

1. Selezionare ciascun gruppo che indica (*Clonazione non riuscita*) sotto il nome del gruppo.
2. Selezionare **Azioni > Clona gruppi**.
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun gruppo che stai clonando.

Per ulteriori informazioni, vedere "[Clona gruppi tenant e utenti](#)".

### Elimina uno o più gruppi

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

### Passi

1. Selezionare **GESTIONE ACCESSI > Gruppi**.
2. Seleziona la casella di controllo per ogni gruppo che desideri eliminare.
3. Selezionare **Azioni > Elimina gruppo** o **Azioni > Elimina gruppi**.
4. Selezionare **Elimina gruppo** o **Elimina gruppi**.

Viene visualizzata una finestra di dialogo di conferma.

## Gestisci gli utenti locali

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



Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), gli utenti locali non potranno accedere a Tenant Manager o all'API Tenant Management, sebbene possano utilizzare le applicazioni client per accedere alle risorse del tenant, in base alle autorizzazioni di gruppo.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Permesso di accesso root](#)" .
- Se il tuo account tenant ha l'autorizzazione **Usa connessione federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni per "[clonazione di gruppi di tenant e utenti](#)" e hai effettuato l'accesso alla griglia di origine del tenant.

### Crea un utente locale

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

Gli utenti S3 che non appartengono ad alcun gruppo non hanno autorizzazioni di gestione né criteri di gruppo S3 applicati. A questi utenti potrebbe essere concesso l'accesso al bucket S3 tramite un criterio bucket.

Gli utenti Swift che non appartengono ad alcun gruppo non hanno autorizzazioni di gestione né accesso al contenitore Swift.

#### Accedi alla procedura guidata Crea utente

##### Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.

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

## Users

View local and federated users. Edit properties and group membership of local users.

1 user

Create user

Actions ▾

**i** This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant users will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

## 2. Seleziona **Crea utente**.

### Inserisci le credenziali

#### Passi

1. Per il passaggio **Inserisci credenziali utente**, compila i seguenti campi.

Campo	Descrizione
Nome e cognome	Il nome completo di questo utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
Nome utente	Il nome che questo utente utilizzerà per accedere. I nomi utente devono essere univoci e non possono essere modificati.  <b>Nota:</b> se l'account tenant dispone dell'autorizzazione <b>Usa connessione federazione griglia</b> , si verificherà un errore di clonazione se lo stesso <b>Nome utente</b> esiste già per il tenant sulla griglia di destinazione.
Password e Conferma password	La password che l'utente utilizzerà inizialmente per effettuare l'accesso.
Nega l'accesso	Selezionare <b>Sì</b> per impedire a questo utente di accedere all'account tenant, anche se potrebbe ancora appartenere a uno o più gruppi.  Ad esempio, seleziona <b>Sì</b> per sospendere temporaneamente la possibilità di un utente di accedere.

## 2. Selezionare **Continua**.

### Assegna ai gruppi

#### Passi

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

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

Gli utenti che non appartengono ad alcun gruppo non avranno autorizzazioni di gestione. I permessi sono cumulativi. Gli utenti avranno tutte le autorizzazioni per tutti i gruppi a cui appartengono. Vedere ["Autorizzazioni di gestione degli inquilini"](#) .

## 2. Seleziona **Crea utente**.

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

## 3. Selezionare **Fine** per tornare alla pagina Utenti.

### Visualizza o modifica l'utente locale

#### Passi

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

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

- Un messaggio banner indica che se modifichi o rimuovi un utente, le modifiche non verranno sincronizzate con l'altra griglia.
- Se necessario, un messaggio banner indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. È possibile [riprova un clone utente che non è riuscito](#) Potrebbe

### 3. Se vuoi cambiare il nome completo dell'utente:

- a. Selezionare la casella di controllo per l'utente.
- b. Seleziona **Azioni > Modifica nome completo**.
- c. Inserisci il nuovo nome.
- d. Seleziona **Salva modifiche**.

### 4. Se desideri visualizzare maggiori dettagli o apportare modifiche aggiuntive, procedi in uno dei seguenti modi:

- Seleziona il nome utente.
- Selezionare la casella di controllo per l'utente e selezionare **Azioni > Visualizza dettagli utente**.

### 5. Esaminare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:

- Nome e cognome
- Nome utente
- Tipo di utente
- Accesso negato
- Modalità di accesso
- Appartenenza al gruppo
- Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si visualizza l'utente sulla griglia di origine del tenant:

- Stato della clonazione, **Riuscito** o **Fallito**
  - Un banner blu che indica che se modifichi questo utente, le tue modifiche non verranno sincronizzate con l'altra griglia.
6. Modificare le impostazioni utente secondo necessità. Vedere [Crea utente locale](#) per i dettagli su cosa inserire.
- Nella sezione Panoramica, modifica il nome completo selezionando il nome o l'icona di modifica .
  - Non è possibile modificare il nome utente.
  - Nella scheda **Password**, modifica la password dell'utente e seleziona **Salva modifiche**.
  - Nella scheda **Accesso**, seleziona **No** per consentire all'utente di accedere oppure seleziona **Sì** per impedirgli di accedere. Quindi, seleziona **Salva modifiche**.
  - Nella scheda **Chiavi di accesso**, seleziona **Crea chiave** e segui le istruzioni per ["creazione delle chiavi di accesso S3 di un altro utente"](#).
  - 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 modificata.

### Utente locale duplicato

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



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

### Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Seleziona la casella di controllo relativa all'utente che desideri duplicare.
3. Selezionare **Azioni > Duplica utente**.
4. Vedere [Crea utente locale](#) per i dettagli su cosa inserire.
5. Seleziona **Crea utente**.

### Riprova la clonazione dell'utente

Per riprovare una clonazione non riuscita:

1. Selezionare ciascun utente che indica (*Clonazione non riuscita*) sotto il nome utente.
2. Seleziona **Azioni > Clona utenti**.
3. Visualizza lo stato dell'operazione di clonazione dalla pagina dei dettagli di ciascun utente che stai clonando.

Per ulteriori informazioni, vedere ["Clona gruppi tenant e utenti"](#).

### Elimina uno o più utenti locali

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

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

 Per eliminare gli utenti federati è necessario utilizzare l'origine dell'identità federata.

## Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Seleziona la casella di controllo per ogni utente che desideri eliminare.
3. Selezionare **Azioni > Elimina utente** oppure **Azioni > Elimina utenti**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Elimina utente** o **Elimina utenti**.

# Gestisci le chiavi di accesso S3

## Gestisci le chiavi di accesso S3

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

Le chiavi di accesso S3 possono essere gestite come segue:

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

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 un criterio bucket.

## Crea le tue chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile creare le proprie chiavi di accesso S3. Per accedere ai tuoi bucket e oggetti devi disporre di una chiave di accesso.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Gestisci le tue credenziali S3](#) o l'autorizzazione di accesso Root" .

### Informazioni su questo compito

Puoi creare una o più chiavi di accesso S3 che ti consentono di creare e gestire i bucket per il tuo account tenant. Dopo aver creato una nuova chiave di accesso, aggiorna l'applicazione con il tuo nuovo ID chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi del necessario ed

elimina quelle che non utilizzi. Se hai una sola chiave e questa sta per scadere, creane una nuova prima che scada quella vecchia, quindi eliminala.

Ogni chiave può avere una scadenza specifica o nessuna scadenza. Per quanto riguarda la scadenza, seguire queste linee guida:

- Imposta una scadenza per le tue chiavi per limitare l'accesso a un determinato periodo di tempo. Impostare un tempo di scadenza breve può aiutare a ridurre il rischio nel caso in cui l'ID della chiave di accesso e la chiave di accesso segreta vengano 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 quelle vecchie.

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

## Passi

### 1. Selezionare **ARCHIVIAZIONE (S3) > Le mie chiavi di accesso**.

Viene visualizzata la pagina **Le mie chiavi di accesso**, in cui sono elencate tutte le chiavi di accesso esistenti.

### 2. Seleziona **Crea chiave**.

### 3. Eseguire 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 corrente. L'orario di scadenza può essere di almeno un minuto rispetto all'orario corrente.

### 4. Seleziona **Crea chiave di accesso**.

Viene visualizzata la finestra di dialogo **Scarica chiave di accesso**, in cui sono elencati l'ID della chiave di accesso e la chiave di accesso segreta.

### 5. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di 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 è possibile copiare o scaricare le chiavi dopo aver chiuso la finestra di dialogo.

### 6. Selezionare **Fine**.

La nuova chiave è elencata nella pagina **Le mie chiavi di accesso**.

7. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, puoi facoltativamente utilizzare l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedere "[Clona le chiavi di accesso S3 utilizzando l'API](#)".

## Visualizza le tue chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone di "[autorizzazione appropriata](#)" , puoi visualizzare un elenco delle tue chiavi di accesso S3. È possibile ordinare l'elenco in base alla data di scadenza, in modo da poter determinare quali chiavi scadranno presto. Se necessario, puoi "[creare nuove chiavi](#)" O "[cancellare i tasti](#)" che non utilizzi più.

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

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha la possibilità di gestire le proprie credenziali S3 "[permesso](#)" .

### Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Le mie chiavi di accesso**.
2. Dalla pagina Le mie chiavi di accesso, ordina tutte le chiavi di accesso esistenti in base a **Ora di scadenza** o **ID chiave di accesso**.
3. Se necessario, crea nuove chiavi o elimina quelle che non utilizzi più.

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

Le chiavi scadute vengono rimosse automaticamente.

## Elimina le tue chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le proprie chiavi di accesso S3. Dopo aver eliminato una chiave di accesso, non sarà più possibile utilizzarla per accedere agli oggetti e ai bucket nell'account tenant.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Tu hai il "[Gestisci le tue autorizzazioni per le credenziali S3](#)" .

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

## Passi

1. Selezionare **ARCHIVIAZIONE (S3) > Le mie chiavi di accesso**.
2. Nella pagina **Le mie chiavi di accesso**, seleziona la casella di controllo per ogni chiave di accesso che desideri rimuovere.
3. Selezionare **Elimina tasto**.
4. Nella finestra di dialogo di conferma, seleziona **Elimina chiave**.

Nell'angolo in alto a destra della pagina appare un messaggio di conferma.

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

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile creare chiavi di accesso S3 per altri utenti, ad esempio applicazioni che necessitano di accedere a bucket e oggetti.

### Prima di iniziare

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

### Informazioni su questo compito

È possibile creare una o più chiavi di accesso S3 per altri utenti, in modo che possano creare e gestire i bucket per il proprio account tenant. Dopo aver creato una nuova chiave di accesso, aggiorna l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quelle necessarie all'utente ed elimina quelle che non vengono utilizzate. Se hai una sola chiave e questa sta per scadere, creane una nuova prima che scada quella vecchia, quindi eliminala.

Ogni chiave può avere una scadenza specifica o nessuna scadenza. Per quanto riguarda la scadenza, seguire queste linee guida:

- Imposta una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. Impostare un tempo di scadenza breve può aiutare a ridurre il rischio nel caso in cui l'ID della chiave di accesso e la chiave di accesso segreta vengano 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 chiavi. Se in seguito decidi di creare nuove chiavi, elimina manualmente quelle vecchie.

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 quell'utente in Tenant Manager.

Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruotare regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

## Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Seleziona l'utente di cui desideri gestire le chiavi di accesso S3.

Viene visualizzata la pagina dei dettagli dell'utente.

3. Selezionare **Chiavi di accesso**, quindi selezionare **Crea chiave**.
4. Eseguire 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 corrente. L'orario di scadenza può essere di almeno un minuto rispetto all'orario corrente.

5. Seleziona **Crea chiave di accesso**.

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

6. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di 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 è possibile copiare o scaricare le chiavi dopo aver chiuso la finestra di dialogo.

7. Selezionare **Fine**.

La nuova chiave è elencata nella scheda Chiavi di accesso della pagina dei dettagli dell'utente.

8. Se il tuo account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, puoi facoltativamente utilizzare l'API di gestione tenant per clonare manualmente le chiavi di accesso S3 dal tenant sulla griglia di origine al tenant sulla griglia di destinazione. Vedere "["Clona le chiavi di accesso S3 utilizzando l'API"](#)" .

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

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

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Tu 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 quell'utente in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruotare regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

### Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Dalla pagina Utenti, seleziona l'utente di cui desideri visualizzare le chiavi di accesso S3.
3. Dalla pagina Dettagli utente, seleziona **Chiavi di accesso**.
4. Ordina le chiavi in base a **Data di scadenza o ID chiave di accesso**.
5. Se necessario, crea nuove chiavi ed elimina manualmente quelle che non sono più in uso.

Se si creano nuove chiavi prima che quelle esistenti scadano, l'utente può iniziare a utilizzare 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

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le chiavi di accesso S3 di un altro utente. Dopo aver eliminato una chiave di accesso, non sarà più possibile utilizzarla per accedere agli oggetti e ai bucket nell'account tenant.

#### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Tu 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 quell'utente in Tenant Manager. Per questo motivo, proteggi le chiavi di accesso come faresti con una password. Ruotare regolarmente le chiavi di accesso, rimuovere dall'account quelle non utilizzate e non condividerle mai con altri utenti.

#### Passi

1. Selezionare **GESTIONE ACCESSI > Utenti**.
2. Dalla pagina Utenti, seleziona l'utente di cui desideri gestire le chiavi di accesso S3.
3. Dalla pagina Dettagli utente, seleziona **Chiavi di accesso**, quindi seleziona la casella di controllo per ogni chiave di accesso che desideri eliminare.
4. Selezionare **Azioni > Elimina chiave selezionata**.
5. Nella finestra di dialogo di conferma, seleziona **Elimina chiave**.

Nell'angolo in alto a destra della pagina appare un messaggio di conferma.

## Gestisci i bucket S3

## Crea un bucket S3

È possibile utilizzare Tenant Manager per creare bucket S3 per i dati degli oggetti.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha accesso Root o Gestisci tutti i bucket "[permesso](#)" . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.



Le autorizzazioni per impostare o modificare le proprietà di blocco degli oggetti S3 di bucket o oggetti possono essere concesse da "[criterio bucket o criterio di gruppo](#)" .

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



Ogni griglia può avere un massimo di 100.000 bucket.

### Accedi alla procedura guidata

#### Passi

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

### Inserisci i dettagli

#### Passi

1. Inserisci i dettagli per il bucket.

Campo	Descrizione
Nome del bucket	<p>Un nome per il bucket che rispetti queste regole:</p> <ul style="list-style-type: none"><li>• Deve essere univoco in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).</li><li>• Deve essere conforme al DNS.</li><li>• Deve contenere almeno 3 e non più di 63 caratteri.</li><li>• Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può contenere solo lettere minuscole, numeri e trattini.</li><li>• Non devono contenere punti nelle richieste in stile ospitato virtuale. I punti causeranno problemi con la verifica dei certificati jolly del server.</li></ul> <p>Per maggiori informazioni, vedere il "<a href="#">"Documentazione di Amazon Web Services (AWS) sulle regole di denominazione dei bucket"</a>" .</p> <p><b>Nota:</b> non è possibile modificare il nome del bucket dopo averlo creato.</p>

Campo	Descrizione
Regione	<p>La regione del bucket.</p> <p>L'amministratore StorageGRID gestisce le regioni disponibili. La regione di un bucket può influire sulla politica di protezione dei dati applicata agli oggetti. Per impostazione predefinita, tutti i bucket vengono creati in <code>us-east-1</code> regione.</p> <p><b>Nota:</b> non è possibile modificare la regione dopo aver creato il bucket.</p>

## 2. Selezionare **Continua**.

### Gestisci le impostazioni

#### Passi

1. Facoltativamente, abilitare il controllo delle versioni degli oggetti per il bucket.

Abilita il controllo delle versioni degli oggetti se vuoi archiviare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto, se necessario. È necessario abilitare il controllo delle versioni degli oggetti se il bucket verrà utilizzato per la replica tra griglie.

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

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



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

Se si abilita S3 Object Lock per un bucket, il controllo delle versioni del bucket viene abilitato automaticamente.

3. Se hai selezionato **Abilita blocco oggetto S3**, abilita facoltativamente **Conservazione predefinita** per questo bucket.



L'amministratore della rete deve darti l'autorizzazione a "utilizzare le funzionalità specifiche di S3 Object Lock".

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

- a. Se è abilitata la **Conservazione predefinita**, specificare una **Modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Governance	<ul style="list-style-type: none"> <li>Utenti con il <code>s3:BypassGovernanceRetention</code> il permesso può utilizzare il <code>x-amz-bypass-governance-retention: true</code> intestazione della richiesta per ignorare le impostazioni di conservazione.</li> <li>Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.</li> <li>Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.</li> </ul>
Conformità	<ul style="list-style-type: none"> <li>L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.</li> <li>La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.</li> <li>La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.</li> </ul> <p><b>Nota:</b> l'amministratore della rete deve consentirti di utilizzare la modalità di conformità.</p>

- b. Se è abilitata l'opzione **Conservazione predefinita**, specificare 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. Specificare un valore inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

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

4. Facoltativamente, seleziona **Abilita limite 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 su disco).

Se non viene impostato alcun limite, la capacità di questo bucket è illimitata. Fare riferimento a "[Utilizzo del limite di capacità](#)" per maggiori informazioni.

5. Seleziona **Crea bucket**.

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

6. Facoltativamente, seleziona **Vai alla pagina dei dettagli del bucket** per "[visualizza i dettagli del bucket](#)" ed eseguire configurazioni aggiuntive.

## Visualizza i dettagli del bucket

Puoi visualizzare i bucket nel tuo account tenant.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Accesso root, autorizzazione Gestisci tutti i bucket o Visualizza tutti i bucket](#)" . Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

### Passi

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

Viene visualizzata la pagina Bucket.

2. Esaminare la tabella riepilogativa per ogni bucket.

A seconda delle necessità, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco avanti e indietro.



I valori visualizzati per Conteggio oggetti, Spazio utilizzato e Utilizzo sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo. Se nei bucket è abilitato il controllo delle versioni, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

#### Nome

Nome univoco del bucket, che non può essere modificato.

#### Funzionalità abilitate

Elenco delle funzionalità abilitate per il bucket.

#### Blocco oggetto S3

Se il blocco oggetti S3 è abilitato per il bucket.

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

#### Regione

La regione del bucket, che non può essere modificata. Per impostazione predefinita, questa colonna è nascosta.

#### Conteggio degli oggetti

Il numero di oggetti in questo bucket. Se nei bucket è abilitato il controllo delle versioni, le versioni degli oggetti non correnti vengono incluse in questo valore.

Quando si aggiungono o si eliminano 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 codificate per cancellazione o per i metadati degli oggetti.

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

## Utilizzo

Percentuale utilizzata del limite di capacità del bucket, se ne è stato impostato uno.

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

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

## Capacità

Se impostato, il limite di capacità per il bucket.

## Data di creazione

Data e ora di creazione del bucket. Per impostazione predefinita, questa colonna è nascosta.

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

Prestare molta attenzione alle avvertenze che compaiono quando si seleziona ciascuna di queste opzioni. Per maggiori informazioni, fare riferimento a:



- ["Elimina tutti gli oggetti in un bucket"](#)
- ["Elimina un bucket"](#) (il secchio deve essere vuoto)

- d. Visualizza o modifica le impostazioni per il bucket in ciascuna scheda, secondo necessità.
  - **Console S3:** visualizza gli oggetti per il bucket. Per ulteriori informazioni, fare riferimento a ["Utilizzare la console S3"](#).
  - **Opzioni bucket:** visualizza o modifica le impostazioni delle opzioni. Alcune impostazioni, come S3 Object Lock, non possono essere modificate dopo la creazione del bucket.
    - ["Gestire la coerenza del bucket"](#)
    - ["Aggiornamenti dell'ultimo orario di accesso"](#)
    - ["Limite di capacità"](#)
    - ["Versionamento degli oggetti"](#)
    - ["Blocco oggetto S3"](#)
    - ["Conservazione predefinita del bucket"](#)
    - ["Gestire la replicazione tra griglie"](#) (se consentito all'inquilino)
  - **Servizi di piattaforma:** ["Gestire i servizi della piattaforma"](#) (se consentito all'inquilino)

- **Accesso bucket:** visualizza o modifica le impostazioni delle opzioni. È necessario disporre di autorizzazioni di accesso specifiche.
  - Configurare "[Condivisione delle risorse tra origini \(CORS\)](#)" in modo che il bucket e gli oggetti al suo interno siano accessibili alle applicazioni web in altri domini.
  - "[Controlla l'accesso degli utenti](#)" per un bucket S3 e gli oggetti in quel bucket.

## Applicare un tag di policy ILM a un bucket

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

La policy ILM controlla dove vengono archiviati i dati dell'oggetto e se vengono eliminati dopo un determinato periodo di tempo. L'amministratore della griglia crea criteri ILM e li assegna ai tag dei criteri ILM quando si utilizzano più criteri attivi.



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

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Accesso root, autorizzazione Gestisci tutti i bucket o Visualizza tutti i bucket](#)" . Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

### Passi

#### 1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.

Viene visualizzata la pagina Bucket. A seconda delle necessità, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco avanti e indietro.

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

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



I valori visualizzati per il conteggio degli oggetti e lo spazio utilizzato sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo. Se nel bucket è abilitato il controllo delle versioni, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

#### 3. Nella scheda Opzioni bucket, espandere l'accordion tag policy ILM. Questa fisarmonica viene visualizzata solo se l'amministratore della griglia ha abilitato l'uso di tag di policy personalizzati.

#### 4. Leggere la descrizione di ciascun tag di policy per determinare quale tag applicare al bucket.



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

#### 5. Selezionare il pulsante di opzione per il tag che si desidera assegnare al bucket.

6. Seleziona **Salva modifiche**. Un nuovo tag bucket S3 verrà impostato sul bucket con la chiave NTAP-SG-ILM-BUCKET-TAG e il valore del nome del tag della policy ILM.



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



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



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 i criteri del bucket

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

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Permesso di accesso root](#)" . Le autorizzazioni Visualizza tutti i bucket e Gestisci tutti i bucket consentono solo la visualizzazione.
- Hai verificato che sia disponibile il numero richiesto di nodi di archiviazione e siti. Se due o più nodi di archiviazione non sono disponibili in nessun sito, oppure se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

### Passi

1. Seleziona **Bucket**, quindi seleziona il bucket che desideri gestire.
2. Nella pagina dei dettagli del bucket, seleziona **Accesso al bucket > Criterio bucket**.
3. Eseguire una delle seguenti operazioni:
  - Immettere un criterio di bucket selezionando la casella di controllo **Abilita criterio**. Quindi inserisci una stringa valida in formato JSON.

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

- Modificare una policy esistente modificando la stringa.
- Disattivare un criterio deselezionando **Abilita criterio**.

Per informazioni dettagliate sulle policy dei bucket, inclusa la sintassi del linguaggio e gli esempi, vedere "[Criteri di esempio per i bucket](#)" .

## Gestire la coerenza del bucket

I valori di coerenza possono essere utilizzati per specificare la disponibilità delle modifiche alle impostazioni del bucket, nonché per fornire un equilibrio tra la disponibilità degli oggetti all'interno di un bucket e la coerenza di tali oggetti tra diversi nodi di archiviazione e siti. È possibile modificare i valori di coerenza in modo che siano diversi

dai valori predefiniti, in modo che le applicazioni client possano soddisfare le proprie esigenze operative.

## Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Gestisci tutti i bucket o l'autorizzazione di accesso Root](#)" . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

## Linee guida sulla coerenza del bucket

La coerenza del bucket viene utilizzata per determinare la coerenza delle applicazioni client che interessano gli oggetti all'interno di quel bucket S3. In generale, dovresti usare la coerenza **Lettura dopo nuova scrittura** per i tuoi bucket.

### Modifica la coerenza del bucket

Se la coerenza **Read-after-new-write** non soddisfa i requisiti dell'applicazione client, è possibile modificarla impostando la coerenza del bucket o utilizzando `Consistency-Control` intestazione. Il `Consistency-Control` l'intestazione sovrascrive la coerenza del bucket.



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

### Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
  2. Selezionare il nome del bucket dalla tabella.
- Viene visualizzata la pagina dei dettagli del bucket.
3. Dalla scheda **Opzioni bucket**, seleziona la fisarmonica \*\*.
  4. Selezionare una coerenza per le operazioni eseguite sugli oggetti in questo bucket.
    - **Tutti**: fornisce il massimo livello di coerenza. Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
    - **Strong-global**: garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti.
    - **Strong-site**: garantisce la coerenza di lettura e scrittura per tutte le richieste client all'interno di un sito.
    - **Lettura dopo nuova scrittura** (predefinito): fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e 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, utilizzare 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 inesistenti). Non supportato per i bucket S3 FabricPool .
  5. Seleziona **Salva modifiche**.

## Cosa succede quando si modificano le impostazioni del bucket

I bucket hanno più impostazioni che influenzano il comportamento dei bucket stessi e degli oggetti al loro interno.

Le seguenti impostazioni del bucket utilizzano per impostazione predefinita la coerenza **forte**. Se due o più nodi di archiviazione non sono disponibili in nessun sito, oppure se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

- ["Eliminazione del bucket vuoto in background"](#)
- ["Ultimo orario di accesso"](#)
- ["Ciclo di vita del bucket"](#)
- ["Politica del bucket"](#)
- ["Etichettatura del secchio"](#)
- ["Versionamento del bucket"](#)
- ["Blocco oggetto S3"](#)
- ["Crittografia del bucket"](#)



Il valore di coerenza per il controllo delle versioni 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 del bucket non utilizzano una coerenza elevata e hanno una maggiore disponibilità per le modifiche. Le modifiche a queste impostazioni potrebbero richiedere del tempo prima di avere effetto.

- ["Configurazione dei servizi della piattaforma: integrazione di notifica, replica o ricerca"](#)
- ["Configurazione CORS"](#)
- [Modifica la coerenza del bucket](#)



Se la coerenza predefinita utilizzata durante la modifica delle impostazioni del bucket non soddisfa i requisiti dell'applicazione client, è possibile modificare la coerenza utilizzando `Consistency-Control` intestazione per il "["API REST S3"](#)" oppure utilizzando il `reducedConsistency` o `force` opzioni nel "["API di gestione degli inquilini"](#)" .

## Abilita o disabilita gli aggiornamenti dell'ultimo orario di accesso

Quando gli amministratori della griglia creano le regole di gestione del ciclo di vita delle informazioni (ILM) per un sistema StorageGRID, possono facoltativamente specificare che l'orario dell'ultimo accesso a un oggetto venga utilizzato per determinare se spostare tale oggetto in una posizione di archiviazione diversa. Se si utilizza un tenant S3, è possibile sfruttare tali 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 orario di accesso** come filtro avanzato o come orario di riferimento. Se il sistema StorageGRID non include tale regola, è possibile ignorare queste istruzioni. Vedere "["Utilizzare l'orario dell'ultimo accesso nelle regole ILM"](#)" per i dettagli.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "["browser web supportato"](#)" .
- Appartieni a un gruppo di utenti che ha il "["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#)" . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

## Informazioni su questo compito

**Ultimo orario di accesso** è una delle opzioni disponibili per l'istruzione di posizionamento **Ora di riferimento** per una regola ILM. Impostando l'Ora di riferimento per una regola su Ora ultimo accesso, gli amministratori della griglia possono specificare che gli oggetti vengano posizionati in determinate posizioni di archiviazione in base all'ultima volta in cui tali oggetti sono stati recuperati (letti o visualizzati).

Ad esempio, per garantire che gli oggetti visualizzati di recente rimangano in un archivio più veloce, un amministratore di griglia può creare una regola ILM che specifichi quanto segue:

- Gli oggetti recuperati nel mese precedente devono rimanere sui nodi di archiviazione locali.
- Gli oggetti che non sono stati recuperati nel mese precedente devono essere spostati in un luogo esterno.

Per impostazione predefinita, gli aggiornamenti all'orario dell'ultimo accesso sono disabilitati. Se il sistema StorageGRID include una regola ILM che utilizza l'opzione **Ultimo orario di accesso** e si desidera che questa opzione venga applicata agli oggetti in questo bucket, è necessario abilitare gli aggiornamenti all'ultimo orario di accesso per i bucket S3 specificati in tale regola.



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

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

- Aggiorna gli oggetti con nuovi timestamp
- Aggiungere gli oggetti alla coda ILM, in modo che possano essere rivalutati in base alle attuali regole e policy ILM

La tabella riepiloga il comportamento applicato a tutti gli oggetti nel bucket quando l'orario dell'ultimo accesso è disabilitato o abilitato.

Tipo di richiesta	Comportamento se l'ultimo orario di accesso è disabilitato (predefinito)		Comportamento se l'ultimo orario di accesso è abilitato	
	Ultimo orario di accesso aggiornato?	Oggetto aggiunto alla coda di valutazione ILM?	Ultimo orario di accesso aggiornato?	Oggetto aggiunto alla coda di valutazione ILM?
Richiesta di recupero di un oggetto, del suo elenco di controllo di accesso o dei suoi 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 all'altro	<ul style="list-style-type: none"> <li>• No, per la copia sorgente</li> <li>• Sì, per la copia di destinazione</li> </ul>	<ul style="list-style-type: none"> <li>• No, per la copia sorgente</li> <li>• Sì, per la copia di destinazione</li> </ul>	<ul style="list-style-type: none"> <li>• Sì, per la copia sorgente</li> <li>• Sì, per la copia di destinazione</li> </ul>	<ul style="list-style-type: none"> <li>• Sì, per la copia sorgente</li> <li>• Sì, per la copia di destinazione</li> </ul>
Richiesta di completamento di un caricamento multiparte	Sì, per l'oggetto assemblato			

### Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
  2. Selezionare il nome del bucket dalla tabella.
- Viene visualizzata la pagina dei dettagli del bucket.
3. Dalla scheda **Opzioni bucket**, seleziona la voce accordian **Aggiornamenti ora ultimo accesso**.
  4. Abilita o disabilita gli aggiornamenti dell'orario dell'ultimo accesso.
  5. Seleziona **Salva modifiche**.

## Modificare il controllo delle versioni degli oggetti per un bucket

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

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Gestisci tutti i bucket o l'autorizzazione di accesso Root](#)" . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- Hai verificato che sia disponibile il numero richiesto di nodi di archiviazione e siti. Se due o più nodi di archiviazione non sono disponibili in nessun sito, oppure se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

### Informazioni su questo compito

È possibile abilitare o sospendere il controllo delle versioni degli oggetti per un bucket. Dopo aver abilitato il controllo delle versioni per un bucket, questo non può tornare a uno stato senza controllo delle versioni. Tuttavia, è possibile sospendere il controllo delle versioni per il bucket.

- Disabilitato: il controllo delle versioni non è mai stato abilitato
- Abilitato: il controllo delle versioni è abilitato
- Sospeso: il controllo delle versioni era precedentemente abilitato ed è sospeso

Per ulteriori informazioni, vedere quanto segue:

- "Versionamento degli oggetti"
- "Regole e policy ILM per oggetti con versione S3 (esempio 4)"
- "Come vengono eliminati gli oggetti"

## Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
  2. Selezionare il nome del bucket dalla tabella.
- Viene visualizzata la pagina dei dettagli del bucket.
3. Dalla scheda **Opzioni bucket**, seleziona la voce accordian **Versionamento oggetto**.
  4. Seleziona uno stato di controllo delle versioni per gli oggetti in questo bucket.

Il controllo delle versioni degli oggetti deve rimanere abilitato per un bucket utilizzato per la replica tra griglie. Se è abilitato il blocco degli oggetti S3 o la conformità legacy, le opzioni di **Versioning degli oggetti** sono disabilitate.

Opzione	Descrizione
Abilita il controllo delle versioni	<p>Abilita il controllo delle versioni degli oggetti se vuoi archiviare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto, se necessario.</p> <p>Gli oggetti già presenti nel bucket verranno sottoposti a versioning quando vengono modificati da un utente.</p>
Sospendi il controllo delle versioni	Sospendi il controllo delle versioni degli oggetti se non desideri più che vengano create nuove versioni degli oggetti. È ancora possibile recuperare tutte le versioni esistenti dell'oggetto.

5. Seleziona **Salva modifiche**.

## Utilizzare S3 Object Lock per conservare gli oggetti

È possibile utilizzare S3 Object Lock se i bucket e gli oggetti devono essere conformi ai requisiti normativi per la conservazione.



L'amministratore della griglia deve concederti l'autorizzazione per utilizzare 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 account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se in un bucket è abilitato S3 Object Lock, è necessario il controllo delle versioni del bucket, che 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 e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

**Un bucket con S3 Object Lock e conservazione predefinita configurata** può contenere 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.

Di fatto, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurata la conservazione predefinita. Gli oggetti esistenti senza impostazioni di conservazione degli oggetti rimangono inalterati.

#### Modalità di conservazione

La funzionalità StorageGRID S3 Object Lock 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 finché non viene raggiunta la data di conservazione.
  - La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità di 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.
  - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

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

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

- **Modalità di conservazione:** conformità o governance.
- **Retain-until-date:** se la retain-until-date di una versione di un oggetto è futura, l'oggetto può essere recuperato, ma non eliminato.
- **Sospensione legale:** l'applicazione di una sospensione legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di scadenza, ma rimane in vigore finché non viene rimossa esplicitamente. Le sospensioni legali sono indipendenti dalla data di conservazione fino alla data di scadenza.



Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

Per i dettagli sulle impostazioni dell'oggetto, vedere "[Utilizzare l'API REST S3 per configurare S3 Object Lock](#)".

## Impostazione di conservazione predefinita per i bucket

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

- **Modalità di conservazione predefinita:** conformità o governance.
- **Periodo di conservazione predefinito:** per quanto tempo devono essere conservate le nuove versioni degli oggetti aggiunte a questo bucket, a partire dal giorno in cui vengono aggiunte.

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

Vedere "[Crea un bucket S3](#)" E "[Aggiorna la conservazione predefinita del blocco degli oggetti S3](#)".

## Attività di blocco degli oggetti S3

Gli elenchi seguenti per gli amministratori della griglia e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzionalità S3 Object Lock.

### Amministratore di rete

- Abilita l'impostazione globale di blocco degli oggetti S3 per l'intero sistema StorageGRID .
- Garantire che le politiche di gestione del ciclo di vita delle informazioni (ILM) siano *conformi*; ovvero, che soddisfino i "[requisiti dei bucket con S3 Object Lock abilitato](#)".
- Se necessario, consentire a un tenant di utilizzare Conformità come modalità di conservazione. In caso contrario, è consentita solo la modalità Governance.
- Se necessario, impostare un periodo massimo di conservazione per un tenant.

### Utente inquilino

- Esaminare le considerazioni relative a bucket e oggetti con S3 Object Lock.
- Se necessario, contattare l'amministratore della griglia per abilitare l'impostazione globale di blocco degli oggetti S3 e impostare le autorizzazioni.
- Crea bucket con S3 Object Lock abilitato.
- Facoltativamente, configura le impostazioni di conservazione predefinite per un bucket:
  - Modalità di conservazione predefinita: Governance o Conformità, se consentita dall'amministratore della rete.
  - Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall'amministratore della griglia.
- Utilizzare l'applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica dell'oggetto:
  - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore della rete.
  - Conserva fino alla data: deve essere inferiore o uguale a quanto consentito dal 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 , è possibile utilizzare Tenant Manager, Tenant Management API o S3 REST API per creare bucket con S3 Object Lock abilitato.

- Se si prevede di utilizzare S3 Object Lock, è necessario abilitarlo quando si crea il bucket. Non è possibile abilitare S3 Object Lock per un bucket esistente.
- Quando S3 Object Lock è abilitato per un bucket, StorageGRID abilita automaticamente il controllo delle versioni per quel bucket. Non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione predefinita e un periodo di conservazione per ciascun bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di impostazioni di conservazione proprie. È possibile ignorare queste impostazioni predefinite specificando una modalità di conservazione e una data di conservazione per ogni versione dell'oggetto quando viene caricata.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con S3 Object Lock abilitato.
- La replica CloudMirror 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 dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure specificare le impostazioni di conservazione per ciascuna versione dell'oggetto. Le impostazioni di conservazione a livello di oggetto possono essere specificate tramite l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni degli oggetti. Una versione di un oggetto può avere sia un'impostazione di conservazione fino alla data di scadenza che un'impostazione di conservazione legale, una ma non l'altra, oppure nessuna delle due. Specificando un'impostazione di conservazione fino a data o di conservazione legale per un oggetto, si protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

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

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

### 1. Ingestione di oggetti

Quando una versione di un oggetto viene aggiunta a un bucket in cui è abilitato il blocco degli oggetti S3, le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte 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 presenti.
- 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, vengono protetti sia l'oggetto sia tutti i metadati S3 definiti dall'utente.

### 2. Conservazione ed eliminazione degli oggetti

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

- Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

## Posso continuare a gestire i bucket Compliant legacy?

La funzionalità S3 Object Lock sostituisce la funzionalità Compliance disponibile nelle versioni precedenti 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, vedere [https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Hybrid\\_Cloud\\_Infrastructure/StorageGRID/How\\_to\\_manage\\_legacy\\_Compliant\\_buckets\\_in\\_StorageGRID\\_11.5](https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5) [“Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5”].

## Aggiorna la conservazione predefinita del blocco degli oggetti S3

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

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Gestisci tutti i bucket o l'autorizzazione di accesso Root](#)" . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- S3 Object Lock è abilitato a livello globale per il sistema StorageGRID e hai abilitato S3 Object Lock quando hai creato il bucket. Vedere "[Utilizzare S3 Object Lock per conservare gli oggetti](#)" .

### Passi

1. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
  2. Selezionare il nome del bucket dalla tabella.
- Viene visualizzata la pagina dei dettagli del bucket.
3. Dalla scheda **Opzioni bucket**, seleziona la voce accordione **Blocco oggetto S3**.
  4. Facoltativamente, abilita o disabilita la **Conservazione predefinita** per questo bucket.

Le modifiche a questa impostazione non si applicano agli oggetti già presenti nel bucket o a quelli che potrebbero avere periodi di conservazione propri.

5. Se è abilitata la **Conservazione predefinita**, specificare una **Modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Governance	<ul style="list-style-type: none"> <li>• Utenti con il <code>s3:BypassGovernanceRetention</code> il permesso può utilizzare il <code>x-amz-bypass-governance-retention: true</code> intestazione della richiesta per ignorare le impostazioni di conservazione.</li> <li>• Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.</li> <li>• Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.</li> </ul>
Conformità	<ul style="list-style-type: none"> <li>• L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.</li> <li>• La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.</li> <li>• La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.</li> </ul> <p><b>Nota:</b> l'amministratore della rete deve consentirti di utilizzare la modalità di conformità.</p>

6. Se è abilitata l'opzione **Conservazione predefinita**, specificare 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. Specificare un valore inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

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

7. Seleziona **Salva modifiche**.

## Configurare la condivisione delle risorse tra origini (CORS)

È possibile configurare la condivisione delle risorse tra origini (CORS) per un bucket S3 se si desidera che il bucket e gli oggetti in esso contenuti siano accessibili alle applicazioni Web in altri domini.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Per le richieste di configurazione GET CORS, appartieni a un gruppo di utenti che ha "[Autorizzazione Gestisci tutti i bucket o Visualizza tutti i bucket](#)" . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- Per le richieste di configurazione PUT CORS, appartieni a un gruppo di utenti che ha "[Gestisci tutti i](#)

permessi dei bucket". Questa autorizzazione sostituisce le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

- IL "Permesso di accesso root" fornisce l'accesso a tutte le richieste di configurazione CORS.

## Informazioni su questo compito

La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni web client in un dominio di accedere alle risorse in un dominio diverso. Ad esempio, supponiamo di utilizzare un bucket S3 denominato Images per memorizzare la grafica. Configurando CORS per il Images bucket, puoi consentire che le immagini in quel bucket vengano visualizzate sul sito web <http://www.example.com>.

### Abilita CORS per un bucket

#### Passi

1. Utilizzare un editor di testo per creare il file XML richiesto. 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
  - Permette solo il <http://www.example.com> dominio per 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 sull'XML di configurazione CORS, vedere ["Documentazione di Amazon Web Services \(AWS\): Guida per l'utente di Amazon Simple Storage Service"](#).

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

Viene visualizzata la pagina dei dettagli del bucket.

4. Dalla scheda **Accesso bucket**, seleziona l'accordian **Condivisione risorse tra origini (CORS)**.
5. Selezionare la casella di controllo **Abilita CORS**.
6. Incollare il file XML di configurazione CORS nella casella di testo.

## 7. Seleziona **Salva modifiche**.

### Modificare l'impostazione CORS

#### Passi

1. Aggiornare l'XML di configurazione CORS nella casella di testo oppure selezionare **Cancella** per ricominciare.
2. Seleziona **Salva modifiche**.

### Disabilita l'impostazione CORS

#### Passi

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

### Elimina gli oggetti nel bucket

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

#### Considerazioni e requisiti

Prima di eseguire questi passaggi, tenere presente quanto segue:

- Quando si eliminano gli oggetti in un bucket, StorageGRID rimuove definitivamente tutti gli oggetti e tutte le versioni degli oggetti in ciascun bucket selezionato da tutti i nodi e siti nel sistema StorageGRID. StorageGRID rimuove anche tutti i metadati degli oggetti correlati. Non sarà possibile recuperare queste informazioni.
- L'eliminazione di tutti gli oggetti in un bucket potrebbe richiedere minuti, giorni o addirittura settimane, a seconda del numero di oggetti, delle copie degli oggetti e delle operazioni simultanee.
- Se un secchio 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** finché non verrà raggiunta la data di conservazione per tutti gli oggetti e non verranno rimossi eventuali blocchi legali.

- Durante l'eliminazione degli oggetti, lo stato del bucket è **Eliminazione oggetti: sola lettura**. In questo stato non è possibile 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 scrittura e riutilizzalo per nuovi oggetti
  - Elimina il bucket
  - Mantieni il bucket in modalità di sola lettura per riservarne il nome per un uso futuro
- Se in un bucket è abilitato il controllo delle versioni degli oggetti, è possibile rimuovere i marcatori di eliminazione creati in StorageGRID 11.8 o versioni successive utilizzando le operazioni Elimina oggetti nel bucket.
- Se in un bucket è abilitato il controllo delle versioni degli oggetti, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11.7 o versioni precedenti. Visualizza le informazioni sull'eliminazione degli oggetti in un bucket in "[Come vengono eliminati gli oggetti con versione](#)

S3" .

- Se usi "replicazione cross-grid" , notare quanto segue:
  - Utilizzando questa opzione non si elimina alcun oggetto dal bucket sull'altra griglia.
  - 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 aggiungerà oggetti al contenitore sull'altra griglia, "disabilitare la replicazione tra griglie" per quel bucket prima di eliminare tutti gli oggetti bucket.

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "browser web supportato" .
- Appartieni a un gruppo di utenti che ha il "Permesso di accesso root" . Questa autorizzazione sostituisce le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.

### Passi

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

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

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

#### Menu 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, rivedere i dettagli, immettere **Sì** e selezionare **OK**.
4. Attendi che l'operazione di eliminazione abbia inizio.

Dopo qualche minuto:

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

## my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

[View bucket contents in Experimental S3 Console](#) 

[Delete bucket](#)

 **All bucket objects are being deleted**

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

[Stop deleting objects](#)

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

Quando selezioni **Interrompi eliminazione oggetti**, il bucket torna in modalità scrittura; tuttavia, non puoi accedere o ripristinare gli oggetti che sono stati eliminati.

6. Attendere il completamento dell'operazione.

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

## my-bucket (read-only)

Region: us-east-1  
 Date created: 2022-12-14 10:09:50 MST  
 Object count: 0

[View bucket contents in Experimental S3 Console](#) 

[Delete bucket](#)

 Bucket is empty but is still read-only.

This bucket is now empty.

- To remove this bucket, select **Delete bucket**.
- To return this bucket to write mode so it can be reused, select **Stop deleting objects**.

[Stop deleting objects](#)

### 7. Eseguire 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 del bucket per un utilizzo futuro.
- Elimina il bucket. È possibile selezionare **Elimina bucket** per eliminare un singolo bucket oppure tornare alla pagina Bucket e selezionare **Azioni** > **Elimina bucket** per rimuovere più di un bucket.



Se non riesci a eliminare un bucket con versione dopo aver eliminato tutti gli oggetti, i marcatori di eliminazione potrebbero rimanere. Per eliminare il bucket, è necessario rimuovere tutti i marcatori di eliminazione rimanenti.

- Riporta il bucket in modalità scrittura e, facoltativamente, riutilizzalo per nuovi oggetti. È possibile selezionare **Interrompi eliminazione oggetti** per un singolo bucket oppure tornare alla pagina Bucket e selezionare **Azione** > **Interrompi eliminazione oggetti** per più di un bucket.

## Elimina bucket S3

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

### Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Appartieni a un gruppo di utenti che ha il "[Gestisci tutti i bucket o l'autorizzazione di accesso Root](#)" . Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- I bucket che vuoi eliminare sono vuoti. Se i bucket che vuoi eliminare *non* sono vuoti, "[elimina gli oggetti dal bucket](#)" .

### Informazioni su questo compito

Queste istruzioni descrivono come eliminare un bucket S3 utilizzando Tenant Manager. È anche possibile eliminare i bucket S3 utilizzando "[API di gestione degli inquilini](#)" o il "[API REST S3](#)" .

Non è possibile eliminare un bucket S3 se contiene oggetti, versioni di oggetti non correnti o marcatori di eliminazione. Per informazioni su come vengono eliminati gli oggetti con versione S3, vedere "[Come vengono eliminati gli oggetti](#)".

## Passi

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

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

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

### Menu Azioni

- a. Seleziona la casella di controllo per ogni bucket che desideri eliminare.
- b. Selezionare **Azioni > Elimina bucket**.

### Pagina dei dettagli

- a. Seleziona il nome di un bucket per visualizzarne i dettagli.
- b. Seleziona **Elimina bucket**.

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

StorageGRID conferma che ogni bucket è vuoto e quindi lo elimina. 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.

## Utilizzare la console S3

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

S3 Console ti consente di:

- Carica, scarica, rinomina, copia, sposta ed elimina oggetti
- Visualizza, ripristina, scarica ed elimina le versioni degli oggetti
- Cerca oggetti per prefisso
- Gestisci i tag degli oggetti
- Visualizza i metadati dell'oggetto
- Visualizza, crea, rinomina, copia, sposta ed elimina cartelle

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



Se l'utilizzo di S3 Console fa sì che le operazioni richiedano troppo tempo (ad esempio, minuti o ore), prendere in considerazione quanto segue:

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

## Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un "[browser web supportato](#)" .
- Se vuoi gestire gli oggetti, devi appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso Root. In alternativa, puoi appartenere a un gruppo di utenti che dispone dell'autorizzazione Utilizza la scheda Console S3 e dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket. Vedere "[Autorizzazioni di gestione degli inquilini](#)" .
- Per l'utente è stato configurato un criterio di gruppo o bucket S3. Vedere "[Utilizzare criteri di accesso a 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 delle chiavi di accesso](#)" .

## Passi

1. Selezionare **ARCHIVIAZIONE > Bucket > nome bucket**.
2. Selezionare 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 \* Sign in\*.
5. Viene visualizzata la tabella degli oggetti bucket. Puoi gestire gli oggetti in base alle tue esigenze.

## Informazioni aggiuntive

- **Cerca per prefisso:** la funzione di ricerca per prefisso cerca solo gli oggetti che iniziano con una parola specifica relativa alla cartella corrente. La ricerca non include gli 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 di folder1/folder2/ cartella e inizia con la parola somefile- .
- **Trascinamento della selezione:** puoi trascinare e rilasciare i file dal file manager del tuo computer a S3 Console. Tuttavia, non è possibile caricare cartelle.
- **Operazioni sulle cartelle:** quando si sposta, si copia o si rinomina una cartella, tutti gli oggetti al suo interno vengono aggiornati uno alla volta, il che potrebbe richiedere del tempo.
- **Eliminazione definitiva quando il controllo delle versioni del bucket è disabilitato:** quando si sovrascrive o si elimina un oggetto in un bucket con il controllo delle versioni disabilitato, l'operazione è definitiva. Vedere "[Modificare il controllo delle versioni degli oggetti per un bucket](#)" .

# Gestire i servizi della piattaforma S3

## Servizi della piattaforma S3

### Panoramica e considerazioni sui servizi della piattaforma

Prima di implementare i servizi della piattaforma, rivedere la panoramica e le considerazioni sull'utilizzo di questi servizi.

Per informazioni su S3, vedere "[Utilizzare l'API REST S3](#)" .

### Panoramica dei servizi della piattaforma

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

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

Per un singolo bucket S3 è possibile configurare qualsiasi combinazione di servizi di piattaforma. Ad esempio, è possibile configurare entrambi l'["Servizio CloudMirror"](#) E ["notifiche"](#) su un bucket StorageGRID S3 in modo da poter eseguire il mirroring di oggetti specifici su Amazon Simple Storage Service (S3), inviando al contempo una notifica su 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 ciascun account tenant da un amministratore StorageGRID tramite Grid Manager o Grid Management API.

### Come sono configurati i servizi della piattaforma

I servizi della piattaforma comunicano con endpoint esterni configurati tramite "[Responsabile degli inquilini](#)" o il "[API di gestione degli inquilini](#)" . Ogni endpoint rappresenta una destinazione esterna, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento Amazon SNS 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.

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

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

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

Servizio di piattaforma	API REST S3	Fare riferimento a
Replica CloudMirror	<ul style="list-style-type: none"> <li>OttieniReplicazioneBucket</li> <li>PutBucketReplication</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">"Replica CloudMirror"</a></li> <li><a href="#">"Operazioni sui bucket"</a></li> </ul>
Notifiche	<ul style="list-style-type: none"> <li>Configurazione di notifica di GetBucket</li> <li>Configurazione della notifica PutBucket</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">"Notifiche"</a></li> <li><a href="#">"Operazioni sui bucket"</a></li> </ul>
Integrazione della ricerca	<ul style="list-style-type: none"> <li>Configurazione della notifica dei metadati del bucket GET</li> <li>Configurazione della notifica dei metadati del bucket PUT</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">"Integrazione della ricerca"</a></li> <li><a href="#">"Operazioni personalizzate StorageGRID"</a></li> </ul>

#### Considerazioni sull'utilizzo dei servizi della piattaforma

Considerazione	Dettagli
Monitoraggio dell'endpoint di destinazione	<p>È necessario monitorare la disponibilità di ciascun endpoint di destinazione. Se la connettività all'endpoint di destinazione viene persa per un periodo di tempo prolungato e si verifica un arretrato di richieste elevato, le richieste client aggiuntive (ad esempio le richieste PUT) a StorageGRID non riusciranno. È necessario riprovare queste richieste non riuscite quando l'endpoint diventa raggiungibile.</p>
Limitazione dell'endpoint di destinazione	<p>Il software StorageGRID potrebbe limitare le richieste S3 in arrivo per un bucket se la velocità con cui vengono inviate le richieste supera la velocità con cui l'endpoint di destinazione può riceverle. La limitazione si verifica solo quando è presente un arretrato di richieste in attesa di essere inviate all'endpoint di destinazione.</p> <p>L'unico effetto visibile è che le richieste S3 in arrivo impiegheranno più tempo per essere eseguite. Se si inizia a rilevare un rallentamento significativo delle prestazioni, è opportuno ridurre la velocità di acquisizione o utilizzare un endpoint con capacità maggiore. Se l'arretrato di richieste continua ad aumentare, le operazioni S3 del client (come le richieste PUT) alla fine falliranno.</p> <p>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.</p>

Considerazione	Dettagli
Garanzie di ordinazione	<p>StorageGRID garantisce l'ordinamento delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni su un oggetto avvengono nello stesso sito, lo stato finale dell'oggetto (per la replica) sarà sempre uguale allo stato in StorageGRID.</p> <p>StorageGRID fa del suo meglio per ordinare le richieste quando le operazioni vengono eseguite tra i siti StorageGRID. Ad esempio, se inizialmente si scrive un oggetto sul sito A e poi si sovrascrive lo stesso oggetto sul sito B, non è garantito che l'oggetto finale replicato da CloudMirror nel bucket di destinazione sia l'oggetto più recente.</p>
Eliminazioni di oggetti guidate da ILM	<p>Per adeguarsi al comportamento di eliminazione di AWS CRR e Amazon Simple Notification Service, le richieste di notifica di eventi e CloudMirror non vengono inviate quando un oggetto nel bucket di origine viene eliminato a causa delle regole StorageGRID ILM. Ad esempio, non vengono inviate richieste di notifiche di eventi o CloudMirror se una regola ILM elimina un oggetto dopo 14 giorni.</p> <p>Al contrario, le richieste di integrazione della ricerca vengono inviate quando gli oggetti vengono eliminati a causa di ILM.</p>
Utilizzo degli endpoint Kafka	<p>Per gli endpoint Kafka, Mutual TLS non è supportato. Di conseguenza, se hai <code>ssl.client.auth</code> impostato su <code>required</code> nella configurazione del broker Kafka, potrebbe causare problemi di configurazione dell'endpoint Kafka.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• SASL/PLAIN</li> <li>• SASL/SCRAM-SHA-256</li> <li>• SASL/SCRAM-SHA-512</li> </ul> <p><b>Nota:</b> le impostazioni del proxy di archiviazione configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.</p>

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

Considerazione	Dettagli
Stato di replicazione	StorageGRID non supporta il <code>x-amz-replication-status</code> intestazione.
Dimensione dell'oggetto	<p>La dimensione massima degli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è 5 TiB, che è la stessa della dimensione massima <i>supportata</i> dell'oggetto.</p> <p><b>Nota:</b> la dimensione massima <i>consigliata</i> per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa invece il caricamento multipart.</p>

Considerazione	Dettagli
Versionamento del bucket e ID versione	<p>Se il bucket S3 di origine in StorageGRID ha il controllo delle versioni abilitato, è necessario abilitare il controllo delle versioni anche per il bucket di destinazione.</p> <p>Quando si utilizza il controllo delle versioni, tenere presente che l'ordinamento delle versioni degli oggetti nel bucket di destinazione è basato sul miglior sforzo possibile e non è garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3.</p> <p><b>Nota:</b> gli ID versione per il bucket di origine in StorageGRID non sono correlati agli ID versione per il bucket di destinazione.</p>
Tagging per le versioni degli oggetti	<p>A causa delle limitazioni del protocollo S3, il servizio CloudMirror non replica alcuna richiesta PutObjectTagging o DeleteObjectTagging che fornisca un ID versione. Poiché gli ID versione per l'origine e la destinazione non sono correlati, non esiste alcun modo per garantire che un aggiornamento del tag a un ID versione specifico venga replicato.</p> <p>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 per l'ultima versione se il bucket è sottoposto a versioning). Vengono replicati anche gli ingest normali con tag (non gli aggiornamenti dei tag).</p>
Caricamenti multiparte e ETag valori	Quando si esegue il mirroring di oggetti caricati tramite un caricamento multiparte, il servizio CloudMirror non conserva le parti. Di conseguenza, il ETag il valore per l'oggetto specchiato sarà diverso da quello ETag valore dell'oggetto originale.
Oggetti crittografati con SSE-C (crittografia lato server con chiavi fornite dal cliente)	Il servizio CloudMirror non supporta oggetti crittografati con SSE-C. Se si tenta di importare un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione fallisce.
Bucket con blocco oggetto S3 abilitato	La replica non è supportata per i bucket di origine o di destinazione con S3 Object Lock abilitato.

## Comprendere il servizio di replica CloudMirror

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

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



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

## CloudMirror e ILM

La replica di CloudMirror funziona indipendentemente dalle policy ILM attive della griglia. Il servizio CloudMirror replica gli oggetti così come vengono archiviati nel bucket di origine e li distribuisce al bucket di destinazione il prima possibile. La consegna degli oggetti replicati viene attivata quando l'acquisizione dell'oggetto riesce.

## CloudMirror e replicazione cross-grid

La replica di CloudMirror presenta importanti somiglianze e differenze con la funzionalità di replica tra griglie. Fare riferimento a "["Confronta la replicazione cross-grid e la replicazione CloudMirror"](#)" .

## CloudMirror e bucket S3

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

### Secchi esistenti

Quando si abilita la replica CloudMirror per un bucket esistente, vengono replicati solo i nuovi oggetti aggiunti a quel bucket. Tutti gli oggetti esistenti nel bucket non vengono replicati. Per forzare la replica di oggetti esistenti, è possibile aggiornare i metadati dell'oggetto esistente eseguendo una copia dell'oggetto.



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

## Più bucket di destinazione

Per replicare gli oggetti in un singolo bucket su più bucket di destinazione, specificare la destinazione per ciascuna regola nel file XML di configurazione della replica. Non è possibile replicare un oggetto in più bucket contemporaneamente.

## Bucket con o senza versione

È possibile configurare la replica di CloudMirror su bucket con o senza versione. I bucket di destinazione possono essere dotati o meno di versione. È possibile utilizzare qualsiasi combinazione di bucket con e senza controllo delle versioni. Ad esempio, è possibile specificare un bucket con versione come destinazione per un bucket di origine senza versione o viceversa. È anche possibile replicare tra bucket senza controllo delle versioni.

## Eliminazione, cicli di replicazione ed eventi

### Comportamento di eliminazione

È lo stesso 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 sottoposti a versioning, il marcitore di eliminazione viene replicato. Se il bucket di destinazione non è sottoposto a controllo di versione, l'eliminazione di un oggetto nel bucket di origine non replica il marcitore di eliminazione nel bucket di destinazione né elimina l'oggetto di destinazione.

### Protezione dai cicli di replicazione

Quando gli oggetti vengono replicati nel bucket di destinazione, StorageGRID li contrassegna come "repliche". Un bucket StorageGRID di destinazione non replicherà più gli oggetti contrassegnati come repliche, proteggendoti da loop di replica accidentali. Questa marcatura della replica è interna a

StorageGRID e non impedisce di sfruttare AWS CRR quando si utilizza un bucket Amazon S3 come destinazione.



L'intestazione personalizzata utilizzata per contrassegnare una replica è `x-ntap-sg-replica`. Questa marcatura impedisce la formazione di uno specchio a cascata. StorageGRID supporta un CloudMirror bidirezionale tra due griglie.

## Eventi nel bucket di destinazione

L'unicità e l'ordinamento degli eventi nel bucket di destinazione non sono garantiti. A seguito delle operazioni intraprese per garantire il successo della consegna, potrebbero essere consegnate alla destinazione più copie identiche di un oggetto sorgente. In rari casi, quando lo stesso oggetto viene aggiornato simultaneamente da due o più siti StorageGRID diversi, l'ordinamento delle operazioni sul bucket di destinazione potrebbe non corrispondere all'ordinamento degli eventi sul bucket di origine.

## Comprendere le notifiche per i bucket

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

Ad esempio, è possibile configurare l'invio di avvisi agli amministratori per ogni oggetto aggiunto a un bucket, dove gli oggetti rappresentano file di registro associati a un evento di sistema critico.

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

L'unicità e l'ordinamento delle notifiche non sono garantiti. A seguito delle operazioni intraprese per garantire il successo della consegna, potrebbero essere recapitate alla destinazione più notifiche relative a un evento. Poiché la consegna è asincrona, non è garantito che l'ordinamento temporale delle notifiche a destinazione corrisponda all'ordinamento degli eventi nel bucket di origine, in particolare per le operazioni che hanno origine da siti StorageGRID diversi. Puoi usare il `sequencer` digitare nel messaggio dell'evento per determinare l'ordine degli eventi per un oggetto specifico, come descritto nella documentazione di Amazon S3.

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

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

Nome chiave	Valore StorageGRID
origineevento	sgws:s3
Regione aws	<i>non incluso</i>
x-amz-id-2	<i>non incluso</i>
arn	urn:sgws:s3:::bucket_name

### Comprendere il servizio di integrazione della ricerca

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

Il servizio di integrazione della ricerca è un servizio StorageGRID personalizzato che invia 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 i suoi metadati o tag vengono aggiornati. È quindi possibile utilizzare strumenti sofisticati di ricerca, analisi dei dati, visualizzazione o apprendimento automatico forniti dal servizio di destinazione per cercare, analizzare e ottenere informazioni dai dati degli oggetti.

Ad esempio, puoi configurare i tuoi bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. Potresti quindi utilizzare Elasticsearch per effettuare ricerche tra i bucket e realizzare analisi sofisticate dei modelli presenti nei metadati degli oggetti.

Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Retain Until Date e Legal Hold) degli oggetti non saranno inclusi nei metadati inviati a Elasticsearch.

 Poiché il servizio di integrazione della ricerca determina l'invio dei metadati degli oggetti a una destinazione, il suo XML di configurazione viene denominato "XML di configurazione della notifica *metadata*". Questo XML di configurazione è diverso dal "XML di configurazione delle notifiche" utilizzato per abilitare le notifiche *event*.

### Integrazione della ricerca e bucket S3

È possibile abilitare il servizio di integrazione della ricerca per qualsiasi bucket con o senza versione. L'integrazione della ricerca viene configurata associando l'XML di configurazione delle notifiche dei metadati al bucket che specifica su quali oggetti agire e la destinazione dei metadati degli oggetti.

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. Ogni notifica di metadati contiene un set standard di metadati di sistema per l'oggetto, oltre a tutti i tag dell'oggetto e ai metadati utente.

 Per i tag e i metadati utente, StorageGRID passa 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, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati di data. È necessario abilitare i mapping dei campi dinamici sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo aver indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

## Notifiche di ricerca

Le notifiche dei metadati vengono generate e messe in coda per la consegna ogni volta che:

- Viene creato un oggetto.
- Un oggetto viene eliminato, anche quando gli oggetti vengono eliminati a seguito dell'esecuzione della politica ILM della griglia.
- I metadati o i tag degli oggetti vengono aggiunti, aggiornati o eliminati. Durante l'aggiornamento viene sempre inviato l'insieme completo di metadati e tag, 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 creati e per tutti gli oggetti modificati aggiornandone i dati, i metadati utente o i tag. Tuttavia, le notifiche non vengono inviate per gli oggetti che erano già presenti nel bucket. Per garantire che i metadati degli oggetti per tutti gli oggetti nel bucket vengano inviati alla destinazione, è necessario effettuare una delle seguenti operazioni:

- Configurare il servizio di integrazione della ricerca subito dopo aver creato il bucket e prima di aggiungere qualsiasi oggetto.
- Esegui un'azione su tutti gli oggetti già presenti nel bucket che attiverà l'invio di un messaggio di notifica dei metadati alla destinazione.

## Servizio di integrazione della ricerca ed Elasticsearch

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

## Gestire gli endpoint dei servizi della piattaforma

### Configurare gli endpoint dei servizi della piattaforma

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

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

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

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

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

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

della piattaforma, si utilizza l'URN dell'endpoint come destinazione nell'XML di configurazione utilizzato per abilitare il servizio.

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

#### **Endpoint per la replica CloudMirror**

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

#### **Endpoint per le notifiche**

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

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

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

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

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

#### **Informazioni correlate**

["Amministra StorageGRID"](#)

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

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

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

#### **Elementi URN**

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

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

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

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

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

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

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

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

#### URN per servizi ospitati su AWS e GCP

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

- Replica CloudMirror:

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

- Notifiche:

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

- Integrazione della ricerca:

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



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

#### URN per servizi ospitati localmente

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

- Replica CloudMirror:

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

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

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

- Notifiche:

Specificare un endpoint Amazon Simple Notification Service:

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

Specificare un endpoint Kafka:

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

- Integrazione della ricerca:

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



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

## Crea endpoint dei servizi della piattaforma

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

### Prima di iniziare

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



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

- Nome univoco della risorsa (URN)

["Specificare l'URN per l'endpoint dei servizi della piattaforma"](#)

- Credenziali di autenticazione (se richieste):

### Cerca endpoint di integrazione

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

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

### Endpoint di replicazione CloudMirror

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

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

### Endpoint Amazon SNS

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

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

### Punti finali di Kafka

Per gli endpoint Kafka, puoi utilizzare le seguenti credenziali:

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

- Certificato di sicurezza (se si utilizza un certificato CA personalizzato)

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

### Passi

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

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

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

Utilizzare uno dei seguenti formati:

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

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

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

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

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

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



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

Allo stesso modo, l'URI per un bucket ospitato su AWS potrebbe essere:

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



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

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



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

6. Selezionare **Continua**.

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

### Cerca endpoint di integrazione

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

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile AWS per autenticare le connessioni con la destinazione.	<ul style="list-style-type: none"><li>• ID chiave di accesso</li><li>• Chiave di accesso segreta</li></ul>
HTTP di base	Utilizza un nome utente e una password per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none"><li>• Nome utente</li><li>• Password</li></ul>

### Endpoint di replicazione CloudMirror

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

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile AWS per autenticare le connessioni con la destinazione.	<ul style="list-style-type: none"><li>• ID chiave di accesso</li><li>• Chiave di accesso segreta</li></ul>
CAP (portale di accesso C2S)	Utilizza certificati e chiavi per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none"><li>• URL delle credenziali temporanee</li><li>• Certificato CA del server (caricamento file PEM)</li><li>• Certificato client (caricamento file PEM)</li><li>• Chiave privata del client (caricamento file PEM, formato crittografato OpenSSL o formato chiave privata non crittografata)</li><li>• Passphrase della chiave privata del client (facoltativa)</li></ul>

### Endpoint Amazon SNS

Inserisci o carica le credenziali per un endpoint Amazon SNS.

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali in stile AWS per autenticare le connessioni con la destinazione.	<ul style="list-style-type: none"><li>• ID chiave di accesso</li><li>• Chiave di accesso segreta</li></ul>

### Punti finali di Kafka

Inserisci o carica le credenziali per un endpoint Kafka.

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
SASL/PLAIN	Utilizza un nome utente e una password con testo normale per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none"><li>• Nome utente</li><li>• Password</li></ul>
SASL/SCRAM-SHA-256	Utilizza un nome utente e una password tramite un protocollo challenge-response e l'hashing SHA-256 per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none"><li>• Nome utente</li><li>• Password</li></ul>
SASL/SCRAM-SHA-512	Utilizza un nome utente e una password tramite un protocollo challenge-response e l'hashing SHA-512 per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none"><li>• Nome utente</li><li>• Password</li></ul>

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

8. Selezionare **Continua**.

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

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

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

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



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

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

#### Informazioni correlate

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

#### Prova la connessione per l'endpoint dei servizi della piattaforma

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

#### Prima di iniziare

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

#### Informazioni su questo compito

StorageGRID non convalida che le credenziali abbiano le autorizzazioni corrette.

#### Passi

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

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

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

Viene visualizzata la pagina dei dettagli dell'endpoint.

## 3. Selezionare **Test connessione**.

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

## Modifica endpoint dei servizi della piattaforma

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

### Prima di iniziare

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

### Passi

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

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

## 2. Seleziona l'endpoint che vuoi modificare.

Viene visualizzata la pagina dei dettagli dell'endpoint.

## 3. Selezionare **Configurazione**.

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



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

a. Per modificare il nome visualizzato per l'endpoint, seleziona l'icona di modifica  .

b. Se necessario, modificare l'URI.

c. Se necessario, modificare il tipo di autenticazione.

- Per l'autenticazione con chiave di accesso, modificare la chiave secondo necessità selezionando **Modifica chiave S3** e incollando un nuovo ID chiave di accesso e una chiave di accesso segreta. Se devi annullare le modifiche, seleziona **Annulla modifica chiave S3**.

- Per l'autenticazione CAP (C2S Access Portal), modificare l'URL delle credenziali temporanee o la passphrase della chiave privata del client facoltativa e caricare nuovi file di certificato e chiave secondo necessità.



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

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

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

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

## Elimina l'endpoint dei servizi della piattaforma

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

### Prima di iniziare

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

### Passi

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

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

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



Se si elimina un endpoint dei servizi di piattaforma in uso, il servizio di piattaforma associato verrà disabilitato per tutti i bucket che utilizzano l'endpoint. Tutte le richieste non ancora completate verranno eliminate. Tutte le nuove richieste continueranno a essere generate finché non modifichi la configurazione del bucket in modo che non faccia più riferimento all'URN eliminato. StorageGRID segnalerà queste richieste come errori irrecuperabili.

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

Appare un messaggio di conferma.

#### 4. Selezionare **Elimina endpoint**.

## Risolvere gli errori degli endpoint dei servizi della piattaforma

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

## Determina se si è verificato un errore

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

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

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

### Passi

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

### Controlla se l'errore è ancora attuale

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

### Passi

1. Selezionare l'endpoint.
2. Viene visualizzata la pagina dei dettagli dell'endpoint.
2. Selezionare **Connessione > Test connessione**.

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

### Risolvi gli errori dell'endpoint

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

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

### Passi

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

#### 4. Selezionare Connessione > Test connessione.

##### Credenziali dell'endpoint con autorizzazioni insufficienti

Quando StorageGRID convalida un endpoint dei servizi della piattaforma, conferma che le credenziali dell'endpoint possono essere utilizzate per contattare la risorsa di destinazione ed esegue un controllo di base delle autorizzazioni. Tuttavia, StorageGRID non convalida tutte le autorizzazioni richieste per determinate operazioni dei servizi della piattaforma. Per questo motivo, se si riceve un errore quando si tenta di utilizzare un servizio della piattaforma (ad esempio "403 Forbidden"), verificare le autorizzazioni associate alle credenziali dell'endpoint.

##### Informazioni correlate

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

## Configurare la replica di CloudMirror

Per abilitare la replica di CloudMirror per un bucket, è necessario creare e applicare un XML di configurazione della replica del bucket valido.

##### Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore StorageGRID .
- Hai già creato un bucket che fungerà da origine di replicazione.
- L'endpoint che intendi utilizzare come destinazione per la replica CloudMirror esiste già e disponi del suo URN.
- Appartieni a un gruppo di utenti che ha il "[Gestisci tutti i bucket o l'autorizzazione di accesso Root](#)" . Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket quando si configura il bucket tramite Tenant Manager.

##### Informazioni su questo compito

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

Per informazioni generali sulla replicazione dei bucket e su come configurarla, vedere "[Documentazione di Amazon Simple Storage Service \(S3\): replica di oggetti](#)" . Per informazioni su come StorageGRID implementa GetBucketReplication, DeleteBucketReplication e PutBucketReplication, vedere "[Operazioni sui bucket](#)" .



La replica di CloudMirror presenta importanti somiglianze e differenze con la funzionalità di replica tra griglie. Per saperne di più, vedere "[Confronta la replicazione cross-grid e la replicazione CloudMirror](#)" .

Quando si configura la replica di CloudMirror, tenere presente i seguenti requisiti e caratteristiche:

- Quando si crea e si applica un XML di configurazione della replica del bucket valido, è necessario utilizzare 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 si abilita la replica CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket

vengono replicati, ma gli oggetti esistenti nel bucket non vengono replicati. Per attivare la replica è necessario aggiornare gli oggetti esistenti.

- Se si specifica una classe di archiviazione nel file XML di configurazione della replica, StorageGRID utilizza tale classe quando esegue operazioni sull'endpoint S3 di destinazione. Anche l'endpoint di destinazione deve supportare la classe di archiviazione specificata. Assicuratevi di seguire tutte le raccomandazioni fornite dal fornitore del sistema di destinazione.

## Passi

### 1. Abilita la replica per il tuo bucket di origine:

- Utilizzare un editor di testo per creare il file XML di configurazione della replicazione necessario per abilitare la replicazione, come specificato nell'API di replicazione S3.
- Durante la configurazione dell'XML:
  - Si noti che StorageGRID supporta solo la versione 1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'uso di `Filter` elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per maggiori dettagli, consultare la documentazione di Amazon sulla configurazione della replica.
  - Utilizzare l'URN di un endpoint del bucket S3 come destinazione.
  - Aggiungere facoltativamente il `<StorageClass>` elemento e specificare una delle seguenti opzioni:
    - **STANDARD**: La classe di archiviazione predefinita. Se non si specifica una classe di archiviazione quando si carica un oggetto, STANDARD viene utilizzata la classe di archiviazione.
    - **STANDARD\_IA**: (Standard - accesso poco frequente.) Utilizzare questa classe di archiviazione per i dati a cui si accede meno frequentemente, ma che richiedono comunque un accesso rapido quando necessario.
    - **REDUCED\_REDUNDANCY**: Utilizzare questa classe di archiviazione per dati non critici e riproducibili che possono essere archiviati con una ridondanza inferiore rispetto a STANDARD classe di archiviazione.
  - Se si specifica un `Role` nella configurazione XML verrà ignorato. Questo valore non è utilizzato da StorageGRID.

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

### 2. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.

### 3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

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



I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID tramite Grid Manager o Grid Management API. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore StorageGRID .

7. Verificare che la replica sia configurata correttamente:

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

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

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

Per gli oggetti di piccole dimensioni la replicazione avviene rapidamente.

#### Informazioni correlate

["Crea endpoint dei servizi della piattaforma"](#)

## Configurare le notifiche degli eventi

È possibile abilitare le notifiche per un bucket creando un XML di configurazione delle notifiche e utilizzando Tenant Manager per applicare l'XML a un bucket.

#### Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore StorageGRID .
- Hai già creato un bucket che fungerà da fonte di notifiche.
- L'endpoint che intendi utilizzare come destinazione per le notifiche degli eventi esiste già e disponi del relativo URN.
- Appartieni a un gruppo di utenti che ha il "["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#)" . Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket quando si configura il bucket tramite Tenant Manager.

#### Informazioni su questo compito

È possibile configurare le notifiche degli eventi associando l'XML di configurazione delle notifiche a un bucket di origine. Il codice XML di configurazione delle notifiche segue le convenzioni S3 per la configurazione delle notifiche dei bucket, con l'argomento di destinazione Kafka o Amazon SNS specificato come URN di un endpoint.

Per informazioni generali sulle notifiche degli eventi e su come configurarle, fare riferimento a ["Documentazione Amazon"](#) . Per informazioni su come StorageGRID implementa l'API di configurazione delle notifiche del bucket S3, fare riferimento a ["istruzioni per l'implementazione di applicazioni client S3"](#) .

Quando si configurano le notifiche degli eventi per un bucket, tenere presente i seguenti requisiti e

caratteristiche:

- Quando si crea e si applica un XML di configurazione delle notifiche valido, è necessario utilizzare l'URN di un endpoint delle notifiche degli eventi per ciascuna destinazione.
- Sebbene la notifica degli eventi possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Conserva fino alla data e Conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.
- Dopo aver configurato le notifiche degli eventi, ogni volta che si verifica un evento specifico per un oggetto nel bucket di origine, viene generata una notifica e inviata all'argomento Amazon SNS o Kafka utilizzato come endpoint di destinazione.
- Se si abilitano le notifiche degli eventi per un bucket che contiene oggetti, le notifiche vengono inviate solo per le azioni eseguite dopo il salvataggio della configurazione delle notifiche.

## Passi

### 1. Abilita le notifiche per il tuo bucket di origine:

- Utilizzare 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 dell'XML, utilizzare l'URN di un endpoint di notifiche degli eventi come argomento di destinazione.

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

### 2. In Tenant Manager, seleziona **ARCHIVIAZIONE (S3) > Bucket**.

### 3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

### 4. Selezionare **Servizi piattaforma > Notifiche eventi**.

### 5. Selezionare 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 ciascun account tenant da un amministratore StorageGRID tramite Grid Manager o Grid Management API. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore StorageGRID .

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

- a. Eseguire un'azione su un oggetto nel bucket di origine che soddisfi i requisiti per l'attivazione di una notifica come configurato nell'XML di configurazione.

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

- b. Conferma che una notifica è stata recapitata all'argomento Amazon SNS o Kafka di destinazione.

Ad esempio, se l'argomento di destinazione è ospitato su Amazon SNS, puoi configurare il servizio in modo che ti venga inviata un'e-mail quando la notifica viene recapitata.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

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

## Informazioni correlate

["Comprendere le notifiche per i bucket"](#)

["Utilizzare l'API REST S3"](#)

["Crea endpoint dei servizi della piattaforma"](#)

## Configurare il servizio di integrazione della ricerca

È possibile abilitare l'integrazione della ricerca per un bucket creando un XML di integrazione della ricerca e utilizzando Tenant Manager per applicare l'XML al bucket.

### Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore 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 dispone del suo URN.
- Appartieni a un gruppo di utenti che ha il "[Gestisci tutti i bucket o l'autorizzazione di accesso Root](#)" . Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket quando si configura il bucket tramite Tenant Manager.

### Informazioni su questo compito

Dopo aver configurato il servizio di integrazione della ricerca per un bucket di origine, la creazione di un oggetto o l'aggiornamento dei metadati o dei tag di un oggetto attiva l'invio dei metadati dell'oggetto all'endpoint di destinazione.

Se si abilita 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. Aggiornare questi oggetti esistenti per garantire che i loro metadati vengano aggiunti all'indice di ricerca di destinazione.

### Passi

#### 1. Abilita l'integrazione della ricerca per un bucket:

- Utilizzare un editor di testo per creare il file XML di notifica dei metadati necessario per abilitare l'integrazione della ricerca.
- Durante la configurazione dell'XML, utilizzare l'URN di un endpoint di integrazione della ricerca come destinazione.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, potresti inviare metadati per oggetti con il prefisso `images` verso una destinazione e metadati per oggetti con il prefisso `videos` all'altro. Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, una configurazione che include una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2` non è consentito.

Se necessario, fare riferimento a [esempi per la configurazione dei metadati XML](#) .

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

Elementi nel file XML di configurazione della notifica dei metadati:

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

Nome	Descrizione	Necessario
Urna	<p>URN della destinazione a cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà:</p> <ul style="list-style-type: none"> <li>• `es` deve essere il terzo elemento.</li> <li>• L'URN deve terminare con l'indice e il tipo in cui sono archiviati i metadati, nel formato domain-name/myindex/mytype .</li> </ul> <p>Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma:</p> <ul style="list-style-type: none"> <li>• arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404.</p> <p>L'URN è incluso nell'elemento Destinazione.</p>	Sì

2. In Tenant Manager seleziona **ARCHIVIAZIONE (S3) > Bucket**.

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Seleziona **Servizi della piattaforma > Integrazione di 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 ciascun account tenant da un amministratore StorageGRID tramite Grid Manager o Management API. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore StorageGRID .

7. Verificare che il servizio di integrazione della ricerca sia configurato correttamente:

a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per l'attivazione di una notifica di metadati come specificato nel file XML di configurazione.

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

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

## Dopo aver finito

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

- Selezionare **ARCHIVIAZIONE (S3) > Bucket** e deselezionare la casella di controllo **Abilita integrazione ricerca**.
- Se si utilizza direttamente l'API S3, utilizzare una richiesta di notifica dei metadati DELETE Bucket. Consultare le istruzioni per l'implementazione delle applicazioni client S3.

#### **Esempio: configurazione della 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, metadati degli oggetti per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti corrispondono al prefisso `/videos` viene inviato 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-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

## Formato di notifica dei metadati

Quando si abilita il servizio di integrazione della ricerca per un bucket, ogni volta che vengono aggiunti, aggiornati o eliminati metadati o tag di un oggetto, viene generato un documento JSON che viene inviato all'endpoint di destinazione.

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 il bucket non è sottoposto a versioning, quindi versionId il 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 oggetti

bucket: Nome del bucket

key: Nome chiave dell'oggetto

versionID: Versione dell'oggetto, per gli oggetti nei bucket con versione

region: Regione del bucket, ad 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 utente 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 passa 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, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati di data. Abilitare i mapping dei campi dinamici sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo aver indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

## Informazioni sul copyright

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

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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