



USA StorageGRID

StorageGRID software

NetApp

January 14, 2026

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid/tenant/index.html> on January 14, 2026. Always check docs.netapp.com for the latest.

Sommario

Utilizzare tenant e client StorageGRID	1
Utilizzare un account tenant	1
Utilizzare un account tenant	1
Come effettuare l'accesso e disconnettersi	2
Comprendere la dashboard di Tenant Manager	4
API di gestione del tenant	7
Utilizzare connessioni di federazione di griglie	12
Gestire gruppi e utenti	26
Gestire le chiavi di accesso S3	44
Gestire i bucket S3	49
Gestire i servizi della piattaforma S3	79
UTILIZZARE L'API REST S3	114
Versioni e aggiornamenti supportati dall'API REST S3	114
Riferimento rapido: Richieste API S3 supportate	117
Eseguire il test della configurazione dell'API REST S3	136
Come StorageGRID implementa l'API REST S3	137
Supporto per Amazon S3 REST API	153
Operazioni personalizzate di StorageGRID	204
Gestire le policy di accesso	226
Operazioni S3 registrate nei registri di audit	253
Utilizza Swift REST API (fine del ciclo di vita)	254
Utilizzare l'API REST di Swift	254

Utilizzare tenant e client StorageGRID

Utilizzare un account tenant

Utilizzare un account tenant

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

Che cos'è un account tenant?

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

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

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



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

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

Come creare un account tenant

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

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

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

Configurare i tenant S3

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

- Configurare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia)
- Gestire gruppi e utenti
- Utilizza la federazione di grid per il clone dell'account e la replica cross-grid
- Gestire le chiavi di accesso S3
- Creare e gestire i bucket S3
- Utilizzare i servizi della piattaforma S3
- USA S3 Select
- Monitorare l'utilizzo dello storage



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

Come effettuare l'accesso e disconnettersi

Accedi a Tenant Manager

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

Prima di iniziare

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

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

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

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

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

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

Fasi

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

4. Accedi al tenant manager.

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

Non si utilizza SSO

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

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

Viene visualizzata la dashboard di Tenant Manager.

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

Utilizzo di SSO

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

- La pagina SSO della tua organizzazione.

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

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

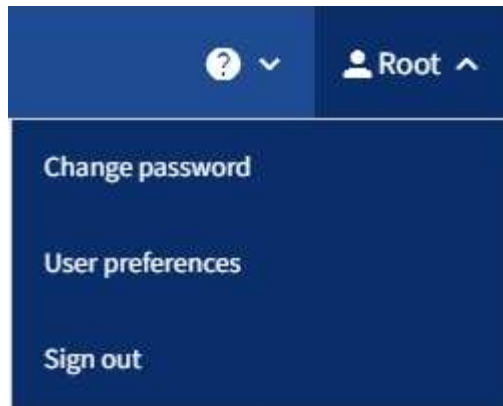
Viene visualizzata la dashboard di Tenant Manager.

Disconnettersi da Tenant Manager

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

Fasi

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



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

- Se SSO non è in uso:

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



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

- Se SSO è attivato:

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



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

Comprendere la dashboard di Tenant Manager

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



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

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

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



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

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

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Informazioni sull'account tenant

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

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

Utilizzo dello storage e delle quote

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

- La quantità di dati oggetto per il tenant.

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

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












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

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

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



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

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

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



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

Avvisi sull'utilizzo delle quote

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

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

Chiedere all'amministratore di rete di aumentare la quota.

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

utilizzo limite di capacità

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

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

Errori degli endpoint

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



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

API di gestione del tenant

Comprendere l'API di gestione dei tenant

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

L'API di gestione dei tenant:

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

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

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

Operazioni API

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

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

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

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



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

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

Dettagli dell'operazione

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

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	<div> Example Value Model </div> <pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" }</pre>

Emettere richieste API



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

Fasi

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

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

Versione dell'API di gestione tenant

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

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

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

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

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

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

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



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

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

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

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

Determinare quali versioni API sono supportate nella release corrente

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

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

Specificare una versione API per una richiesta

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

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

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

Protezione contro la contraffazione delle richieste (CSRF)

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

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

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

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

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

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

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

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

Per configurare la protezione CSRF, utilizzare ["API di Grid Management"](#) o ["API di gestione del tenant"](#).



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

Utilizzare connessioni di federazione di griglie

Clonare utenti e gruppi tenant

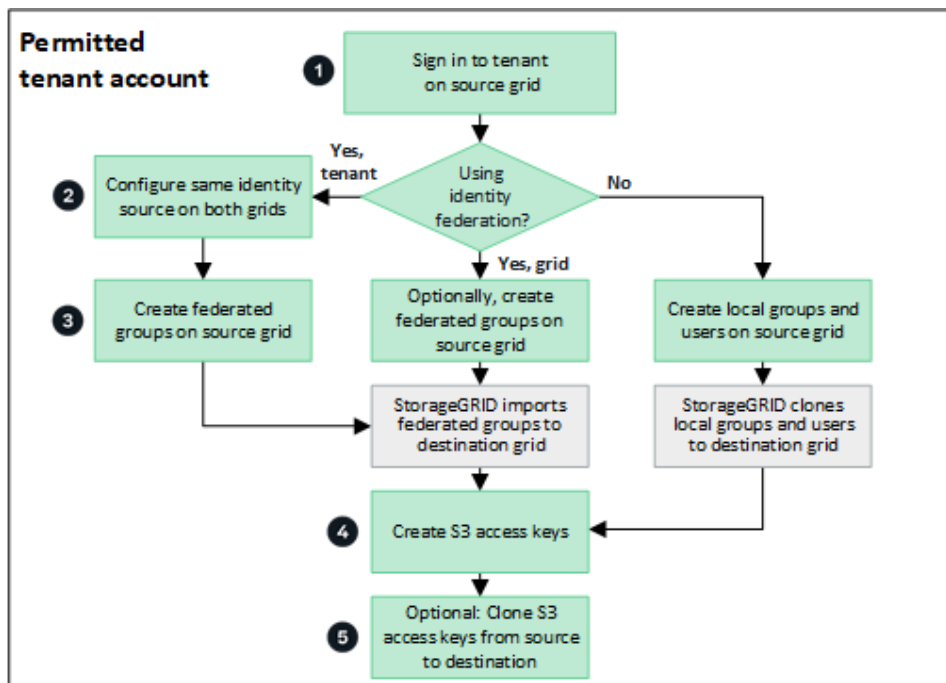
Se un tenant è stato creato o modificato per utilizzare una connessione federazione grid, tale tenant viene replicato da un sistema StorageGRID (il tenant di origine) a un altro sistema StorageGRID (il tenant di replica). Dopo la replica del tenant, tutti i gruppi e gli utenti aggiunti al tenant di origine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

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

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

Workflow del tenant per il clone dell'account

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



Questi sono i passaggi principali del flusso di lavoro:

1

Accedere al tenant

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

2

Facoltativamente, configurare la federazione delle identità

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

3

Creare gruppi e utenti

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

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

4

Creare S3 chiavi di accesso

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

In alternativa, è possibile clonare le chiavi di accesso S3

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

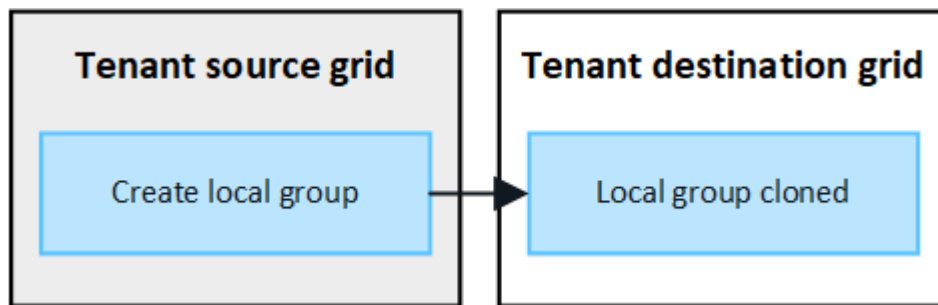
Come vengono clonati gruppi, utenti e chiavi di accesso S3?

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

I gruppi locali creati sulla griglia di origine vengono clonati

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

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

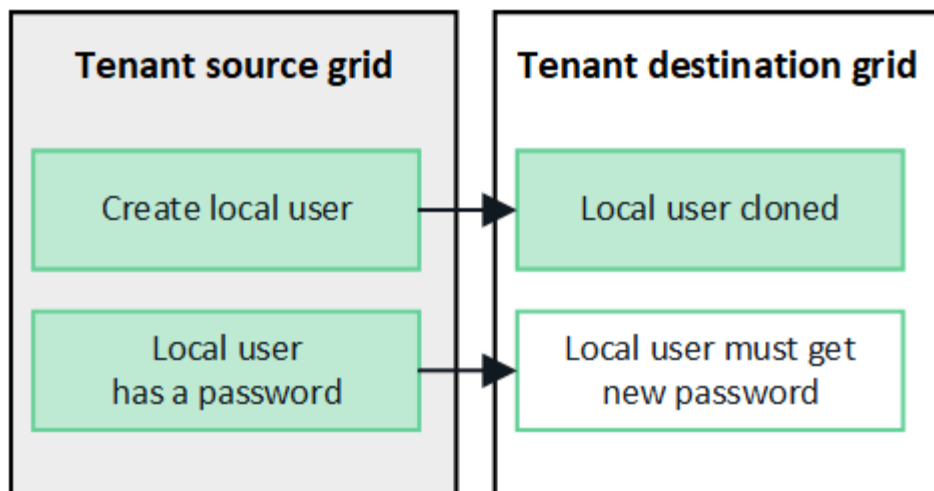


Tutti gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando si crea il gruppo. Al momento della creazione degli utenti, selezionare il gruppo.

Gli utenti locali creati sulla griglia di origine vengono clonati

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

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

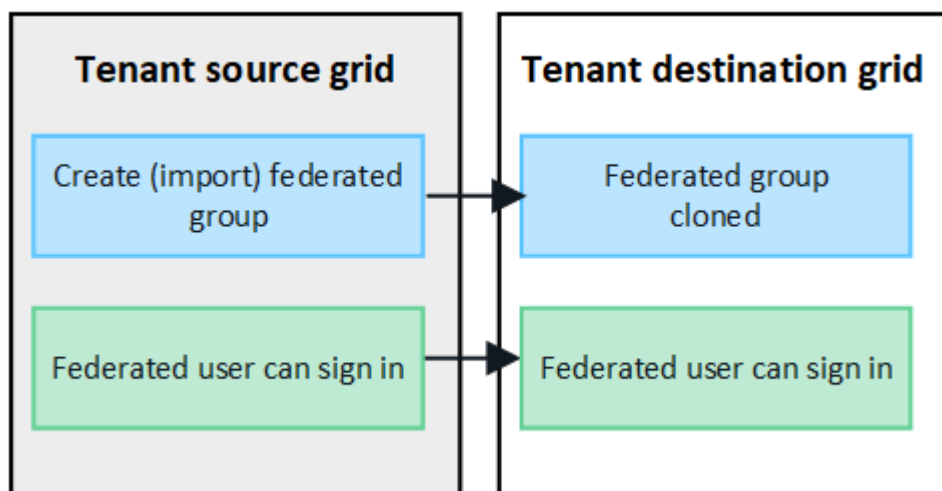


I gruppi federati creati sulla griglia di origine vengono clonati

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

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

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

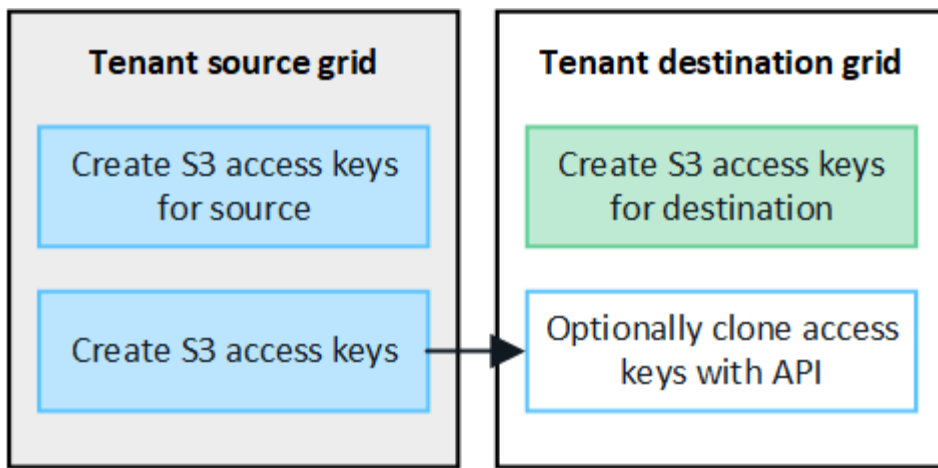


Le chiavi di accesso S3 possono essere clonate manualmente

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

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

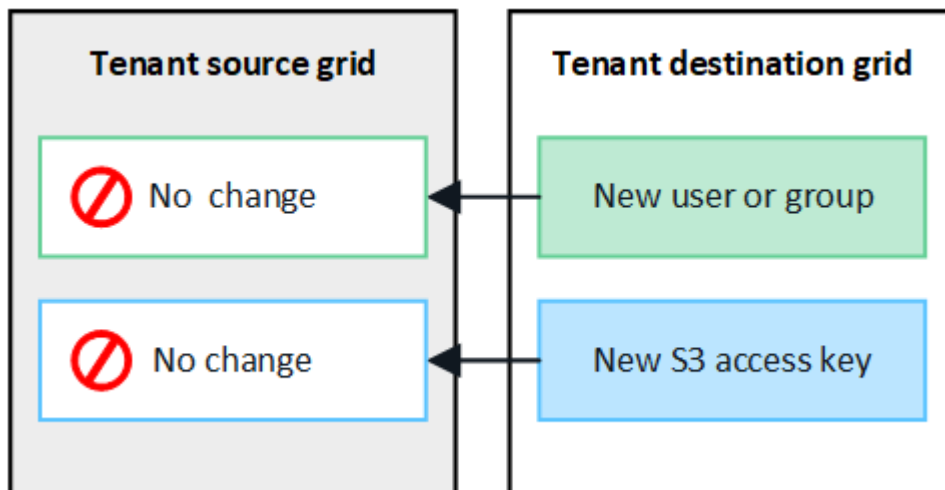
- Se non è necessario utilizzare gli stessi tasti per ogni griglia, è possibile ["creare le proprie chiavi di accesso"](#) o ["creare le chiavi di accesso di un altro utente"](#) su ogni griglia.
- Se è necessario utilizzare gli stessi tasti su entrambe le griglie, è possibile creare i tasti sulla griglia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



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

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

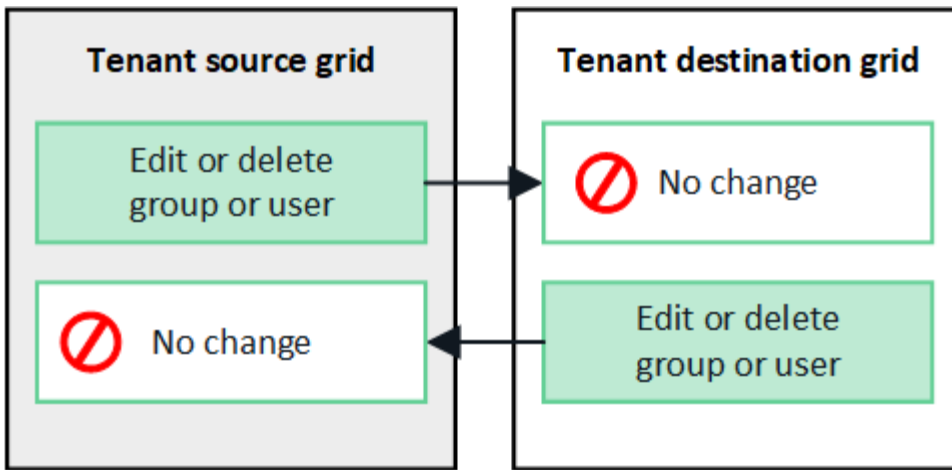
La clonazione avviene solo dalla griglia di origine del tenant alla griglia di destinazione del tenant. Se si creano o importano gruppi e utenti nella griglia di destinazione del tenant, StorageGRID non clonerà questi elementi nella griglia di origine del tenant.



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

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

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



Clonare le chiavi di accesso S3 utilizzando l'API

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

Prima di iniziare

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



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

Clonare le proprie chiavi di accesso

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

Fasi

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

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

POST

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



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

Assicurarsi di conservare le virgolette doppie intorno a ciascuna stringa.



The screenshot shows a REST client interface with a green header bar. On the left, the word "body" is followed by a red asterisk and the word "required". Below it, "(body)" is written. To the right of the header bar are two tabs: "Edit Value" and "Model". The "Model" tab is selected, and it displays a JSON object with three key-value pairs: "accessKey", "secretAccessKey", and "expires". The values are enclosed in double quotes.

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

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

Clonare le chiavi di accesso di un altro utente

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

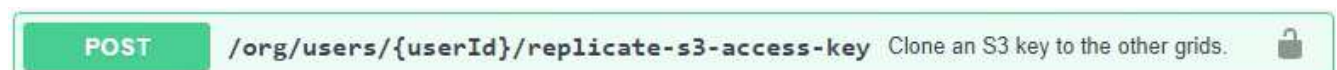
Fasi

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

```
GET /org/users
```

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

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



The screenshot shows a REST client interface with a green header bar. On the left, the word "POST" is written in white on a green background. To the right of "POST" is the endpoint "/org/users/{userId}/replicate-s3-access-key". Further to the right, the text "Clone an S3 key to the other grids." is displayed. On the far right, there is a lock icon.

5. Selezionare **Provalo**.

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

Assicurarsi di conservare le virgolette doppie intorno alla stringa.

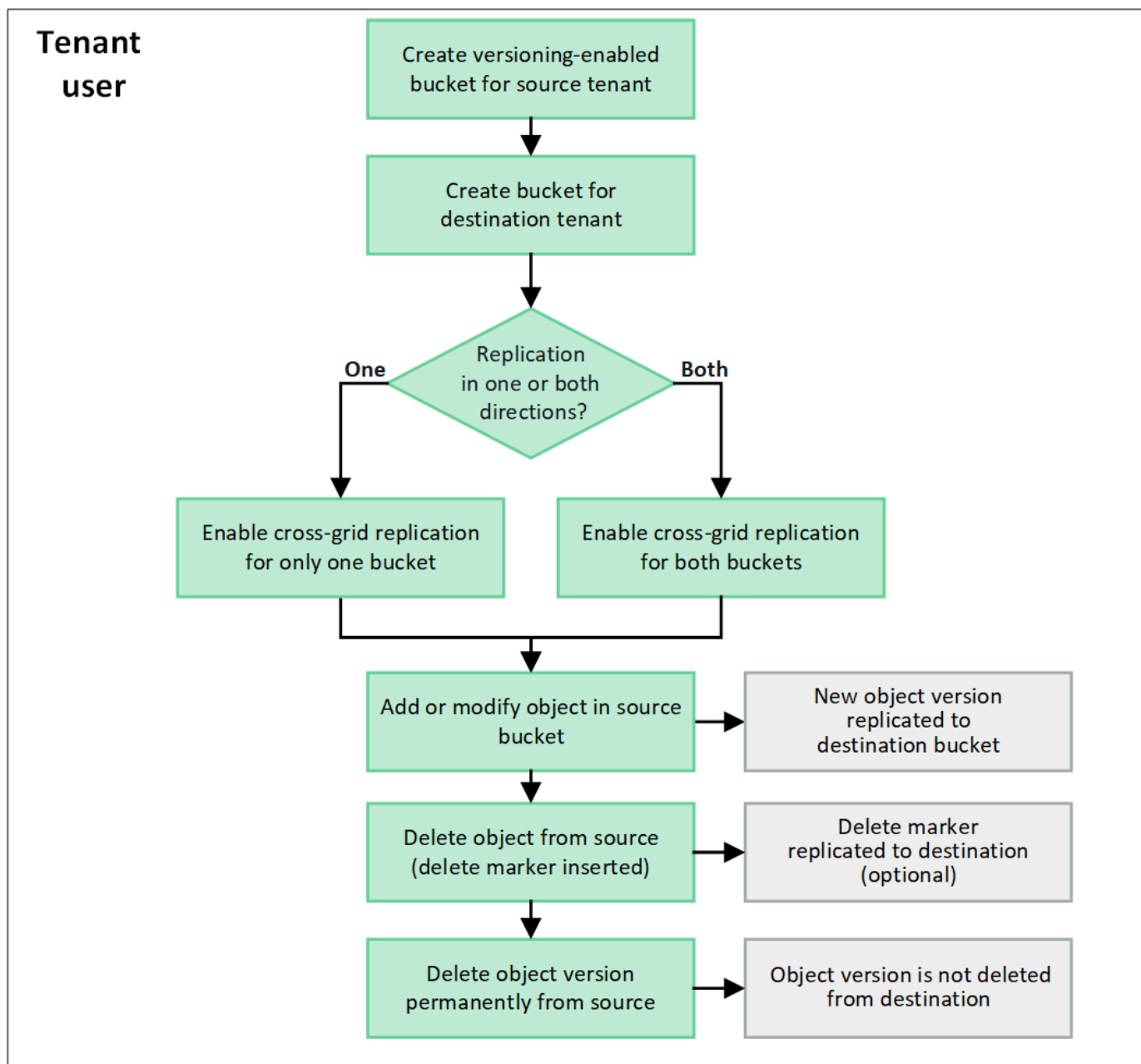
8. Se la chiave scade, sostituire la voce di esempio **Expires** con la data e l'ora di scadenza come stringa nel formato dati-ora ISO 8601 (ad esempio, `2023-02-28T22:46:33-08:00`). Se la chiave non scade, inserire **Null** come valore per la voce **Expires** (oppure rimuovere la riga **Expires** e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

Gestire la replica cross-grid

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

Workflow per la replica cross-grid

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



Configurare la replica cross-grid

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

Prima di iniziare

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

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

Crea due bucket

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

Fasi

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

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

- b. Seguire le istruzioni a ["Creare un bucket S3"](#).



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

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



Secondo necessità, ogni benna può utilizzare una regione diversa.

Abilitare la replica cross-grid

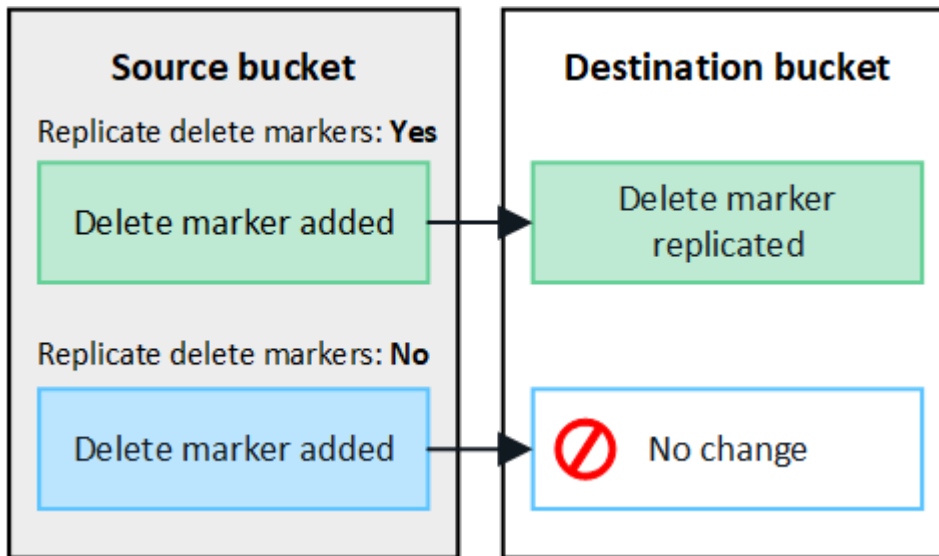
È necessario eseguire questi passaggi prima di aggiungere oggetti a uno dei bucket.

Fasi

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

g. Facoltativamente, modificare l'impostazione di **Replicate delete markers** per determinare cosa accade nella griglia di destinazione se un client S3 invia una richiesta di eliminazione alla griglia di origine che non include un ID di versione:

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



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

Fare riferimento a "[Che cos'è la replica cross-grid](#)" per i dettagli.

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

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

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

Test di replica tra griglie

Se la replica cross-grid è attivata per un bucket, potrebbe essere necessario verificare che la connessione e la replica cross-grid funzionino correttamente e che i bucket di origine e di destinazione soddisfino ancora tutti i requisiti (ad esempio, il controllo delle versioni è ancora attivato).

Prima di iniziare

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

Fasi

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

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

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

Disattiva la replica cross-grid

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

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

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



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

Prima di iniziare

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

Fasi

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

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

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

Visualizza connessioni di federazione di griglie

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

Prima di iniziare

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

Fasi

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

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

Colonna	Descrizione
Nome della connessione	Le connessioni della federazione di griglie che il tenant dispone dell'autorizzazione per l'utilizzo.
Bucket con replica cross-grid	Per ogni connessione a federazione di grid, i bucket tenant con replica cross-grid attivata. Gli oggetti aggiunti a questi bucket verranno replicati nell'altra griglia della connessione.

Colonna	Descrizione
Ultimo errore	Per ogni connessione a federazione di griglie, si verifica l'errore più recente, se presente, quando i dati venivano replicati nell'altra griglia. Vedere Eliminare l'ultimo errore .

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

Cancella l'ultimo errore

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

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



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

Fasi

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

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

Grid federation connections

Displaying one result

Connection name	Buckets with cross-grid replication	Last error
<input type="radio"/> 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 le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso nel bucket di destinazione per la replica cross-grid, riabilitare il controllo delle versioni per quel bucket.
3. Selezionare la connessione dalla tabella.
4. Selezionare **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.



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

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

Gestire gruppi e utenti

USA la federazione delle identità

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

Configurare la federazione delle identità per Tenant Manager

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

Prima di iniziare

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



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

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

A proposito di questa attività

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



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

Inserire la configurazione

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

Fasi

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

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other
------------------	----------	----------	-------

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

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



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

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

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

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

seguenti attributi:

- sAMAccountName O uid
 - objectGUID, entryUUID O nsuniqueid
 - cn
 - memberOf O isMemberOf
 - **Active Directory:** objectSid, primaryGroupID, userAccountControl E userPrincipalName
 - **ID di ingresso:** accountEnabled E userPrincipalName
- **Password:** La password associata al nome utente.



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

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



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

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



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

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

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

Immettere uno di questi modelli:

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

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

6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.

- **Usa STARTTLS:** usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Microsoft Entra ID.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Microsoft Entra ID.

- **Non utilizzare TLS:** il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Microsoft Entra ID.



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

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.

- **Usa certificato CA del sistema operativo:** Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
- **Usa certificato CA personalizzato:** Utilizza un certificato di protezione personalizzato.

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

Verificare la connessione e salvare la configurazione

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

Fasi

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

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

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

[Cancel](#) [Test Connection](#)

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

Forzare la sincronizzazione con l'origine dell'identità

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

Fasi

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

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



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

Disattiva la federazione delle identità

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

A proposito di questa attività

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

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

Fasi

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

Linee guida per la configurazione del server OpenLDAP

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



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

MemberOf e refint overlay

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

Indicizzazione

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

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

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

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

Gestire i gruppi di tenant

Creare gruppi per un tenant S3

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

Prima di iniziare

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

Accedere alla procedura guidata Crea gruppo

Come prima fase, accedere alla procedura guidata Crea gruppo.

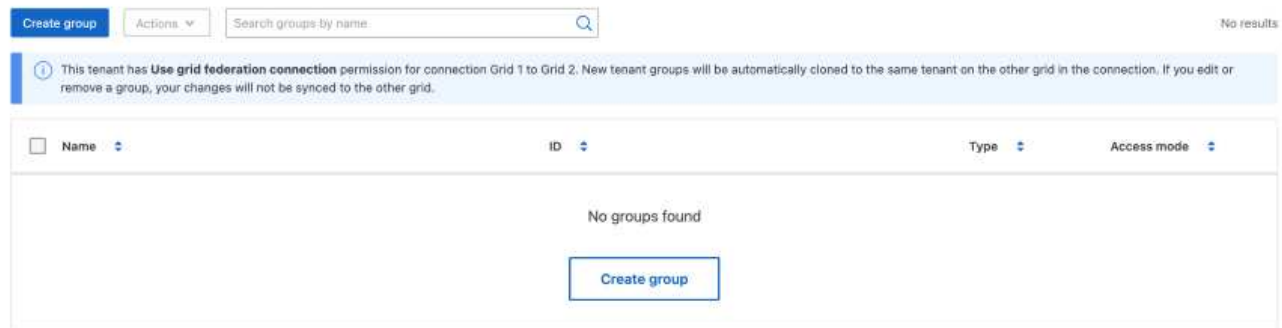
Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, verificare che venga visualizzato un banner blu che indica che i nuovi gruppi creati in questa griglia verranno clonati nello

stesso tenant nell'altra griglia della connessione. Se questo banner non viene visualizzato, potresti aver effettuato l'accesso alla griglia di destinazione del tenant.

Groups

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



3. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

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

Fasi

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

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

2. Inserire il nome del gruppo.

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



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

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

3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

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

Fasi

1. Per la modalità **Access**, selezionare una delle seguenti opzioni:

- **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
- **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API di gestione tenant Manager o tenant. Gli utenti locali di sola lettura possono modificare le proprie password.



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

2. Selezionare una o più autorizzazioni per questo gruppo.

Vedere "[Permessi di gestione del tenant](#)".

3. Selezionare **continua**.

Impostare i criteri di gruppo S3

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

Fasi

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

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

Policy di gruppo	Descrizione
Personalizzato	Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

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

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

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

Aggiunta di utenti (solo gruppi locali)

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



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

Fasi

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

Il gruppo creato viene visualizzato nell'elenco dei gruppi.

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

Permessi di gestione del tenant

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

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

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

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

funzionalità.



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

È possibile assegnare le seguenti autorizzazioni a un gruppo.

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

Gestire i gruppi

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

Prima di iniziare

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

Visualizzare o modificare il gruppo

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

Fasi


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

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

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

- Stato di cloning, **Success** o **Failure**
- Un banner blu che indica che se modifichi o elimini questo gruppo, le modifiche non verranno sincronizzate con l'altra griglia.

6. Modificare le impostazioni del gruppo secondo necessità. Fare riferimento a "[Creare gruppi per un tenant S3](#)" per i dettagli su cosa inserire.

- Nella sezione Panoramica, modificare il nome visualizzato selezionando il nome o l'icona di modifica .
- Nella scheda **permessi di gruppo**, aggiornare le autorizzazioni e selezionare **Salva modifiche**.
- Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.

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

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

- Selezionare la scheda Users (utenti).



Manage users

You can add users to this group or remove users from this group.

[Add users](#) [Remove users](#)

Displaying one result

Username	Full name	Denied access
User_02	User_02_Managers	No

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

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

8. Per rimuovere utenti locali dal gruppo:

- Selezionare la scheda Users (utenti).
- Selezionare **Rimuovi utenti**.
- Selezionare gli utenti che si desidera rimuovere e selezionare **Rimuovi utenti**.

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

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

Gruppo duplicato

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



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

Fasi

- Selezionare **Gestione accessi > Gruppi**.

2. Selezionare la casella di controllo del gruppo che si desidera duplicare.
3. Selezionare **azioni > Duplica gruppo**.
4. Vedere ["Creare gruppi per un tenant S3"](#) per i dettagli su cosa inserire.
5. Selezionare **Crea gruppo**.

Riprova clone di gruppo

Per riprovare un clone non riuscito:

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

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

Eliminare uno o più gruppi

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



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

Fasi

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

Viene visualizzata una finestra di dialogo di conferma.

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

Imposta AssumeRole

Prima di iniziare

Per configurare AssumeRole devi essere un amministratore.

A proposito di questa attività

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

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

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Fare clic sul nome del gruppo.
3. Selezionare la scheda **Criterio di attendibilità S3**.
4. Aggiungi i tuoi criteri di attendibilità S3, incluso un elenco di utenti che possono eseguire AssumeRole.
5. Selezionare **Save Changes** (Salva modifiche).
6. Selezionare la scheda **Criteri di gruppo S3**.
7. Modificare il criterio S3 per specificare solo le azioni S3 richieste per gli utenti attendibili aggiunti nel criterio di attendibilità S3 di questo gruppo.
8. Selezionare **Save Changes** (Salva modifiche).

Esempio di una policy di trust AssumeRole S3

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

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

Gestire gli utenti

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



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

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).

- L'utente appartiene a un gruppo di utenti che dispone di "[Autorizzazione di accesso root](#)".
- Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è stato esaminato il flusso di lavoro e le considerazioni relative a "[clonazione di utenti e gruppi tenant](#)" e si è effettuato l'accesso alla griglia di origine del tenant.

Crea un utente locale

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

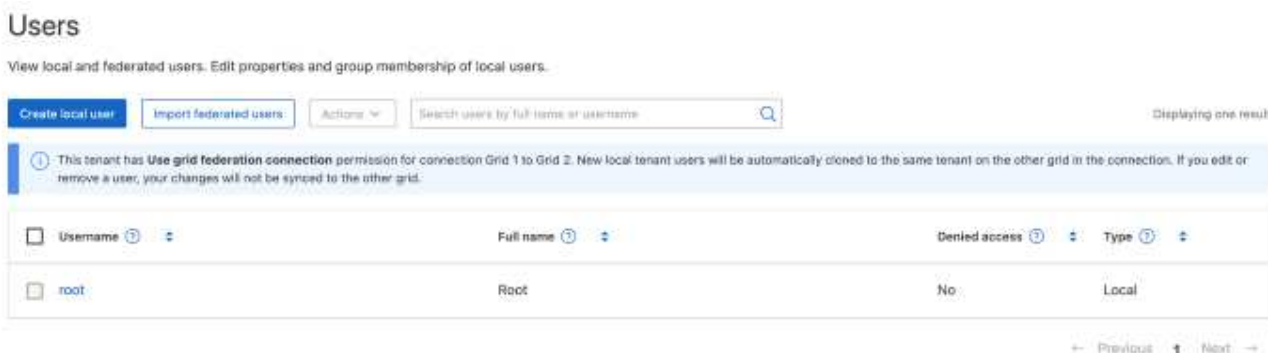
Gli utenti S3 che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o criteri di gruppo S3 applicati. Questi utenti potrebbero avere accesso al bucket S3 concesso tramite una policy bucket.

Accedere alla procedura guidata Crea utente

Fasi

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

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



2. Selezionare **Crea utente**.

Immettere le credenziali

Fasi

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

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

Campo	Descrizione
Password e Conferma password	La password che l'utente utilizzerà inizialmente al momento dell'accesso.
Negare l'accesso	<p>Selezionare Sì per impedire a questo utente di accedere all'account tenant, anche se potrebbe ancora appartenere a uno o più gruppi.</p> <p>Ad esempio, selezionare Sì per sospendere temporaneamente la possibilità di accesso dell'utente.</p>

2. Selezionare **continua**.

Assegnare ai gruppi

Fasi

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

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

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

2. Selezionare **Crea utente**.

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e ci si trova nella griglia di origine del tenant, il nuovo utente locale viene clonato nella griglia di destinazione del tenant.

Success viene visualizzato come **Cloning status** nella sezione Overview della pagina dei dettagli dell'utente.

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

Visualizzare o modificare l'utente locale


Fasi

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

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

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

3. Se si desidera modificare il nome completo dell'utente:
 - a. Selezionare la casella di controllo dell'utente.
 - b. Selezionare **azioni > Modifica nome completo**.

- c. Inserire il nuovo nome.
 - d. Selezionare **Salva modifiche**.
4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:
- Selezionare il nome utente.
 - Selezionare la casella di controllo dell'utente e selezionare **azioni > Visualizza dettagli utente**.
5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
- Nome completo
 - Nome utente
 - Tipo di utente
 - Accesso negato
 - Modalità di accesso
 - Appartenenza al gruppo
 - Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e l'utente viene visualizzato nella griglia di origine del tenant:
 - Stato di cloning, **Success** o **Failure**
 - Un banner blu che indica che se modifichi questo utente, le modifiche non verranno sincronizzate con l'altra griglia.
6. Modificare le impostazioni utente in base alle esigenze. Vedere [Creare un utente locale](#) per i dettagli su cosa immettere.
- a. Nella sezione Panoramica , modificare il nome completo selezionando il nome o l'icona di modifica  .
- Impossibile modificare il nome utente.
- b. Nella scheda **Password**, modificare la password dell'utente e selezionare **Salva modifiche**.
 - c. Nella scheda **accesso**, selezionare **No** per consentire all'utente di accedere o selezionare **Sì** per impedire all'utente di accedere. Quindi, selezionare **Salva modifiche**.
 - d. Nella scheda **tasti di accesso**, selezionare **Crea tasto** e seguire le istruzioni per "[Creazione delle chiavi di accesso S3 di un altro utente](#)".
 - e. Nella scheda **gruppi**, selezionare **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai gruppi. Quindi, selezionare **Save Changes** (Salva modifiche).
7. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Importa utenti federati

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

Fasi

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

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

4. Selezionare **Importa**.

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

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

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

Utente locale duplicato

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



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

Fasi

- Selezionare **Gestione accessi > Utenti**.
- Selezionare la casella di controllo dell'utente che si desidera duplicare.
- Selezionare **azioni > utente duplicato**.
- Vedere [Creare un utente locale](#) per i dettagli su cosa immettere.
- Selezionare **Crea utente**.

Riprova clone utente

Per riprovare un clone non riuscito:

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

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

Eliminare uno o più utenti locali

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



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



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

Fasi

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

Viene visualizzata una finestra di dialogo di conferma.

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

Gestire le chiavi di accesso S3

Gestire le chiavi di accesso S3

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

Le chiavi di accesso S3 possono essere gestite come segue:

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

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

Creare le proprie chiavi di accesso S3

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

rimosse automaticamente.

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



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

Fasi

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

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

2. Selezionare **Crea chiave**.

3. Effettuare una delle seguenti operazioni:

- Selezionare **non impostare una scadenza** per creare una chiave che non scadrà. (Impostazione predefinita)
- Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.



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

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

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

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



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

6. Selezionare **fine**.

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

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

Visualizzare le chiavi di accesso S3

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



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

Prima di iniziare

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

Fasi

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

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

Le chiavi scadute vengono rimosse automaticamente.

Eliminare le proprie chiavi di accesso S3

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

Prima di iniziare

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



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

Fasi

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

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

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

Creare le chiavi di accesso S3 di un altro utente

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

Prima di iniziare

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

A proposito di questa attività

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

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

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



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

Fasi

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

Viene visualizzata la pagina User Detail (Dettagli utente).

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

4. Effettuare una delle seguenti operazioni:

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



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

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

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

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



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

7. Selezionare **fine**.

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

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

Visualizzare le chiavi di accesso S3 di un altro utente

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

Prima di iniziare

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



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

Fasi

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

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

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

Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

- ["Creare le chiavi di accesso S3 di un altro utente"](#)
- ["Eliminare le chiavi di accesso S3 di un altro utente"](#)

Eliminare le chiavi di accesso S3 di un altro utente

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

Prima di iniziare

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



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

Fasi

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

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

Gestire i bucket S3

Creare un bucket S3

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

Prima di iniziare

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



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

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



Ogni griglia può avere un massimo di 100.000 bucket, inclusi ["secchi di rami"](#).

Accedere alla procedura guidata

Fasi

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

Inserire i dettagli

Fasi

1. Inserire i dettagli del bucket.

Campo	Descrizione
Nome bucket	<p>Un nome per il bucket conforme alle seguenti regole:</p> <ul style="list-style-type: none">• Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).• Deve essere conforme al DNS.• Deve contenere almeno 3 e non più di 63 caratteri.• Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini.• Non deve contenere periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. <p>Per ulteriori informazioni, vedere "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione del bucket".</p> <p>Nota: 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. Se la regione predefinita è configurata su una regione diversa da <code>us-east-1</code>, questa altra regione viene inizialmente selezionata nel menu a discesa.</p> <p>Nota: Non è possibile modificare l'area dopo aver creato il bucket.</p>

2. Selezionare **continua**.

Gestire le impostazioni

Fasi

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

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

È necessario abilitare il controllo delle versioni degli oggetti se:

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

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

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



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

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

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



L'amministratore di rete deve concedere l'autorizzazione a "[Utilizzare funzioni specifiche di blocco oggetti S3](#)".

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

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

Modalità di conservazione predefinita	Descrizione
Governance	<ul style="list-style-type: none">• Gli utenti con <code>s3:BypassGovernanceRetention</code> autorizzazione possono utilizzare l' <code>`x-amz-bypass-governance-retention: true`</code> intestazione della richiesta per ignorare le impostazioni di conservazione.• Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.• Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.
Conformità	<ul style="list-style-type: none">• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.• La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.• La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. <p>Nota: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.</p>

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

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

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

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

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

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

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

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

6. Selezionare **Crea bucket**.

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

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

Puoi anche ["creare bucket di rami"](#) secondo necessità.

Visualizza i dettagli del bucket

È possibile visualizzare i bucket nell'account tenant.

Prima di iniziare

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

Fasi

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

Viene visualizzata la pagina Bucket.

2. Rivedere la tabella di riepilogo per ciascun bucket.

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



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

Nome

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

Funzionalità attivate

L'elenco delle funzioni attivate per il bucket.

Blocco oggetti S3

Se S3 Object Lock è attivato per il bucket.

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

Regione

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

Numero di oggetti

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

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

Spazio utilizzato

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

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

Utilizzo

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

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

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

Capacità

Se impostato, il limite di capacità per la benna.

Data di creazione

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

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



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

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

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

bucket.

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

Cos'è un branch bucket?

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

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

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

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

Si noti le seguenti caratteristiche dei bucket di diramazione:

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

Esempi di utilizzo del bucket di diramazione

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

Operazioni sugli oggetti nei bucket di diramazione

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

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

Fare riferimento anche a ["Modalità di eliminazione degli oggetti con versione S3"](#).

Gestisci i bucket delle filiali

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

Prima di iniziare

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

A proposito di questa attività

Notare le seguenti informazioni per i bucket di diramazione:

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



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

Crea bucket di diramazione

Fasi

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

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

Inserire i dettagli

Fasi

1. Inserisci i dettagli per il bucket della filiale.

Campo	Descrizione
Nome del bucket di filiale	<p>Un nome per il bucket di diramazione che rispetti queste regole:</p> <ul style="list-style-type: none"> • Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). • Deve essere conforme al DNS. • Deve contenere almeno 3 e non più di 63 caratteri. • Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. • Non deve contenere periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. <p>Per ulteriori informazioni, vedere "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione del bucket".</p> <p>Nota: non è possibile modificare il nome dopo aver creato il bucket di diramazione.</p>
Regione (non modificabile per i bucket di filiale)	<p>Regione del bucket del ramo.</p> <p>La regione del bucket di diramazione deve corrispondere alla regione del bucket di base, pertanto questo campo è disabilitato per i bucket di diramazione.</p>
Prima del tempo	<p>Tempo limite entro il quale le versioni degli oggetti create nel bucket di base devono essere accessibili dal bucket di diramazione. Il bucket branch fornisce l'accesso alle versioni degli oggetti create prima del tempo Prima.</p> <p>Prima del tempo deve esserci una data e un'ora trascorse. Non può essere una data futura.</p>
Tipo di secchio per rami	<ul style="list-style-type: none"> • Lettura-scrittura: è possibile aggiungere o eliminare oggetti o versioni di oggetti nel bucket del ramo. • Sola lettura: non è possibile modificare gli oggetti nel bucket del ramo. <p>Nota: è possibile impostare il tipo di bucket di diramazione su sola lettura solo se il bucket di diramazione è vuoto. Se il tipo per un bucket di branch esistente è impostato su lettura-scrittura e non hai scritto su di esso, puoi modificare il tipo in sola lettura.</p>

2. Selezionare **continua**.

Gestisci le impostazioni dell'oggetto (facoltativo)

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

Fasi

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

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

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



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

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



L'amministratore di rete deve concedere l'autorizzazione a ["Utilizzare funzioni specifiche di blocco oggetti S3"](#).

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

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

Modalità di conservazione predefinita	Descrizione
Governance	<ul style="list-style-type: none">• Gli utenti con <code>s3:BypassGovernanceRetention</code> autorizzazione possono utilizzare l' <code>`x-amz-bypass-governance-retention: true`</code> intestazione della richiesta per ignorare le impostazioni di conservazione.• Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.• Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.
Conformità	<ul style="list-style-type: none">• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.• La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.• La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. <p>Nota: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.</p>

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

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

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

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

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

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

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



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

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

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



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

5. Selezionare **Crea bucket**.

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

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

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

Applicare un tag di criterio ILM a un bucket

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

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



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

Prima di iniziare

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

Fasi

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

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

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

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



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

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



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

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



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



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



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

Gestire le policy del bucket

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

Prima di iniziare

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

Fasi

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

Ogni criterio bucket ha un limite di dimensioni di 20.480 byte.
 - Modificare un criterio esistente modificando la stringa.
 - Disattivare un criterio deselectando **attiva criterio**.

Per informazioni dettagliate sui criteri bucket, inclusi esempi e sintassi del linguaggio, vedere ["Esempio di policy bucket"](#).

Gestire la coerenza del bucket

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

Prima di iniziare

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

Linee guida per la coerenza della benna

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

modificare la coerenza del bucket

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



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

Fasi

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

2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **.

4. Selezionare una coerenza per le operazioni eseguite sugli oggetti in questo bucket.

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

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

Cosa accade quando si modificano le impostazioni della benna

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

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

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



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

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

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



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

Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso

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

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

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

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



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

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

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

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

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

Richiesta di copia di un oggetto da un bucket all'altro	<ul style="list-style-type: none"> • No, per la copia di origine • Sì, per la copia di destinazione 	<ul style="list-style-type: none"> • No, per la copia di origine • Sì, per la copia di destinazione 	<ul style="list-style-type: none"> • Sì, per la copia di origine • Sì, per la copia di destinazione 	<ul style="list-style-type: none"> • Sì, per la copia di origine • Sì, per la copia di destinazione
Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Fasi

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

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

Modificare la versione degli oggetti per un bucket

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

Prima di iniziare

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

A proposito di questa attività

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

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

Per ulteriori informazioni, vedere quanto segue:

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

- "Modalità di eliminazione degli oggetti"

Fasi

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

Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

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

USA il blocco oggetti S3 per conservare gli oggetti

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



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

Che cos'è il blocco oggetti S3?

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

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

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

Un bucket con blocco oggetti S3 può avere oggetti con e senza impostazioni di conservazione specificate

dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

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

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

Modalità di conservazione

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

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

Impostazioni di conservazione per le versioni degli oggetti

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

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



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

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

Impostazione di conservazione predefinita per i bucket

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

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

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

Vedere ["Creare un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).

S3 attività di blocco degli oggetti

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

Amministratore di grid

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

Utente tenant

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

Requisiti per i bucket con S3 Object Lock attivato

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

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

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

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

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

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

1. Acquisizione oggetto

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

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

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

2. Conservazione ed eliminazione degli oggetti

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

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

Posso comunque gestire i bucket conformi alle versioni precedenti?

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

Aggiorna la conservazione predefinita del blocco oggetti S3

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

Prima di iniziare

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

Fasi

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

Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

Modalità di conservazione predefinita	Descrizione
Governance	<ul style="list-style-type: none"> • Gli utenti con <code>s3:BypassGovernanceRetention</code> autorizzazione possono utilizzare l' <code>`x-amz-bypass-governance-retention: true`</code> intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.
Conformità	<ul style="list-style-type: none"> • L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. <p>Nota: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.</p>

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

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

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

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

Configurare StorageGRID CORS per bucket e oggetti

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

Prima di iniziare

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

- ["Autorizzazione di accesso root"](#) Fornisce l'accesso a tutte le richieste di configurazione CORS.

A proposito di questa attività

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

`http://www.example.com`.

Abilitare il CORS per un bucket

Fasi

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

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

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

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

Viene visualizzata la pagina dei dettagli del bucket.

4. Dalla scheda **bucket access**, selezionare la fisarmonica **Cross-Origin Resource Sharing (CORS)**.
5. Selezionare la casella di controllo **Enable CORS** (attiva CORS*).
6. Incollare l'XML di configurazione CORS nella casella di testo.

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

Modificare l'impostazione CORS

Fasi

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

Disattiva l'impostazione CORS

Fasi

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

Informazioni correlate

["Configurare StorageGRID CORS per un'interfaccia di gestione"](#)

Eliminare gli oggetti nel bucket

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

Considerazioni e requisiti

Prima di eseguire questa procedura, tenere presente quanto segue:

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



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

- Durante l'eliminazione degli oggetti, lo stato del bucket è **eliminazione degli oggetti: Sola lettura**. In questo stato, non è possibile aggiungere nuovi oggetti al bucket.
- Una volta cancellati tutti gli oggetti, il bucket rimane in stato di sola lettura. È possibile eseguire una delle seguenti operazioni:
 - Riportare il bucket in modalità di scrittura e riutilizzarlo per nuovi oggetti
 - Eliminare il bucket
 - Mantenere il bucket in modalità di sola lettura per riservare il proprio nome per un utilizzo futuro
- Se in un bucket è attivata la versione oggetto, è possibile rimuovere i marcatori di eliminazione creati in StorageGRID 11,8 o versioni successive utilizzando le operazioni Elimina oggetti nel bucket.
- Se in un bucket è attivata la versione oggetto, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11,7 o versioni precedenti. Vedere le informazioni

sull'eliminazione di oggetti in un bucket in ["Modalità di eliminazione degli oggetti con versione S3"](#).

- Se si utilizza ["replica cross-grid"](#), tenere presente quanto segue:
 - L'utilizzo di questa opzione non elimina alcun oggetto dal bucket dell'altra griglia.
 - Se si seleziona questa opzione per il bucket di origine, l'avviso **errore replica cross-grid** verrà attivato se si aggiungono oggetti al bucket di destinazione sull'altra griglia. Se non è possibile garantire che nessuno aggiungerà oggetti al bucket sull'altra griglia, ["disattiva la replica cross-grid"](#) per quel bucket prima di eliminare tutti gli oggetti bucket.

Prima di iniziare

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

Fasi

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

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

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

Menu delle azioni

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

Pagina dei dettagli

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

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

Dopo alcuni minuti:

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

Buckets > my-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

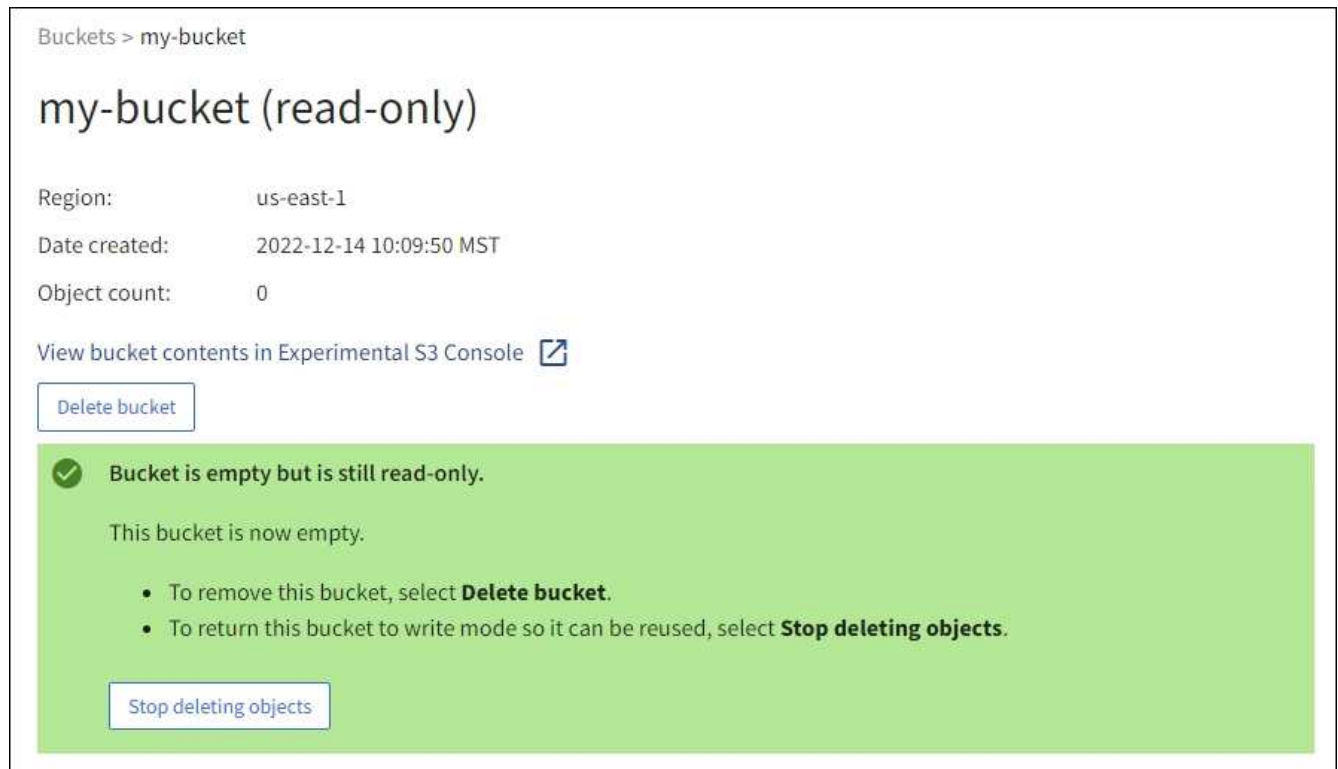
Success
Starting to delete objects from one bucket.

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

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

- Attendere il completamento dell'operazione.

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



7. Effettuare una delle seguenti operazioni:

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



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

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

Elimina bucket S3

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

Prima di iniziare

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

A proposito di questa attività

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

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

Fasi

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

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

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

Menu delle azioni

- a. Selezionare la casella di controllo per ciascun bucket che si desidera eliminare.
- b. Selezionare **azioni > Elimina bucket**.

Pagina dei dettagli

- a. Selezionare il nome di un bucket per visualizzarne i dettagli.
- b. Selezionare **Delete bucket** (Elimina bucket).

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

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

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

Utilizzare la console S3

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

La console S3 consente di:

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

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



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

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

Prima di iniziare

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

Fasi

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

Ulteriori informazioni

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

Gestire i servizi della piattaforma S3

Servizi della piattaforma S3

Panoramica e considerazioni sui servizi di piattaforma

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

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

Panoramica dei servizi della piattaforma

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

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

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



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

Modalità di configurazione dei servizi della piattaforma

I servizi della piattaforma comunicano con endpoint esterni configurati tramite ["Manager tenant"](#) o il ["API di gestione del tenant"](#). Ogni endpoint rappresenta una destinazione esterna, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento Amazon SNS, un endpoint webhook o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

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

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

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

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

Servizio di piattaforma	API REST S3	Fare riferimento a.
Replica di CloudMirror	<ul style="list-style-type: none"> • GetBucketReplication • PutBucketReplication 	<ul style="list-style-type: none"> • "Replica di CloudMirror" • "Operazioni sui bucket"
Notifiche	<ul style="list-style-type: none"> • GetBucketNotificationConfiguration • PutBucketNotificationConfiguration 	<ul style="list-style-type: none"> • "Notifiche" • "Operazioni sui bucket"
Integrazione della ricerca	<ul style="list-style-type: none"> • OTTENERE la configurazione della notifica dei metadati del bucket • INSERIRE la configurazione della notifica dei metadati del bucket 	<ul style="list-style-type: none"> • "Integrazione della ricerca" • "Operazioni personalizzate di StorageGRID"

Considerazioni sull'utilizzo dei servizi della piattaforma

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

Considerazione	Dettagli
Garanzie di ordinazione	<p>StorageGRID garantisce l'ordine delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni relative a un oggetto si trovano all'interno dello stesso sito, lo stato finale dell'oggetto (per la replica) sarà sempre uguale allo stato in StorageGRID.</p> <p>StorageGRID tenta al meglio di ordinare le richieste quando le operazioni vengono eseguite nei siti StorageGRID. Ad esempio, se si scrive inizialmente un oggetto nel sito A e successivamente si sovrascrive lo stesso oggetto nel sito B, l'oggetto finale replicato da CloudMirror nel bucket di destinazione non è garantito come l'oggetto più recente.</p>
Eliminazioni di oggetti basate su ILM	<p>Per far fronte al comportamento di eliminazione del CRR AWS e del servizio di notifica Amazon Simple, CloudMirror e le richieste di notifica degli eventi non vengono inviate quando un oggetto nel bucket di origine viene eliminato a causa delle regole ILM di StorageGRID. Ad esempio, se una regola ILM elimina un oggetto dopo 14 giorni, non viene inviata alcuna richiesta di notifica di CloudMirror o di evento.</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, il TLS reciproco non è supportato. Di conseguenza, se si è <code>ssl.client.auth</code> impostato su <code>required</code> nella configurazione del broker Kafka, potrebbero verificarsi problemi di configurazione degli 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 per nome utente e password.</p> <ul style="list-style-type: none"> • SASL/SEMPlice • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 <p>Nota: le impostazioni 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 della replica	StorageGRID non supporta la <code>x-amz-replication-status</code> testata.

Considerazione	Dettagli
Dimensione dell'oggetto	<p>La dimensione massima per gli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è 5 TiB, che corrisponde alla dimensione massima dell'oggetto <i>supportata</i>.</p> <p>Nota: La dimensione massima <i>raccomandata</i> per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.</p>
Versioni e ID della versione del bucket	<p>Se il bucket S3 di origine in StorageGRID ha attivato la versione, è necessario attivare anche la versione per il bucket di destinazione.</p> <p>Quando si utilizza la versione, tenere presente che l'ordinamento delle versioni degli oggetti nel bucket di destinazione è il massimo sforzo e non garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3.</p> <p>Nota: Gli ID della versione per il bucket di origine in StorageGRID non sono correlati agli ID della versione per il bucket di destinazione.</p>
Tagging per le versioni degli oggetti	<p>Il servizio CloudMirror non replica le richieste PutObjectTagging o DeleteObjectTagging che forniscono un ID di versione, a causa delle limitazioni del protocollo S3. Poiché gli ID di versione per l'origine e la destinazione non sono correlati, non esiste alcun modo per garantire che venga replicato un aggiornamento del tag a un ID di versione specifico.</p> <p>Al contrario, il servizio CloudMirror replica le richieste PutObjectTagging o DeleteObjectTagging che non specificano un ID di versione. Queste richieste aggiornano i tag per la chiave più recente (o la versione più recente se il bucket è in versione). Vengono replicati anche i normali ingest con tag (senza tagging degli aggiornamenti).</p>
Caricamenti e valori multiparte ETag	<p>Quando si esegue il mirroring degli oggetti caricati utilizzando un caricamento multiparte, il servizio CloudMirror non conserva le parti. Di conseguenza, il ETag valore per l'oggetto speculare sarà diverso dal ETag valore dell'oggetto originale.</p>
Oggetti crittografati con SSE-C (crittografia lato server con chiavi fornite dal cliente)	<p>Il servizio CloudMirror non supporta oggetti crittografati con SSE-C. se si tenta di acquisire un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione non riesce.</p>
Bucket con blocco oggetti S3 attivato	<p>La replica non è supportata per i bucket di origine o di destinazione con blocco oggetti S3 attivato.</p>

Comprendere il servizio di replica CloudMirror

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

Ad esempio, è possibile utilizzare la replica di CloudMirror per eseguire il mirroring di record specifici dei clienti

in Amazon S3 e sfruttare i servizi AWS per eseguire analisi dei dati.



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

CloudMirror e ILM

La replica CloudMirror funziona indipendentemente dalle policy ILM attive del grid. Il servizio CloudMirror replica gli oggetti memorizzati nel bucket di origine e li consegna al bucket di destinazione il prima possibile. La consegna degli oggetti replicati viene attivata quando l'acquisizione degli oggetti ha esito positivo.

CloudMirror e replica cross-grid

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

Bucket Cloud Mirror e S3

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

Bucket esistenti

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



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

Bucket multipli di destinazione

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

Benne in versione o non in versione

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

Eliminazione, loop di replica ed eventi

Comportamento di eliminazione

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

Protezione dai loop di replica

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



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

Eventi nel bucket di destinazione

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

Comprendere le notifiche per i bucket

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

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

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

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

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

- Sono supportati i seguenti tipi di evento:
 - S3:ObjectCreated:
 - s3:ObjectCreated:put
 - s3:ObjectCreated:Post
 - s3:ObjectCreated:Copy
 - s3:ObjectCreated:CompleteMultipartUpload
 - S3:ObjectRemoved:
 - s3:ObjectRemoved:Elimina
 - s3:ObjectRemoved>DeleteMarkerCreated
 - s3:ObjectRestore:Post

- Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ma non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nella tabella:

Nome della chiave	Valore StorageGRID
EventSource	sgws:s3
AwsRegion	<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 attivare l'integrazione della ricerca per un bucket S3 se si desidera utilizzare un servizio di ricerca e analisi dei dati esterno per i metadati degli oggetti.

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

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

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



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

Integrazione di ricerca e bucket S3

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

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



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

Cerca notifiche

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

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

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

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

Servizio di integrazione della ricerca ed Elasticsearch

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

Gestire gli endpoint dei servizi della piattaforma

Configurare gli endpoint dei servizi della piattaforma

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

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

Che cos'è un endpoint di servizi di piattaforma?

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

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

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

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

Endpoint per la replica di CloudMirror

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

Endpoint per le notifiche

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

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

Endpoint per il servizio di integrazione della ricerca

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

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

Informazioni correlate

["Amministrare StorageGRID"](#)

Specificare URN per l'endpoint dei servizi della piattaforma

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

endpoint deve essere univoco.

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

Elementi DI URNA

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

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

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

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

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

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

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

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

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

Urns per i servizi ospitati su AWS e GCP

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

- Replica di CloudMirror:

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

- Notifiche:

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

- Integrazione della ricerca:

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



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

Urns per servizi in hosting locale

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

- Replica di CloudMirror:

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

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

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

- Notifiche:

Specificare un endpoint di Amazon Simple Notification Service:

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

Specificare un endpoint Kafka:

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

Specificare un endpoint webhook:

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

- Integrazione della ricerca:

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



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

Creare endpoint di servizi di piattaforma

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

Prima di iniziare

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



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

- Nome risorsa univoco (URN)

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

- Credenziali di autenticazione (se richieste):

Endpoint di integrazione della ricerca

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

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

Endpoint di replica CloudMirror

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

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

Endpoint Amazon SNS

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

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

Endpoint Kafka

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

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

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

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

Fasi

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

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

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

Utilizzare uno dei seguenti formati:

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

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

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

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

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

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



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

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

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



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

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



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

6. Selezionare **continua**.

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



Se si desidera l'autenticazione per gli endpoint webhook, configurare Mutual Transport Layer Security (mTLS) in [Fase 9](#).

Endpoint di integrazione della ricerca

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

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

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

Endpoint di replica CloudMirror

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

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

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

Endpoint Amazon SNS

Immettere o caricare le credenziali per un endpoint Amazon SNS.

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	<ul style="list-style-type: none">• ID chiave di accesso• Chiave di accesso segreta

Endpoint Kafka

Immettere o caricare le credenziali per un endpoint Kafka.

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
SASL/SEMPlice	Utilizza un nome utente e una password con testo normale per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none">• Nome utente• Password
SASL/SCRAM-SHA-256	Utilizza un nome utente e una password utilizzando un protocollo di risposta alla verifica e l'hash SHA-256 per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none">• Nome utente• Password
SASL/SCRAM-SHA-512	Utilizza un nome utente e una password utilizzando un protocollo di risposta alla verifica e l'hash SHA-512 per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none">• Nome utente• Password

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

8. Selezionare **continua**.

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

La maggior parte degli endpoint

Verificare la connessione TLS per l'integrazione della ricerca, la replica di CloudMirror, Amazon SNS o gli endpoint Kafka.

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

Solo endpoint webhook

Verificare la connessione TLS per gli endpoint webhook.

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

Selezionando **mTLS**, queste opzioni diventano disponibili.

Tipo di verifica del certificato	Descrizione
Non verificare il certificato del server	Disabilita la verifica del certificato del server, il che significa che l'identità del server non viene verificata. Questa opzione non è sicura.
Certificato del client	Il certificato client viene utilizzato per verificare l'identità del client durante la connessione all'endpoint.

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

10. Selezionare **Test e creare endpoint**.

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



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

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

Informazioni correlate

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

Verifica della connessione per l'endpoint dei servizi della piattaforma

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

Prima di iniziare

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

A proposito di questa attività

StorageGRID non convalida che le credenziali dispongano delle autorizzazioni corrette.

Fasi

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

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

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

Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Test di connessione**.

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

Modifica dell'endpoint dei servizi della piattaforma

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

Prima di iniziare

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

Fasi

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

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


2. Selezionare l'endpoint che si desidera modificare.

Viene visualizzata la pagina dei dettagli dell'endpoint.

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



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

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



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

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

5. Selezionare **Test e salvare le modifiche**.

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

Eliminare l'endpoint dei servizi della piattaforma

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

Prima di iniziare

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

Fasi

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

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

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



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

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

Viene visualizzato un messaggio di conferma.

4. Selezionare **Delete endpoint** (Elimina endpoint).

Risolvere gli errori degli endpoint dei servizi della piattaforma

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi della piattaforma, viene visualizzato un messaggio sul dashboard. Nella pagina Platform Services Endpoint, la colonna Last error (ultimo errore) indica per quanto tempo si è verificato l'errore. Se le autorizzazioni associate alle credenziali di un endpoint non sono corrette, non viene visualizzato alcun errore.

Determinare se si è verificato un errore

Se si sono verificati errori degli endpoint dei servizi della piattaforma negli ultimi 7 giorni, la dashboard di Tenant Manager visualizza un messaggio di avviso. Per ulteriori informazioni sull'errore, visitare la pagina relativa agli endpoint dei servizi della piattaforma.



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 visualizzato nella dashboard viene visualizzato anche nella parte superiore della pagina Platform Services Endpoint. Per visualizzare un messaggio di errore più dettagliato:

Fasi

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

Controllare se l'errore è ancora aggiornato

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

Fasi

1. Selezionare l'endpoint.

Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Selezionare **connessione** > **verifica connessione**.

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

Risolvi gli errori degli endpoint

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

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

Fasi

1. Selezionare l'endpoint.
2. Nella pagina dei dettagli dell'endpoint, selezionare **Configurazione**.
3. Modificare la configurazione dell'endpoint in base alle necessità.

4. Selezionare **connessione > verifica connessione**.

Credenziali endpoint con autorizzazioni insufficienti

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

Informazioni correlate

- [Amministrare StorageGRID > risolvere i problemi relativi ai servizi della piattaforma](#)
- ["Creare endpoint di servizi di piattaforma"](#)
- ["Verifica della connessione per l'endpoint dei servizi della piattaforma"](#)
- ["Modifica dell'endpoint dei servizi della piattaforma"](#)

Configurare la replica di CloudMirror

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

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- È già stato creato un bucket per fungere da origine della replica.
- L'endpoint che si intende utilizzare come destinazione per la replica CloudMirror esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

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

Per informazioni generali sulla replica bucket e su come configurarla, vedere ["Documentazione di Amazon Simple Storage Service \(S3\): Replica di oggetti"](#). Per informazioni sull'implementazione di GetBucketReplication, DeleteBucketReplication e PutBucketReplication da parte di StorageGRID, vedere ["Operazioni sui bucket"](#).



La replica di CloudMirror presenta importanti analogie e differenze con la funzionalità di replica cross-grid. Per ulteriori informazioni, vedere ["Confronta la replica cross-grid e la replica CloudMirror"](#).

Durante la configurazione della replica di CloudMirror, osservare i seguenti requisiti e caratteristiche:

- Quando si crea e si applica un XML di configurazione di replica bucket valido, è necessario utilizzare l'URN di un endpoint bucket S3 per ogni destinazione.
- La replica non è supportata per i bucket di origine o di destinazione con blocco oggetti S3 attivato.
- Se si attiva la replica CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket

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

- Se si specifica una classe di storage nell'XML di configurazione della replica, StorageGRID utilizza tale classe quando esegue operazioni sull'endpoint S3 di destinazione. L'endpoint di destinazione deve supportare anche la classe di storage specificata. Assicurarsi di seguire le raccomandazioni fornite dal vendor del sistema di destinazione.

Fasi

1. Abilita la replica per il bucket di origine:

- Utilizzare un editor di testo per creare l'XML di configurazione della replica richiesto per attivare la replica, come specificato nell'API di replica S3.
- Durante la configurazione dell'XML:
 - Tenere presente che StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo dell'`Filter` elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, consultare la documentazione di Amazon sulla configurazione della replica.
 - Utilizzare l'URN di un endpoint del bucket S3 come destinazione.
 - Se lo si desidera, aggiungere l'`<StorageClass>` elemento e specificare una delle seguenti opzioni:
 - **STANDARD:** La classe di archiviazione predefinita. Se non si specifica una classe di archiviazione quando si carica un oggetto, viene utilizzata la **STANDARD** classe di archiviazione.
 - **STANDARD_IA:** (Accesso standard - non frequente) Utilizza questa classe di storage per i dati a cui si accede meno frequentemente, ma che richiedono comunque un accesso rapido quando necessario.
 - **REDUCED_REDUNDANCY:** Utilizzare questa classe di archiviazione per i dati non critici e riproducibili che possono essere memorizzati con una ridondanza minore rispetto alla **STANDARD** classe di archiviazione.
- Se si specifica un nell'XML di configurazione, **Role** questo verrà ignorato. Questo valore non viene utilizzato da StorageGRID.

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

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

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Replication**.
5. Selezionare la casella di controllo **Enable Replication** (attiva replica).
6. Incollare il file XML di configurazione della replica nella casella di testo e selezionare **Save changes** (Salva modifiche).



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

7. Verificare che la replica sia configurata correttamente:
 - a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per la replica come specificato nella configurazione della replica.

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

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

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

Informazioni correlate

["Creare endpoint di servizi di piattaforma"](#)

Configurare le notifiche degli eventi

È possibile attivare le notifiche per un bucket creando un XML di configurazione delle notifiche e utilizzando Gestione tenant per applicare il file XML a un bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- Hai già creato un bucket per fungere da origine delle notifiche.
- L'endpoint che si intende utilizzare come destinazione per le notifiche degli eventi esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

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

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

Durante la configurazione delle notifiche degli eventi per un bucket, osservare i seguenti requisiti e caratteristiche:

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

Fasi

1. Abilita le notifiche per il bucket di origine:

- Utilizzare un editor di testo per creare l'XML di configurazione delle notifiche richiesto per attivare le notifiche degli eventi, come specificato nell'API di notifica S3.
- Quando si configura l'XML, utilizzare l'URN di un endpoint di notifica degli eventi come argomento di destinazione.

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

2. In Tenant Manager, selezionare **STORAGE (S3) > Bucket**.

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Event Notifications**.

5. Selezionare la casella di controllo **attiva notifiche eventi**.

6. Incollare l'XML di configurazione della notifica nella casella di testo e selezionare **Salva modifiche**.



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

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

- a. Eseguire un'azione su un oggetto nel bucket di origine che soddisfi i requisiti per l'attivazione di una notifica come configurato nel XML di configurazione.

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

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

Ad esempio, se l'argomento di destinazione è ospitato su Amazon SNS, è possibile configurare il servizio in modo che invii un'e-mail al momento della consegna della notifica.

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "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"](#)

- ["Creare endpoint di servizi di piattaforma"](#)

Configurare il servizio di integrazione della ricerca

È possibile abilitare l'integrazione della ricerca per un bucket creando l'integrazione della ricerca XML e utilizzando Tenant Manager per applicare l'XML al bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- È già stato creato un bucket S3 di cui si desidera indicizzare il contenuto.
- L'endpoint che si intende utilizzare come destinazione per il servizio di integrazione della ricerca esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

Dopo aver configurato il servizio di integrazione della ricerca per un bucket di origine, la creazione di un oggetto o l'aggiornamento dei metadati o dei tag di un oggetto attiva l'invio dei metadati dell'oggetto all'endpoint di destinazione.

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

Fasi

1. Consentire l'integrazione della ricerca per un bucket:

- Utilizzare un editor di testo per creare l'XML di notifica dei metadati necessario per abilitare l'integrazione della ricerca.
- Quando si configura l'XML, utilizzare l'URN di un endpoint di integrazione della ricerca come destinazione.

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

Se necessario, fare riferimento alla [Esempi di XML di configurazione dei metadati](#).

```

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

```

Elementi nella configurazione della notifica dei metadati XML:

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	<p>Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati.</p> <p>Contiene uno o più elementi della regola.</p>	Sì
Regola	<p>Tag container 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 della regola.</p> <p>Incluso nell'elemento Rule.</p>	No
Stato	<p>Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Prefisso	<p>Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata.</p> <p>Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Destinazione	<p>Tag container per la destinazione di una regola.</p> <p>Incluso nell'elemento Rule.</p>	Sì

Nome	Descrizione	Obbligatorio
Urna	<p>URNA della destinazione in 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"> • <code>es</code> deve essere il terzo elemento. • L'URN deve terminare con l'indice e digitare dove sono memorizzati i metadati, nel formato <code>domain-name/myindex/mytype</code>. <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404.</p> <p>L'URN è incluso nell'elemento Destination.</p>	Sì

2. In Tenant Manager, selezionare **STORAGE (S3) > Bucket**.

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Search Integration**

5. Selezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).

6. Incollare la configurazione di notifica dei metadati nella casella di testo e selezionare **Salva modifiche**.



I servizi della piattaforma devono essere attivati per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che il servizio di integrazione della ricerca sia configurato correttamente:

- Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per l'attivazione di una notifica dei metadati come specificato nel file XML di configurazione.

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

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

Al termine

Se necessario, è possibile disattivare l'integrazione della ricerca per un bucket utilizzando uno dei seguenti

metodi:

- Selezionare **STORAGE (S3) > Bucket** e deselezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).
- Se si utilizza direttamente l'API S3, utilizzare una richiesta DI notifica DELETE Bucket metadata. Consultare le istruzioni per l'implementazione delle applicazioni client S3.

esempio: Configurazione di notifica dei metadati che si applica a tutti gli oggetti

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

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

Esempio: Configurazione della notifica di metadati con due regole

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

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Formato di notifica dei metadati

Quando si attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. La `test` benna non è in versione, quindi l'etichetta `versionId` è vuota.

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

Campi inclusi nel documento JSON

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

Informazioni su bucket e oggetti

bucket: Nome del bucket

key: Nome chiave oggetto

versionID: Versione oggetto, per gli oggetti nei bucket in versione

region: Area bucket, ad esempio us-east-1

Metadati di sistema

size: Dimensione dell'oggetto (in byte) come visibile a un client HTTP

md5: Hash oggetto

Metadati dell'utente

metadata: Tutti i metadati utente per l'oggetto, come coppie chiave-valore

key:value

Tag

tags: Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore

key:value

Come visualizzare i risultati in Elasticsearch

Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o

numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Attivare le mappature dinamiche dei campi nell'indice prima di configurare il servizio di integrazione della ricerca. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

UTILIZZARE L'API REST S3

Versioni e aggiornamenti supportati dall'API REST S3

StorageGRID supporta l'API S3 (Simple Storage Service), implementata come set di servizi Web REST (Representational state Transfer).

Il supporto per l'API REST S3 consente di connettere le applicazioni orientate ai servizi sviluppate per i servizi Web S3 con lo storage a oggetti on-premise che utilizza il sistema StorageGRID. Sono necessarie modifiche minime all'utilizzo corrente delle chiamate API REST S3 da parte di un'applicazione client.

Versioni supportate

StorageGRID supporta le seguenti versioni specifiche di STS, S3 e HTTP:

Elemento	Versione
Specifiche API STS AssumeRole	"Documentazione di Amazon Web Services (AWS): Riferimento API Amazon Assumerole" Per ulteriori informazioni su AssumeRole, fare riferimento a "Imposta AssumeRole" .
Specifica API S3	"Documentazione AWS: Riferimento API di Amazon Simple Storage Service"
HTTP	1,1 Per ulteriori informazioni su HTTP, vedere HTTP/1.1 (RFC 7230-35). "IETF RFC 2616: Protocollo di trasferimento ipertestuale (HTTP/1.1)" Nota: StorageGRID non supporta la pipelining HTTP/1.1.

Aggiornamenti al supporto delle API REST S3

Rilasciare	Commenti
12,0	<ul style="list-style-type: none"> • Aggiunto il supporto per la condivisione delle risorse tra origini (CORS) per un'interfaccia di gestione, che consente a un altro dominio di accedere ai dati in StorageGRID utilizzando le API di gestione. "Scopri di più" . • Aggiunto supporto per STS AssumeRole e policy di sessione. Vedere "un esempio di politica di sessione" . È possibile impostare AssumeRole nei gruppi tenant.
11,9	<ul style="list-style-type: none"> • Aggiunto supporto per valori checksum SHA-256 pre-calcolati per le seguenti richieste e intestazioni supportate. È possibile utilizzare questa funzione per verificare l'integrità degli oggetti caricati: <ul style="list-style-type: none"> ◦ CompleteMultipartUpload: x-amz-checksum-sha256 ◦ CreateMultipartUpload: x-amz-checksum-algorithm ◦ GetObject: x-amz-checksum-mode ◦ HeadObject (scarto capo): x-amz-checksum-mode ◦ ListParts ◦ PutObject: x-amz-checksum-sha256 ◦ UploadPart: x-amz-checksum-sha256 • È stata aggiunta la possibilità per l'amministratore di grid di controllare le impostazioni di conservazione e conformità a livello di tenant. Queste impostazioni influiscono sulle impostazioni di blocco degli oggetti S3. <ul style="list-style-type: none"> ◦ Modalità di conservazione predefinita bucket e modalità di conservazione degli oggetti: Governance o conformità, se consentite dall'amministratore del grid. ◦ Periodo di conservazione predefinito del bucket e conservazione dell'oggetto fino alla data: Deve essere minore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia. • Supporto migliorato per la aws-chunked codifica del contenuto e i valori di streaming x-amz-content-sha256. Limitazioni: <ul style="list-style-type: none"> ◦ Se presente, chunk-signature è facoltativo e non convalidato ◦ Se presente, x-amz-trailer il contenuto viene ignorato
11,8	<p>Aggiornati i nomi delle operazioni S3 in modo che corrispondano ai nomi utilizzati in "Documentazione Amazon Web Services (AWS): Riferimento API Amazon Simple Storage Service" .</p>
11,7	<ul style="list-style-type: none"> • Aggiunto "Riferimento rapido: Richieste API S3 supportate". • Aggiunto supporto per l'utilizzo della modalità DI GOVERNANCE con S3 Object Lock. • Aggiunto supporto per l'intestazione di risposta specifica di StorageGRID x-ntap-sg-cgr-replication-status per le richieste di oggetti GET e HEAD. Questa intestazione fornisce lo stato di replica di un oggetto per la replica cross-grid. • Le richieste SelectObjectContent ora supportano gli oggetti Parquet.

Rilasciare	Commenti
11,6	<ul style="list-style-type: none"> • Aggiunto il supporto per l'utilizzo del <code>partNumber</code> parametro di richiesta nelle richieste GET Object e HEAD Object. • Aggiunto supporto per una modalità di conservazione predefinita e un periodo di conservazione predefinito a livello di bucket per S3 Object Lock. • È stato aggiunto il supporto per <code>s3:object-lock-remaining-retention-days</code> la chiave della condizione della policy per impostare l'intervallo di periodi di conservazione consentiti per gli oggetti. • Modifica della dimensione massima <i>consigliata</i> per un'operazione di singolo oggetto PUT in 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.
11,5	<ul style="list-style-type: none"> • Aggiunto supporto per la gestione della crittografia bucket. • Aggiunto supporto per S3 Object Lock e richieste legacy di Compliance obsolete. • Aggiunto il supporto per l'utilizzo DELL'ELIMINAZIONE di più oggetti nei bucket con versione. • L'`Content-MD5` intestazione della richiesta è ora supportata correttamente.
11,4	<ul style="list-style-type: none"> • Aggiunto supporto per L'ELIMINAZIONE di tag bucket, L'AGGIUNTA DI tag bucket E L'AGGIUNTA di tag bucket. I tag di allocazione dei costi non sono supportati. • Per i bucket creati in StorageGRID 11.4, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. • Aggiunto il supporto per le notifiche bucket sul <code>s3:ObjectRestore:Post</code> tipo di evento. • I limiti di dimensione AWS per le parti multipart vengono ora applicati. Ogni parte di un caricamento multiparte deve essere compresa tra 5 MiB e 5 GiB. L'ultima parte può essere inferiore a 5 MiB. • Aggiunto supporto per TLS 1.3
11,3	<ul style="list-style-type: none"> • Aggiunto supporto per la crittografia lato server dei dati a oggetti con chiavi fornite dal cliente (SSE-C). • Aggiunto supporto per le operazioni di ELIMINAZIONE, RECUPERO e INSERIMENTO DEL ciclo di vita del bucket (solo azione scadenza) e per l'`x-amz-expiration` intestazione della risposta. • Aggiornamento DI PUT object, PUT object - Copy e Multipart Upload per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono durante l'acquisizione. • Le crittografia TLS 1.1 non sono più supportate.

Rilasciare	Commenti
11,2	<p>Aggiunto supporto per il ripristino POST-oggetto da utilizzare con i Cloud Storage Pools. Aggiunto supporto per l'utilizzo della sintassi AWS per ARN, chiavi di condizione dei criteri e variabili dei criteri in policy di gruppo e bucket. Le policy di gruppo e bucket esistenti che utilizzano la sintassi StorageGRID continueranno a essere supportate.</p> <p>Nota: gli utilizzi di ARN/URN in altre configurazioni JSON/XML, inclusi quelli utilizzati nelle funzionalità personalizzate di StorageGRID, non sono cambiati.</p>
11,1	Aggiunto supporto per la condivisione delle risorse tra origini (CORS), HTTP per connessioni client S3 ai nodi di rete e impostazioni di conformità sui bucket.
11,0	Supporto aggiunto per la configurazione dei servizi della piattaforma (replica CloudMirror, notifiche e integrazione della ricerca Elasticsearch) per i bucket. Inoltre, è stato aggiunto il supporto per i vincoli di posizione dei tag degli oggetti per i bucket e la coerenza disponibile.
10,4	Aggiunto supporto per le modifiche di scansione ILM alle versioni, agli aggiornamenti delle pagine dei nomi di dominio degli endpoint, alle condizioni e alle variabili nei criteri, agli esempi di policy e all'autorizzazione PutOverwriteObject.
10,3	Aggiunto supporto per il controllo delle versioni.
10,2	Aggiunto supporto per policy di accesso di gruppo e bucket e per copia multiparte (carica parte - Copia).
10,1	Aggiunto supporto per upload multiparte, richieste virtuali in stile host e autenticazione v4.
10,0	Supporto iniziale dell'API REST S3 da parte del sistema StorageGRID . La versione attualmente supportata del <i>Simple Storage Service API Reference</i> è 2006-03-01.

Riferimento rapido: Richieste API S3 supportate

In questa pagina viene riepilogato il modo in cui StorageGRID supporta le API di Amazon Simple Storage Service (S3).

Questa pagina include solo le operazioni S3 supportate da StorageGRID.



Per visualizzare la documentazione AWS relativa a ciascuna operazione, selezionare il collegamento nell'intestazione.

Parametri di query URI comuni e intestazioni di richiesta

Se non specificato, sono supportati i seguenti parametri di query URI comuni:

- `versionId` (come richiesto per le operazioni a oggetti)

Se non specificato, sono supportate le seguenti intestazioni di richiesta comuni:

- Authorization
- Connection
- Content-Length
- Content-MD5
- Content-Type
- Date
- Expect
- Host
- x-amz-date

Informazioni correlate

- ["Dettagli sull'implementazione dell'API REST S3"](#)
- ["Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni"](#)

"AbortMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre a questo parametro di query URI aggiuntivo:

- uploadId

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni per caricamenti multiparte"](#)

"CompleteMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre a questo parametro di query URI aggiuntivo:

- uploadId
- x-amz-checksum-sha256

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- ChecksumSHA256
- CompleteMultipartUpload
- ETag

- Part
- PartNumber

Documentazione StorageGRID

["CompleteMultipartUpload"](#)

"Oggetto CopyObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-`<metadata-name>`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Oggetto CopyObject"](#)

"CreateBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- x-amz-bucket-object-lock-enabled

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"CreateMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["CreateMultipartUpload"](#)

"DeleteBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteBucketLifecycle"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

- ["Operazioni sui bucket"](#)
- ["Creare la configurazione del ciclo di vita S3"](#)

"DeleteBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteObject (Elimina oggetto)"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre all'intestazione della richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"DeleteObjects"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre all'intestazione della richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"DeleteObjectTagging"

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"GetBucketAcl"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketLifecycleConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

- ["Operazioni sui bucket"](#)
- ["Creare la configurazione del ciclo di vita S3"](#)

"GetBucketLocation"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketNotificationConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketVersioning"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri di query URI aggiuntivi:

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

E queste intestazioni di richiesta aggiuntive:

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["GetObject"](#)

["GetObjectAcl"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

["GetObjectLegalHold"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

["GetObjectLockConfiguration"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

["GetObjectRetention"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

"GetObjectTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"HeadBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"HeadObject (oggetto intestazione)"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- x-amz-checksum-mode
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["HeadObject \(oggetto intestazione\)"](#)

"ListBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

[Operazioni sul servizio](#) > [ListBuckets](#)

"ListMultipartUploads"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["ListMultipartUploads"](#)

"ListObjects (oggetti elenco)"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"ListObjectsV2"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"ListObjectVersions"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"ListParts"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- max-parts

- part-number-marker
- uploadId

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["ListMultipartUploads"](#)

"PutBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"PutBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"PutBucketLifecycleConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentazione StorageGRID

- ["Operazioni sui bucket"](#)
- ["Creare la configurazione del ciclo di vita S3"](#)

"PutBucketNotificationConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Per i dettagli sui campi del corpo JSON supportati, vedere ["Utilizza policy di accesso a bucket e gruppi"](#) .

"PutBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Tag XML del corpo della richiesta

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketVersioning"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Parametri del corpo della richiesta

StorageGRID supporta questi parametri del corpo della richiesta:

- VersioningConfiguration
- Status

Documentazione StorageGRID

"Operazioni sui bucket"

"PutObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Corpo della richiesta

- Dati binari dell'oggetto

Documentazione StorageGRID

"PutObject"

"PutObjectLegalHold"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

"PutObjectLockConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

"PutObjectRetention"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre a questa intestazione aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

"PutObjectTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"RestoreObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Per informazioni dettagliate sui campi corpo supportati, vedere ["RestoreObject"](#).

"SelectObjectContent"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Per ulteriori informazioni sui body field supportati, vedere quanto segue:

- "USA S3 Select"
- "SelectObjectContent"

"UploadPart"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri di query URI aggiuntivi:

- partNumber
- uploadId

E queste intestazioni di richiesta aggiuntive:

- x-amz-checksum-sha256
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

Corpo della richiesta

- Dati binari della parte

Documentazione StorageGRID

"UploadPart"

"UploadPartCopy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri di query URI aggiuntivi:

- partNumber
- uploadId

E queste intestazioni di richiesta aggiuntive:

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match

- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["UploadPartCopy"](#)

Eseguire il test della configurazione dell'API REST S3

Puoi utilizzare l'interfaccia a riga di comando (CLI AWS) di Amazon Web Services per verificare la tua connessione al sistema e verificare che sia possibile leggere e scrivere oggetti.

Prima di iniziare

- È stato scaricato e installato l'interfaccia CLI di AWS da ["aws.amazon.com/cli"](https://aws.amazon.com/cli/).
- In alternativa, si dispone di ["creato un endpoint del bilanciamento del carico"](#). In caso contrario, si conosce l'indirizzo IP del nodo di archiviazione a cui si desidera connettersi e il numero di porta da utilizzare. Vedere ["Indirizzi IP e porte per le connessioni client"](#).
- Si dispone di ["Creato un account tenant S3"](#).
- È stato effettuato l'accesso al tenant e ["ha creato una chiave di accesso"](#) a .

Per ulteriori informazioni su questi passi, vedere ["Configurare le connessioni client"](#).

Fasi

1. Configurare le impostazioni dell'interfaccia utente di AWS per utilizzare l'account creato nel sistema StorageGRID:
 - a. Accedere alla modalità di configurazione: `aws configure`
 - b. Inserire l'ID della chiave di accesso per l'account creato.
 - c. Inserire la chiave di accesso segreta per l'account creato.
 - d. Immettere la regione predefinita da utilizzare. Ad esempio, `us-east-1`.
 - e. Immettere il formato di output predefinito da utilizzare oppure premere **Invio** per selezionare JSON.
2. Creare un bucket.

In questo esempio si presuppone che sia stato configurato un endpoint del bilanciamento del carico per utilizzare l'indirizzo IP 10.96.101.17 e la porta 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Se il bucket viene creato correttamente, viene restituita la posizione del bucket, come mostrato nell'esempio seguente:

```
"Location": "/testbucket"
```

3. Caricare un oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Se l'oggetto viene caricato correttamente, viene restituito un ETAG che rappresenta un hash dei dati dell'oggetto.

4. Elencare i contenuti del bucket per verificare che l'oggetto sia stato caricato.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Eliminare l'oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Eliminare il bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Come StorageGRID implementa l'API REST S3

Richieste client in conflitto

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite".

La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Coerenza

La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la loro coerenza in diversi nodi e siti storage. È possibile modificare la coerenza come richiesto dall'applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET successivo a un PUT completato con successo sarà in grado di leggere i dati appena scritti. Le sovrascritture di oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni alla fine risultano coerenti.

Se si desidera eseguire operazioni a oggetti con una coerenza diversa, è possibile:

- Specificare una coerenza per [ogni secchio](#) .
- Specificare una coerenza per [Ogni operazione API](#).
- Modificare la coerenza predefinita a livello di griglia eseguendo una delle seguenti operazioni:
 - In Grid Manager, vai a **Configurazione > Sistema > Impostazioni di archiviazione > Coerenza predefinita del bucket**.
 - .



Una modifica alla coerenza a livello di griglia si applica solo ai bucket creati dopo la modifica dell'impostazione. Per determinare i dettagli di una modifica, vedere il registro di controllo situato in `/var/local/log` (cercare **consistencyLevel**).

Valori di coerenza

La coerenza influisce sul modo in cui i metadati utilizzati da StorageGRID per tracciare gli oggetti vengono distribuiti tra i nodi. La coerenza influisce sulla disponibilità degli oggetti per le richieste dei client.

È possibile impostare la coerenza per un bucket o un'operazione API su uno dei seguenti valori:

- **All:** Tutti i nodi ricevono immediatamente i metadati degli oggetti o la richiesta non riesce.
- **Strong-global:** garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti. Quando la semantica del quorum è configurata, si applicano i seguenti comportamenti:
 - Consente la tolleranza ai guasti del sito per le richieste dei client quando le griglie hanno tre o più siti. Le griglie a due siti non avranno tolleranza ai guasti del sito.
 - Le seguenti operazioni S3 non riusciranno se un sito è inattivo:
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Se necessario, puoi ["configurare la semantica del quorum StorageGRID per una coerenza globale forte"](#) .

- **Strong-site:** I metadati degli oggetti vengono immediatamente distribuiti ad altri nodi del sito. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write:** Fornisce coerenza lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available:** Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Utilizzare la coerenza "Read-after-new-write" e "available"

Quando un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write", StorageGRID esegue la ricerca in più passaggi, come segue:

- Per prima cosa, cerca l'oggetto utilizzando una bassa coerenza.
- Se la ricerca non riesce, ripete la ricerca al valore di coerenza successivo finché non raggiunge una coerenza equivalente al comportamento per strong-Global.

Se un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write" ma l'oggetto non esiste, la ricerca degli oggetti raggiungerà sempre una coerenza equivalente al comportamento per strong-Global. Poiché questa coerenza richiede la disponibilità di più copie dei metadati degli oggetti in ogni sito, è possibile ricevere un elevato numero di errori del server interno 500 nel caso in cui due o più nodi storage nello stesso sito non fossero disponibili.

A meno che non si richiedano garanzie di coerenza simili a Amazon S3, è possibile evitare questi errori per le operazioni HEAD and GET impostando la coerenza su "disponibile". Quando un'operazione HEAD o GET utilizza la consistenza "disponibile", StorageGRID fornisce solo la consistenza finale. Non ritenta un'operazione non riuscita ad aumentare la coerenza, pertanto non richiede la disponibilità di più copie dei metadati degli oggetti.

specificare la coerenza per l'operazione API

Per impostare la coerenza per una singola operazione API, i valori di coerenza devono essere supportati per l'operazione ed è necessario specificare la coerenza nell'intestazione della richiesta. Nell'esempio riportato di seguito viene impostata la coerenza su "strong-Site" per un'operazione GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



È necessario utilizzare la stessa coerenza per entrambe le operazioni PutObject e GetObject.

Specifica la coerenza per il bucket

Per impostare la coerenza per il bucket, è possibile utilizzare la richiesta StorageGRID **"METTI la coerenza del bucket"**. In alternativa, è possibile **"modificare la consistenza di un bucket"** rivolgersi al responsabile del tenant.

Quando si imposta la consistenza per un secchio, tenere presente quanto segue:

- L'impostazione della consistenza per un bucket determina la consistenza utilizzata per S3 operazioni eseguite sugli oggetti nel bucket o nella configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- La coerenza per una singola operazione API sovrascrive la coerenza per il bucket.
- In generale, i bucket devono utilizzare la coerenza predefinita, "Read-after-new-write". Se le richieste non funzionano correttamente, modificare il comportamento del client dell'applicazione, se possibile. In alternativa, configurare il client per specificare la coerenza per ogni richiesta API. Impostare la consistenza a livello del bucket solo come ultima risorsa.

Come interagiscono coerenza e regole ILM per influenzare la protezione dei dati

Sia la scelta della coerenza che la regola ILM influiscono sulla protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, la coerenza utilizzata durante la memorizzazione di un oggetto influisce sul posizionamento iniziale dei metadati degli oggetti, mentre il comportamento di acquisizione selezionato per la regola ILM influisce sul posizionamento iniziale delle copie degli oggetti. Poiché StorageGRID richiede l'accesso sia ai metadati dell'oggetto che ai relativi dati per soddisfare le richieste del client, la selezione di livelli di protezione corrispondenti per il comportamento di coerenza e acquisizione può offrire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Per le regole ILM sono disponibili le seguenti "opzioni di acquisizione" opzioni:

Commit doppio

StorageGRID effettua immediatamente copie provvisorie dell'oggetto e restituisce il successo al cliente. Le copie specificate nella regola ILM vengono eseguite quando possibile.

Rigoroso

Tutte le copie specificate nella regola ILM devono essere eseguite prima che l'operazione sia restituita al cliente.

Bilanciato

StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono create copie provvisorie e viene restituita al cliente l'avvenuta esecuzione. Le copie specificate nella regola ILM vengono eseguite quando possibile.

Esempio di interazione tra la regola coerenza e ILM

Supponiamo di avere una griglia a tre siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM:** creare tre copie dell'oggetto, una nel sito locale e una in ciascun sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **Coerenza:** Strong-global (i metadati degli oggetti vengono distribuiti immediatamente su più siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue tutte e tre le copie dell'oggetto e distribuisce i metadati a più siti prima di restituire l'esito positivo al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione corretta del messaggio. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, copie sia dei dati dell'oggetto sia dei metadati dell'oggetto sono ancora presenti nei siti remoti. L'oggetto è completamente recuperabile dagli altri siti.

Se invece si utilizzasse la stessa regola ILM e la coerenza del sito forte, il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati nei siti remoti, ma prima che i metadati dell'oggetto vengano distribuiti lì. In questo caso, il livello di protezione dei metadati degli oggetti non corrisponde al livello di protezione dei dati degli oggetti. Se il sito locale viene perso subito dopo l'acquisizione, anche i metadati dell'oggetto vengono persi. L'oggetto non può essere recuperato.

L'interrelazione tra coerenza e regole ILM può essere complessa. Contattare NetApp per assistenza.

Versione degli oggetti

È possibile impostare lo stato di versione di un bucket se si desidera mantenere più versioni di ciascun oggetto. L'abilitazione della versione per un bucket può aiutare a proteggere dalla cancellazione accidentale di oggetti e consente di recuperare e ripristinare le versioni precedenti di un oggetto.

Il sistema StorageGRID implementa il controllo delle versioni con il supporto per la maggior parte delle funzionalità e con alcune limitazioni. StorageGRID supporta fino a 10,000 versioni di ciascun oggetto.

La versione degli oggetti può essere combinata con la gestione del ciclo di vita delle informazioni di StorageGRID (ILM) o con la configurazione del ciclo di vita del bucket S3. È necessario attivare esplicitamente il controllo delle versioni per ogni bucket. Quando la versione è abilitata per un bucket, a ogni oggetto aggiunto al bucket viene assegnato un ID di versione, che viene generato dal sistema StorageGRID.

L'utilizzo dell'autenticazione MFA (multi-factor Authentication) Delete non è supportato.



Il controllo delle versioni può essere attivato solo sui bucket creati con StorageGRID versione 10.3 o successiva.

ILM e versione

I criteri ILM vengono applicati a ogni versione di un oggetto. Un processo di scansione ILM esegue una scansione continua di tutti gli oggetti e li rivaluti in base al criterio ILM corrente. Qualsiasi modifica apportata ai criteri ILM viene applicata a tutti gli oggetti precedentemente acquisiti. Sono incluse le versioni precedentemente ingerite se è abilitato il controllo delle versioni. La scansione ILM applica le nuove modifiche ILM agli oggetti acquisiti in precedenza.

Per gli oggetti S3 nei bucket abilitati per le versioni, il supporto per le versioni consente di creare regole ILM che utilizzano "tempo non corrente" come ora di riferimento (selezionare **Sì** per la domanda "Applica questa regola solo alle versioni precedenti degli oggetti?" in ["Passaggio 1 della creazione guidata di una regola ILM"](#)). Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. L'utilizzo di un filtro "tempo non corrente" consente di creare policy per ridurre l'impatto sullo storage delle versioni precedenti di oggetti.



Quando si carica una nuova versione di un oggetto utilizzando un'operazione di caricamento multiparte, l'ora non corrente per la versione originale dell'oggetto si riflette quando il caricamento multiparte è stato creato per la nuova versione, non quando il caricamento multiparte è stato completato. In casi limitati, il tempo non corrente per la versione originale potrebbe essere di ore o giorni prima del tempo per la versione corrente.

Informazioni correlate

- ["Modalità di eliminazione degli oggetti con versione S3"](#)
- ["Regole e criteri ILM per gli oggetti con versione S3 \(esempio 4\)"](#).

Utilizzare l'API REST S3 per configurare il blocco oggetti S3

Se l'impostazione blocco oggetti S3 globale è attivata per il sistema StorageGRID, è possibile creare bucket con blocco oggetti S3 attivato. È possibile specificare la conservazione predefinita per ogni bucket o impostazioni di conservazione per ciascuna versione dell'oggetto.

Come attivare il blocco oggetti S3 per un bucket

Se l'impostazione globale di blocco oggetti S3 è attivata per il sistema StorageGRID, è possibile attivare il blocco oggetti S3 quando si crea ciascun bucket.

S3 Object Lock è un'impostazione permanente che può essere attivata solo quando si crea un bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket.

Per attivare il blocco oggetti S3 per un bucket, utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando il tenant Manager. Vedere ["Creare un bucket S3"](#).
- Creare il bucket utilizzando una richiesta CreateBucket con l'`x-amz-bucket-object-lock-enabled` intestazione della richiesta. Vedere ["Operazioni sui bucket"](#).

S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando viene creato il bucket. Non puoi sospendere il controllo delle versioni per il bucket. Vedere ["Versione degli oggetti"](#).

Impostazioni di conservazione predefinite per un bucket

Quando S3 Object Lock è attivato per un bucket, è possibile attivare la conservazione predefinita per il bucket e specificare una modalità di conservazione predefinita e un periodo di conservazione predefinito.

Modalità di conservazione predefinita

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

Periodo di conservazione predefinito

Ogni bucket può avere un periodo di conservazione predefinito specificato in anni o giorni.

Come impostare la conservazione predefinita per un bucket

Per impostare la conservazione predefinita per un bucket, utilizzare uno dei seguenti metodi:

- Gestire le impostazioni del bucket da Tenant Manager. Vedere ["Creare un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).
- Eseguire una richiesta PutObjectLockConfiguration per il bucket per specificare la modalità predefinita e il numero predefinito di giorni o anni.

PutObjectLockConfiguration

La richiesta PutObjectLockConfiguration consente di impostare e modificare la modalità di conservazione predefinita e il periodo di conservazione predefinito per un bucket con blocco oggetti S3 attivato. È inoltre possibile rimuovere le impostazioni di conservazione predefinite precedentemente configurate.

Quando le nuove versioni degli oggetti vengono acquisite nel bucket, la modalità di conservazione predefinita viene applicata se `x-amz-object-lock-mode` e `x-amz-object-lock-retain-until-date` non sono specificate. Il periodo di conservazione predefinito viene utilizzato per calcolare la data di conservazione-fino-alla-data se `x-amz-object-lock-retain-until-date` non è specificato.

Se il periodo di conservazione predefinito viene modificato dopo l'acquisizione di una versione dell'oggetto, la data di conservazione della versione dell'oggetto rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.

Per completare questa operazione, è necessario disporre dell'`s3:PutBucketObjectLockConfiguration` autorizzazione o essere account root.

L'`Content-MD5` intestazione della richiesta deve essere specificata nella richiesta PUT.

Esempio di richiesta

Questo esempio attiva il blocco oggetti S3 per un bucket e imposta la modalità di conservazione predefinita su COMPLIANCE e il periodo di conservazione predefinito su 6 anni.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Come determinare la conservazione predefinita per un bucket

Per determinare se S3 Object Lock è attivato per un bucket e per visualizzare la modalità di conservazione e il periodo di conservazione predefiniti, utilizzare uno dei seguenti metodi:

- Visualizza il bucket nel tenant manager. Vedere ["Visualizza i bucket S3"](#).
- Eseguire una richiesta `GetObjectLockConfiguration`.

GetObjectLockConfiguration

La richiesta `GetObjectLockConfiguration` consente di determinare se S3 Object Lock è attivato per un bucket e, se è attivato, verificare se sono presenti una modalità di conservazione predefinita e un periodo di conservazione configurato per il bucket.

Quando le nuove versioni degli oggetti vengono acquisite nel bucket, la modalità di conservazione predefinita viene applicata se `x-amz-object-lock-mode` non è specificata. Il periodo di conservazione predefinito viene utilizzato per calcolare la data di conservazione-fino-alla-data se `x-amz-object-lock-retain-until-date` non è specificato.

Per completare questa operazione, è necessario disporre dell'`s3:GetBucketObjectLockConfiguration` autorizzazione o essere account root.

Esempio di richiesta

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Esempio di risposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Come specificare le impostazioni di conservazione per un oggetto

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza le impostazioni di conservazione S3 Object Lock.

Le impostazioni di conservazione a livello di oggetto vengono specificate utilizzando l'API REST S3. Le impostazioni di conservazione per un oggetto sovrascrivono le impostazioni di conservazione predefinite per il bucket.

È possibile specificare le seguenti impostazioni per ciascun oggetto:

- **Modalità di conservazione:** CONFORMITÀ o GOVERNANCE.
- **Conserva-fino-data:** Una data che specifica per quanto tempo la versione dell'oggetto deve essere conservata da StorageGRID.

- In modalità COMPLIANCE, se la data di conservazione è futura, l'oggetto può essere recuperato, ma non può essere modificato o cancellato. È possibile aumentare la data di conservazione fino alla data prevista, ma non è possibile ridurla o rimuoverla.
- In modalità GOVERNANCE, gli utenti con autorizzazioni speciali possono ignorare l'impostazione di conservazione fino alla data odierna. Possono eliminare una versione dell'oggetto prima che sia trascorso il periodo di conservazione. Possono anche aumentare, diminuire o addirittura rimuovere il mantenimento fino ad oggi.

- **Conservazione legale:** L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa.

L'impostazione di conservazione legale per un oggetto è indipendente dalla modalità di conservazione e dalla conservazione fino alla data. Se una versione dell'oggetto è sottoposta a blocco legale, nessuno può eliminare tale versione.

Per specificare le impostazioni di blocco degli oggetti S3 quando si aggiunge una versione dell'oggetto a un bucket "PutObject", eseguire una richiesta , "Oggetto CopyObject" o "CreateMultipartUpload".

È possibile utilizzare quanto segue:

- `x-amz-object-lock-mode`, Che può essere CONFORMITÀ o GOVERNANCE (distinzione tra maiuscole e minuscole).



Se si specifica `x-amz-object-lock-mode`, è necessario specificare anche `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
 - Il valore Retain-until-date deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
 - La data di conservazione deve essere in futuro.
- `x-amz-object-lock-legal-hold`

Se la conservazione legale È ATTIVA (sensibile al maiuscolo/minuscolo), l'oggetto viene collocato sotto una conservazione legale. Se l'opzione Legal Hold è disattivata, non viene effettuata alcuna conservazione a fini giudiziari. Qualsiasi altro valore genera un errore 400 Bad Request (InvalidArgument).

Se si utilizza una di queste intestazioni di richiesta, tenere presente le seguenti restrizioni:

- L'intestazione `Content-MD5` della richiesta è necessaria se nella richiesta PutObject è presente un'intestazione di richiesta ``x-amz-object-lock-*`. ``Content-MD5` Non è richiesto per CopyObject o CreateMultipartUpload.
- Se nel bucket non è abilitato il blocco oggetto S3 ed è presente un'intestazione della richiesta ``x-amz-object-lock-*`, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta PutObject supporta l'uso di `x-amz-storage-class: REDUCED_REDUNDANCY` per abbinare il comportamento AWS. Tuttavia, quando un oggetto viene acquisito in un bucket con il blocco oggetti S3 attivato, StorageGRID eseguirà sempre un ingest a doppio commit.

- Una risposta successiva alla versione GET o HeadObject includerà le intestazioni `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e `x-amz-object-lock-legal-hold`, se configurate e se il mittente della richiesta dispone delle autorizzazioni corrette `s3:Get*`.

È possibile utilizzare il `s3:object-lock-remaining-retention-days` campo delle condizioni della policy per limitare i periodi di conservazione minimo e massimo consentiti per gli oggetti.

Come aggiornare le impostazioni di conservazione per un oggetto

Se è necessario aggiornare le impostazioni di conservazione o conservazione a fini giudiziari per una versione di oggetto esistente, è possibile eseguire le seguenti operazioni di sottorisorsa oggetto:

- `PutObjectLegalHold`

Se IL nuovo valore di conservazione a fini giudiziari è ATTIVO, l'oggetto viene collocato sotto una conservazione a fini giudiziari. Se il valore di conservazione a fini giudiziari è OFF, la conservazione a fini giudiziari viene revocata.

- `PutObjectRetention`
 - Il valore della modalità può essere COMPLIANCE o GOVERNANCE (distinzione tra maiuscole e minuscole).
 - Il valore Retain-until-date deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
 - Se una versione a oggetti ha un valore di conservazione esistente fino alla data odierna, è possibile aumentarlo. Il nuovo valore deve essere in futuro.

Come utilizzare LA modalità DI GOVERNANCE

Gli utenti che dispongono dell' `s3:BypassGovernanceRetention` autorizzazione possono ignorare le impostazioni di conservazione attive di un oggetto che utilizza la modalità di GOVERNANCE. Tutte le operazioni di ELIMINAZIONE o `PutObjectRetention` devono includere l' `x-amz-bypass-governance-retention:true` intestazione della richiesta. Questi utenti possono eseguire queste operazioni aggiuntive:

- Eseguire operazioni `DeleteObject` o `DeleteObjects` per eliminare una versione dell'oggetto prima che sia trascorso il periodo di conservazione.

Non è possibile eliminare gli oggetti che si trovano sotto un blocco legale. La sospensione legale deve essere disattivata.

- Eseguire le operazioni `PutObjectRetention` che modificano la modalità di una versione dell'oggetto dalla GOVERNANCE alla CONFORMITÀ prima che sia trascorso il periodo di conservazione dell'oggetto.

Non è mai consentito cambiare la modalità dalla CONFORMITÀ alla GOVERNANCE.

- Eseguire le operazioni `PutObjectRetention` per aumentare, ridurre o rimuovere il periodo di conservazione di una versione oggetto.

Informazioni correlate

- ["Gestire gli oggetti con S3 Object Lock"](#)
- ["USA il blocco oggetti S3 per conservare gli oggetti"](#)
- ["Guida dell'utente di Amazon Simple Storage Service: Blocco degli oggetti"](#)

Creare la configurazione del ciclo di vita S3

È possibile creare una configurazione del ciclo di vita S3 per controllare quando oggetti specifici vengono cancellati dal sistema StorageGRID.

Il semplice esempio di questa sezione illustra come una configurazione del ciclo di vita S3 può controllare quando alcuni oggetti vengono cancellati (scaduti) da specifici bucket S3. L'esempio in questa sezione è a solo scopo illustrativo. Per informazioni dettagliate sulla creazione di configurazioni del ciclo di vita S3, vedere ["Guida utente di Amazon Simple Storage Service: Gestione del ciclo di vita degli oggetti"](#). Nota: StorageGRID supporta solo le azioni di scadenza e non le azioni di transizione.

Che cos'è la configurazione del ciclo di vita

Una configurazione del ciclo di vita è un insieme di regole applicate agli oggetti in specifici bucket S3. Ogni regola specifica quali oggetti sono interessati e quando scadranno (in una data specifica o dopo un certo numero di giorni).

StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML:

- Scadenza: Consente di eliminare un oggetto quando viene raggiunta una data specificata o quando viene raggiunto un numero di giorni specificato, a partire dalla data di acquisizione dell'oggetto.
- NoncurrentVersionExpiration (NoncurrentExpiration versione): Consente di eliminare un oggetto quando viene raggiunto un numero di giorni specificato, a partire da quando l'oggetto è diventato non corrente.
- Filtro (prefisso, tag)
- Stato
- ID

Ciascun oggetto segue le impostazioni di conservazione di un ciclo di vita bucket S3 o di un criterio ILM. Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti corrispondenti al filtro del ciclo di vita del bucket. Gli oggetti che non corrispondono al filtro del ciclo di vita del bucket utilizzano le impostazioni di conservazione del criterio ILM. Se un oggetto corrisponde a un filtro del ciclo di vita bucket e non sono specificate esplicitamente azioni di scadenza, le impostazioni di conservazione del criterio ILM non vengono utilizzate ed è implicito che le versioni degli oggetti vengano mantenute per sempre. Vedere ["Esempi di priorità per il ciclo di vita dei bucket S3 e la politica ILM"](#).

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora applicabili all'oggetto. Oppure, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni di posizionamento ILM per l'oggetto. Per ulteriori informazioni, vedere ["Come ILM opera per tutta la vita di un oggetto"](#).



La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

StorageGRID supporta l'utilizzo delle seguenti operazioni bucket per gestire le configurazioni del ciclo di vita:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Creare la configurazione del ciclo di vita

Come primo passo nella creazione di una configurazione del ciclo di vita, è possibile creare un file JSON che includa una o più regole. Ad esempio, questo file JSON include tre regole, come segue:

1. La regola 1 si applica solo agli oggetti che corrispondono al prefisso `category1/` e che hanno un `key2` valore di `tag2`. Il `Expiration` parametro specifica che gli oggetti corrispondenti al filtro scadranno a mezzanotte del 22 agosto 2020.
2. La regola 2 si applica solo agli oggetti che corrispondono al prefisso `category2/`. Il `Expiration` parametro specifica che gli oggetti corrispondenti al filtro scadranno 100 giorni dopo l'acquisizione.



Le regole che specificano un numero di giorni sono relative al momento in cui l'oggetto è stato acquisito. Se la data corrente supera la data di acquisizione più il numero di giorni, alcuni oggetti potrebbero essere rimossi dal bucket non appena viene applicata la configurazione del ciclo di vita.

3. La regola 3 si applica solo agli oggetti che corrispondono al prefisso `category3/`. Il `Expiration` parametro specifica che tutte le versioni non correnti degli oggetti corrispondenti scadranno 50 giorni dopo che diventano non correnti.

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```


Applica la configurazione del ciclo di vita al bucket

Dopo aver creato il file di configurazione del ciclo di vita, applicarlo a un bucket inviando una richiesta `PutBucketLifecycleConfiguration`.

Questa richiesta applica la configurazione del ciclo di vita nel file di esempio agli oggetti in un bucket denominato `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Per verificare che una configurazione del ciclo di vita sia stata applicata correttamente al bucket, eseguire una richiesta `GetBucketLifecycleConfiguration`. Ad esempio:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Una risposta corretta elenca la configurazione del ciclo di vita appena applicata.

Verificare che la scadenza del ciclo di vita del bucket si applichi all'oggetto

È possibile determinare se una regola di scadenza nella configurazione del ciclo di vita si applica a un oggetto specifico quando si invia una richiesta `PutObject`, `HeadObject` o `GetObject`. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando l'oggetto scade e quale regola di scadenza è stata abbinata.



Poiché il ciclo di vita del bucket sovrascrive ILM, `expiry-date` viene visualizzata la data effettiva in cui l'oggetto verrà eliminato. Per ulteriori informazioni, vedere ["Come viene determinata la conservazione degli oggetti"](#).

Ad esempio, questa richiesta `PutObject` è stata emessa il 22 giugno 2020 e inserisce un oggetto nel `testbucket` bucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La risposta corretta indica che l'oggetto scadrà tra 100 giorni (01 ottobre 2020) e che corrisponde alla regola 2 della configurazione del ciclo di vita.

```
{
  *Expiration: "expiry-date=\\"Thu, 01 Oct 2020 09:07:49 GMT\\", rule-
id=\\"rule2\\",
  ETag: "\\"9762f8a803bc34f5340579d4446076f7\\""}
}
```

Ad esempio, questa richiesta `HeadObject` è stata utilizzata per ottenere metadati per lo stesso oggetto nel bucket `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La risposta di successo include i metadati dell'oggetto e indica che l'oggetto scadrà tra 100 giorni e che corrisponde alla regola 2.

```
{
  "AcceptRanges": "bytes",
  *Expiration: "expiry-date=\\"Thu, 01 Oct 2020 09:07:48 GMT\\", rule-
id=\\"rule2\\",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\\"9762f8a803bc34f5340579d4446076f7\\""}
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



Per i bucket abilitati per la versione, l'`x-amz-expiration` intestazione della risposta si applica solo alle versioni correnti di oggetti.

Raccomandazioni per l'implementazione dell'API REST S3

Seguire questi consigli quando si implementa l'API REST S3 per l'utilizzo con StorageGRID.

Raccomandazioni per la gestione di oggetti inesistenti

Se la tua applicazione controlla regolarmente se un oggetto esiste in un percorso in cui non ti aspetti che l'oggetto esista effettivamente, dovresti usare "Disponibile"["coerenza"](#). Ad esempio, dovresti usare la coerenza "Disponibile" se la tua applicazione esegue l'HEAD di una posizione prima di eseguirvi un PUT.

In caso contrario, se l'operazione HEAD non trova l'oggetto, è possibile ricevere un numero elevato di errori del server interno 500 se due o più nodi di archiviazione nello stesso sito non sono disponibili o un sito remoto non è raggiungibile.

È possibile impostare la coerenza "disponibile" per ciascun bucket utilizzando la richiesta oppure specificare la coerenza nell'intestazione della ["METTI la coerenza del bucket"](#) richiesta per una singola operazione API.

Raccomandazioni per le chiavi a oggetti

Seguire questi consigli per i nomi delle chiavi degli oggetti, in base alla prima volta che il bucket è stato creato.

Bucket creati in StorageGRID 11.4 o versioni precedenti

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi oggetto. Ciò è in contrasto con la precedente raccomandazione AWS per i prefissi principali. Utilizzare invece prefissi non casuali e non univoci, ad esempio `image`.
- Se si segue la precedente raccomandazione AWS per utilizzare caratteri casuali e univoci nei prefissi delle chiavi, inserire un prefisso tra le chiavi degli oggetti e il nome della directory. Ovvero, utilizzare questo formato:

```
mybucket/mydir/f8e3-image3132.jpg
```

Invece di questo formato:

```
mybucket/f8e3-image3132.jpg
```

Bucket creati in StorageGRID 11.4 o versioni successive

Non è necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. Nella maggior parte dei casi, è possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi degli oggetti.



Un'eccezione è rappresentata da un carico di lavoro S3 che rimuove continuamente tutti gli oggetti dopo un breve periodo di tempo. Per ridurre al minimo l'impatto delle performance per questo caso d'utilizzo, modificare una parte iniziale del nome della chiave ogni diverse migliaia di oggetti con qualcosa di simile alla data. Si supponga, ad esempio, che un client S3 scriva in genere 2,000 oggetti al secondo e che il criterio del ciclo di vita di ILM o bucket rimuova tutti gli oggetti dopo tre giorni. Per ridurre al minimo l'impatto sulle prestazioni, è possibile assegnare un nome alle chiavi utilizzando uno schema simile al seguente:

```
/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg
```

Raccomandazioni per "letture di gamma"

Se ["opzione globale per comprimere gli oggetti memorizzati"](#) è attivato, le applicazioni client S3 devono evitare di eseguire operazioni `GetObject` che specificano un intervallo di byte da restituire. Queste operazioni di "lettura dell'intervallo" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. Le operazioni `GetObject` che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

Se gli intervalli vengono letti da oggetti compressi, le richieste del client possono scadere.



Se è necessario comprimere gli oggetti e l'applicazione client deve utilizzare le letture dell'intervallo, aumentare il timeout di lettura per l'applicazione.

Supporto per Amazon S3 REST API

Dettagli sull'implementazione dell'API REST S3

Il sistema StorageGRID implementa l'API del servizio di storage semplice (API versione

2006-03-01) con il supporto per la maggior parte delle operazioni e con alcune limitazioni. È necessario comprendere i dettagli dell'implementazione quando si integrano le applicazioni client API REST S3.

Il sistema StorageGRID supporta sia richieste virtuali in stile host che richieste in stile percorso.

Gestione della data

L'implementazione StorageGRID dell'API REST S3 supporta solo formati di data HTTP validi.

Il sistema StorageGRID supporta solo i formati di data HTTP validi per tutte le intestazioni che accettano i valori di data. La parte temporale della data può essere specificata nel formato GMT (Greenwich Mean Time) o UTC (Universal Coordinated Time) senza offset del fuso orario (deve essere specificato ++1). Se si include l'`x-amz-date` intestazione nella richiesta, questo sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza la versione 4 della firma AWS, l'`x-amz-date` intestazione deve essere presente nella richiesta firmata perché l'intestazione della data non è supportata.

Intestazioni di richiesta comuni

Il sistema StorageGRID supporta le intestazioni delle richieste comuni definite da ["Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni"](#), con un'eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per firma AWS versione 2 Supporto per firma AWS versione 4, con le seguenti eccezioni: <ul style="list-style-type: none">Quando si fornisce il valore checksum del payload effettivo in <code>x-amz-content-sha256</code>, il valore viene accettato senza convalida, come se il valore <code>UNSIGNED-PAYLOAD</code> fosse stato fornito per l'intestazione. Quando si fornisce un <code>x-amz-content-sha256</code> valore di intestazione che implica <code>aws-chunked</code> lo streaming (ad esempio, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), le firme dei frammenti non vengono verificate in base ai dati dei frammenti.

Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite dal *referimento API del servizio di storage semplice*, con un'eccezione.

Intestazione della risposta	Implementazione
<code>x-amz-id-2</code>	Non utilizzato

Autenticare le richieste

Il sistema StorageGRID supporta l'accesso anonimo e autenticato agli oggetti utilizzando l'API S3.

L'API S3 supporta Signature versione 2 e Signature versione 4 per l'autenticazione delle richieste API S3.

Le richieste autenticate devono essere firmate utilizzando l'ID della chiave di accesso e la chiave di accesso segreta.

Il sistema StorageGRID supporta due metodi di autenticazione: L'intestazione HTTP `Authorization` e i parametri di query.

Utilizzare l'intestazione autorizzazione HTTP

L'intestazione HTTP `Authorization` viene utilizzata da tutte le operazioni API S3, ad eccezione delle richieste anonime, laddove consentito dal criterio bucket. L' `Authorization` intestazione contiene tutte le informazioni di firma necessarie per autenticare una richiesta.

Utilizzare i parametri di query

È possibile utilizzare i parametri di query per aggiungere informazioni di autenticazione a un URL. Questa operazione è nota come prefirma dell'URL, che può essere utilizzata per concedere l'accesso temporaneo a risorse specifiche. Gli utenti con l'URL con prefisso non devono conoscere la chiave di accesso segreta per accedere alla risorsa, consentendo così l'accesso limitato a una risorsa da parte di terze parti.

Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
ListBucket (Precedentemente denominato GET Service)	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
OTTIENI l'utilizzo dello storage	La richiesta StorageGRID " OTTIENI l'utilizzo dello storage " indica la quantità totale di storage utilizzata da un account e per ogni bucket associato all'account. Si tratta di un'operazione sul servizio con un percorso di / e un parametro di query personalizzato (<code>?x-ntap-sg-usage</code>) aggiunto.
OPZIONI /	Le applicazioni client possono OPTIONS / inviare richieste alla porta S3 su un nodo di archiviazione, senza fornire credenziali di autenticazione S3, per determinare se il nodo di archiviazione è disponibile. È possibile utilizzare questa richiesta per il monitoraggio o per consentire ai bilanciatori di carico esterni di identificare quando un nodo di storage è inattivo.

Operazioni sui bucket

Il sistema StorageGRID supporta un massimo di 5,000 bucket per ciascun account tenant S3.

Ogni griglia può avere un massimo di 100.000 secchi.

Per supportare 5.000 bucket, ogni nodo di storage nella griglia deve avere un minimo di 64 GB di RAM.

Le restrizioni dei nomi dei bucket seguono le restrizioni delle regioni AWS US Standard, ma è necessario limitarle ulteriormente alle convenzioni di denominazione DNS per supportare le richieste di tipo host virtuale S3.

Per ulteriori informazioni, vedere quanto segue:

- ["Guida utente di Amazon Simple Storage Service: Quote, restrizioni e limitazioni dei bucket"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

Le operazioni ListObjects (GET Bucket) e ListObjectVersions (GET Bucket object versions) supportano StorageGRID ["valori di coerenza"](#).

È possibile verificare se gli aggiornamenti dell'ultimo tempo di accesso sono attivati o disattivati per i singoli bucket. Vedere ["OTTIENI l'ultimo tempo di accesso a bucket"](#).

La seguente tabella descrive come StorageGRID implementa le operazioni del bucket API REST S3. Per eseguire una di queste operazioni, è necessario fornire le credenziali di accesso necessarie per l'account.

Operazione	Implementazione
CreateBucket	<p>Crea un nuovo bucket. Creando il bucket, diventerai il proprietario del bucket.</p> <ul style="list-style-type: none"> • I nomi dei bucket devono rispettare le seguenti regole: <ul style="list-style-type: none"> ◦ Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). ◦ Deve essere conforme al DNS. ◦ Deve contenere almeno 3 e non più di 63 caratteri. ◦ Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. ◦ Non deve essere simile a un indirizzo IP formattato con testo. ◦ Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. • Per impostazione predefinita, i bucket vengono creati nella <code>us-east-1</code> regione; tuttavia, è possibile utilizzare l' <code>`LocationConstraint`</code> elemento di richiesta nel corpo della richiesta per specificare un'area diversa. Quando si utilizza l' <code>`LocationConstraint`</code> elemento, è necessario specificare il nome esatto di una regione definita utilizzando Grid Manager o l'API di gestione griglia. Contattare l'amministratore di sistema se non si conosce il nome della regione da utilizzare. <p>Nota: Si verifica un errore se la richiesta CreateBucket utilizza una regione non definita in StorageGRID.</p> <ul style="list-style-type: none"> • È possibile includere l' <code>`x-amz-bucket-object-lock-enabled`</code> intestazione della richiesta per creare un bucket con blocco oggetto S3 attivato. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3". <p>È necessario attivare il blocco oggetti S3 quando si crea il bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket. S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando si crea il bucket.</p>
DeleteBucket	Elimina il bucket.
DeleteBucketCors	Elimina la configurazione CORS per il bucket.
DeleteBucketEncryption	Elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma i nuovi oggetti aggiunti al bucket non vengono crittografati.
DeleteBucketLifecycle	Elimina la configurazione del ciclo di vita dal bucket. Vedere "Creare la configurazione del ciclo di vita S3" .

Operazione	Implementazione
DeleteBucketPolicy	Elimina il criterio allegato al bucket.
DeleteBucketReplication	Elimina la configurazione di replica collegata al bucket.
DeleteBucketTagging	<p>Utilizza la <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un bucket.</p> <p>Attenzione: Se per questo bucket è impostato un tag criterio ILM non predefinito, vi sarà un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket con un valore assegnato. Non inviare una richiesta <code>DeleteBucketTagging</code> se è presente un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket. Al contrario, eseguire una richiesta <code>PutBucketTagging</code> con solo il <code>NTAP-SG-ILM-BUCKET-TAG</code> tag e il relativo valore assegnato per rimuovere tutti gli altri tag dal bucket. Non modificare o rimuovere l' <code>NTAP-SG-ILM-BUCKET-TAG</code> etichetta della benna.</p>
GetBucketAcl	Restituisce una risposta positiva e l'ID, il <code>DisplayName</code> e l'autorizzazione del proprietario del bucket, indicando che il proprietario ha accesso completo al bucket.
GetBucketCors	Restituisce la <code>cors</code> configurazione per la benna.
GetBucketEncryption	Restituisce la configurazione di crittografia predefinita per il bucket.
GetBucketLifecycleConfiguration (Precedentemente denominato ciclo di vita bucket GET)	Restituisce la configurazione del ciclo di vita per il bucket. Vedere "Creare la configurazione del ciclo di vita S3" .
GetBucketLocation	Restituisce l'area impostata utilizzando l' <code>LocationConstraint</code> elemento nella richiesta <code>CreateBucket</code> . Se la regione del bucket è <code>us-east-1</code> , viene restituita una stringa vuota per la regione.
GetBucketNotificationConfiguration (Precedentemente denominata notifica bucket GET)	Restituisce la configurazione di notifica collegata al bucket.
GetBucketPolicy	Restituisce la policy allegata al bucket.
GetBucketReplication	Restituisce la configurazione di replica collegata al bucket.

Operazione	Implementazione
GetBucketTagging	<p>Utilizza la <code>tagging</code> sottorisorsa per restituire tutti i tag per un bucket.</p> <p>Attenzione: Se per questo bucket è impostato un tag criterio ILM non predefinito, vi sarà un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket con un valore assegnato. Non modificare o rimuovere questo tag.</p>
GetBucketVersioning	<p>Questa implementazione utilizza la <code>versioning</code> sottorisorsa per restituire lo stato di versione di un bucket.</p> <ul style="list-style-type: none"> • <i>Blank</i>: La versione non è mai stata abilitata (bucket "Unversioned") • <i>Enabled</i> (attivato): Il controllo delle versioni è attivato • <i>Suspended</i> (sospeso): Il controllo delle versioni era stato precedentemente attivato e sospeso
GetObjectLockConfiguration	<p>Restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurato.</p> <p>Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".</p>
HeadBucket	<p>Determina se esiste un bucket e si dispone dell'autorizzazione per accedervi.</p> <p>Questa operazione restituisce:</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: UUID del bucket in formato UUID. • <code>x-ntap-sg-trace-id</code>: L'ID di traccia univoco della richiesta associata.

Operazione	Implementazione
ListObjects e ListObjectsV2 (Precedentemente denominato GET Bucket)	<p>Restituisce alcuni o tutti gli oggetti (fino a 1.000) in un bucket. La classe di archiviazione per gli oggetti può avere due valori, anche se l'oggetto è stato acquisito con l' `REDUCED_REDUNDANCY` opzione della classe di archiviazione:</p> <ul style="list-style-type: none"> • STANDARD, Che indica che l'oggetto è memorizzato in un pool di archiviazione costituito da nodi di archiviazione. • GLACIER, Che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool. <p>Se il bucket contiene un numero elevato di chiavi eliminate con lo stesso prefisso, la risposta potrebbe includere alcune <code>CommonPrefixes</code> che non contengono chiavi.</p> <p>Per le richieste <code>HeadObject</code> e <code>ListObject</code>, <code>StorageGRID</code> restituisce i timestamp <code>LastModified</code> con una precisione diversa, mentre <code>AWS</code> restituisce i timestamp con la stessa precisione, come mostrato negli esempi seguenti:</p> <ul style="list-style-type: none"> • <code>StorageGRID HeadObject</code>: "Ultima modifica": "2024-09-26T16:43:24+00:00" • <code>StorageGRID ListObject</code>: "Ultima modifica": "2024-09-26T16:43:24.931000+00:00" • <code>AWS HeadObject</code>: "Ultima modifica": "2023-10-17T00:19:54+00:00" • <code>AWS ListObject</code>: "Ultima modifica": "2023-10-17T00:19:54+00:00"
ListObjectVersions (Precedentemente denominate versioni oggetto GET Bucket)	<p>Con l'accesso IN LETTURA IN un bucket, questa operazione con le <code>versions</code> risorse secondarie elenca i metadati di tutte le versioni di oggetti nel bucket.</p>
PutBucketCors	<p>Imposta la configurazione CORS per un bucket in modo che il bucket possa gestire le richieste cross-origin. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Ad esempio, si supponga di utilizzare un bucket S3 denominato <code>images</code> per memorizzare la grafica. Impostando la configurazione CORS per il <code>images</code> bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito Web <code>http://www.example.com</code>.</p>

Operazione	Implementazione
PutBucketEncryption	<p>Consente di impostare lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è attivata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati. StorageGRID supporta la crittografia lato server con le chiavi gestite da StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare il <code>SSEAlgorithm</code> parametro su <code>AES256</code> e non utilizzare il <code>KMSMasterKeyID</code> parametro.</p> <p>La configurazione della crittografia predefinita del bucket viene ignorata se la richiesta di caricamento dell'oggetto specifica già la crittografia (ovvero, se la richiesta include l' <code>`x-amz-server-side-encryption-*</code> intestazione della richiesta).</p>
PutBucketLifecycleConfiguration (Precedentemente denominato ciclo di vita bucket PUT)	<p>Crea una nuova configurazione del ciclo di vita per il bucket o sostituisce una configurazione del ciclo di vita esistente. StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML:</p> <ul style="list-style-type: none"> • Scadenza (giorni, data, <code>ExpiredObjectDeleteMarker</code>) • <code>NoncurrentVersionExpiration</code> (<code>NewerNoncurrentVersions</code>, <code>NoncurrentDays</code>) • Filtro (prefisso, tag) • Stato • ID <p>StorageGRID non supporta queste azioni:</p> <ul style="list-style-type: none"> • <code>AbortIncompleteMultipartUpload</code> • Transizione <p>Vedere "Creare la configurazione del ciclo di vita S3". Per comprendere in che modo l'azione scadenza in un ciclo di vita bucket interagisce con le istruzioni di posizionamento ILM, vedere "Come ILM opera per tutta la vita di un oggetto".</p> <p>Nota: La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.</p>

Operazione	Implementazione
PutBucketNotificationConfiguration (Precedentemente denominata notifica bucket PUT)	<p>Configura le notifiche per il bucket utilizzando l'XML di configurazione delle notifiche incluso nel corpo della richiesta. È necessario conoscere i seguenti dettagli di implementazione:</p> <ul style="list-style-type: none"> StorageGRID supporta argomenti Amazon Simple Notification Service (Amazon SNS), argomenti Kafka o endpoint webhook come destinazioni. Gli endpoint Simple Queue Service (SQS) o AWS Lambda non sono supportati. La destinazione delle notifiche deve essere specificata come URN di un endpoint StorageGRID. Gli endpoint possono essere creati utilizzando il tenant Manager o l'API di gestione tenant. <p>L'endpoint deve esistere perché la configurazione della notifica abbia esito positivo. Se l'endpoint non esiste, viene restituito un 400 Bad Request errore con il codice <code>InvalidArgument</code>.</p> <ul style="list-style-type: none"> Non è possibile configurare una notifica per i seguenti tipi di evento. Questi tipi di evento sono non supportati. <ul style="list-style-type: none"> <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ad eccezione del fatto che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente: <ul style="list-style-type: none"> EventSource <code>sgws:s3</code> AwsRegion non incluso x-amz-id-2 non incluso arn <code>urn:sgws:s3:::bucket_name</code>
PutBucketPolicy	Imposta la policy associata al bucket. Vedere "Utilizza policy di accesso a bucket e gruppi" .

Operazione	Implementazione
PutBucketReplication	<p data-bbox="475 155 1492 260">Si configura "Replica di StorageGRID CloudMirror" per il bucket utilizzando l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica di CloudMirror, è necessario conoscere i seguenti dettagli di implementazione:</p> <ul data-bbox="500 291 1492 785" style="list-style-type: none"> <li data-bbox="500 291 1492 470">• StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo dell' <code>Filter</code> elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, vedere "Guida utente di Amazon Simple Storage Service: Configurazione della replica". <li data-bbox="500 480 1492 554">• La replica del bucket può essere configurata su bucket con versione o senza versione. <li data-bbox="500 564 1492 669">• È possibile specificare un bucket di destinazione diverso in ciascuna regola dell'XML di configurazione della replica. Un bucket di origine può replicare in più di un bucket di destinazione. <li data-bbox="500 680 1492 785">• I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID, come specificato in Gestione tenant o nell'API di gestione tenant. Vedere "Configurare la replica di CloudMirror". <p data-bbox="521 816 1492 963">L'endpoint deve esistere per il successo della configurazione della replica. Se l'endpoint non esiste, la richiesta non riesce come <code>400 Bad Request</code>. Il messaggio di errore indica: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></p> <ul data-bbox="500 995 1492 1478" style="list-style-type: none"> <li data-bbox="500 995 1492 1068">• Non è necessario specificare un <code>Role</code> nell'XML di configurazione. Questo valore non viene utilizzato da StorageGRID e verrà ignorato se inviato. <li data-bbox="500 1079 1492 1184">• Se si omette la classe di archiviazione dall'XML di configurazione, StorageGRID utilizza la <code>STANDARD</code> classe di archiviazione per impostazione predefinita. <li data-bbox="500 1194 1492 1478">• Se si elimina un oggetto dal bucket di origine o si elimina lo stesso bucket di origine, il comportamento della replica tra regioni è il seguente: <ul data-bbox="548 1289 1492 1478" style="list-style-type: none"> <li data-bbox="548 1289 1492 1362">◦ Se si elimina l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non viene replicato e non viene inviata alcuna notifica. <li data-bbox="548 1373 1492 1478">◦ Se elimini l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento standard di eliminazione di Amazon S3 per V1 della replica tra regioni.

Operazione	Implementazione
PutBucketTagging	<p>Utilizza la <code>tagging</code> sottorisorsa per aggiungere o aggiornare una serie di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni:</p> <ul style="list-style-type: none"> • StorageGRID e Amazon S3 supportano fino a 50 tag per ciascun bucket. • Le etichette associate a un bucket devono avere chiavi tag univoche. Una chiave tag può contenere fino a 128 caratteri Unicode. • I valori dei tag possono contenere fino a 256 caratteri Unicode. • Chiave e valori distinguono tra maiuscole e minuscole. <p>Attenzione: Se per questo bucket è impostato un tag criterio ILM non predefinito, vi sarà un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket con un valore assegnato. Assicurarsi che il <code>NTAP-SG-ILM-BUCKET-TAG</code> tag bucket sia incluso con il valore assegnato in tutte le richieste <code>PutBucketTagging</code>. Non modificare o rimuovere questo tag.</p> <p>Nota: Questa operazione sovrascriverà tutti i tag correnti già presenti nel bucket. Se qualsiasi tag esistente viene omesso dal set, tali tag verranno rimossi per il bucket.</p>
PutBucketVersioning	<p>Utilizza la <code>versioning</code> sottorisorsa per impostare lo stato di versione di un bucket esistente. È possibile impostare lo stato di versione con uno dei seguenti valori:</p> <ul style="list-style-type: none"> • Enabled (attivato): Attiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID di versione univoco. • Suspended (sospeso): Disattiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione <code>null</code>.
PutObjectLockConfiguration	<p>Configura o rimuove la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito.</p> <p>Se il periodo di conservazione predefinito viene modificato, la data di conservazione delle versioni degli oggetti esistenti rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.</p> <p>Per informazioni dettagliate, vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".</p>

Operazioni sugli oggetti

Operazioni sugli oggetti

Questa sezione descrive come il sistema StorageGRID implementa le operazioni API REST S3 per gli oggetti.

Le seguenti condizioni si applicano a tutte le operazioni a oggetti:

- StorageGRID "valori di coerenza" sono supportati da tutte le operazioni sugli oggetti, ad eccezione delle seguenti:
 - `GetObjectAcl`
 - `OPTIONS /`
 - `PutObjectLegalHold`
 - `PutObjectRetention`
 - `SelectObjectContent`
- Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.
- Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, inclusi gli oggetti creati da un utente anonimo o da un altro account.

Nella tabella seguente viene descritto il modo in cui StorageGRID implementa le operazioni degli oggetti API REST S3.

Operazione	Implementazione
DeleteObject (Elimina oggetto)	<p>L'autenticazione multifattore (MFA) e l'intestazione della risposta <code>x-amz-mfa</code> non sono supportate.</p> <p>Durante l'elaborazione di una richiesta DeleteObject, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni memorizzate. Se l'esito è positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio, perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito.</p> <p>Versione</p> <p>Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare la <code>versionId</code> sottorisorsa. L'utilizzo di questa sottorisorsa elimina in modo permanente la versione. Se il <code>versionId</code> corrisponde a un marcatore di eliminazione, l'intestazione della risposta <code>x-amz-delete-marker</code> viene riportata impostata su <code>true</code>.</p> <ul style="list-style-type: none"> • Se un oggetto viene eliminato senza la <code>versionId</code> sottorisorsa in un bucket con il controllo delle versioni attivato, viene generato un indicatore di eliminazione. Il <code>versionId</code> marcatore per l'eliminazione viene restituito utilizzando l' <code>x-amz-version-id</code> intestazione della risposta e l' <code>x-amz-delete-marker</code> intestazione della risposta viene riportata impostata su <code>true</code>. • Se un oggetto viene eliminato senza la <code>versionId</code> sottorisorsa in un bucket con la versione sospesa, si ottiene l'eliminazione permanente di una versione 'null' già esistente o di un marcatore 'null' e la generazione di un nuovo marcatore 'null'. L' <code>x-amz-delete-marker</code> intestazione della risposta viene riportata impostata su <code>true</code>. <p>Nota: In alcuni casi, per un oggetto potrebbero esistere più contrassegni di eliminazione.</p> <p>Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.</p>
DeleteObjects (Precedentemente denominato ELIMINA più oggetti)	<p>L'autenticazione multifattore (MFA) e l'intestazione della risposta <code>x-amz-mfa</code> non sono supportate.</p> <p>È possibile eliminare più oggetti nello stesso messaggio di richiesta.</p> <p>Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.</p>

Operazione	Implementazione
DeleteObjectTagging	<p>Utilizza la <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un oggetto.</p> <p>Versione</p> <p>Se il <code>versionId</code> parametro query non è specificato nella richiesta, l'operazione elimina tutti i tag dalla versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con l' <code>x-amz-delete-marker</code> intestazione della risposta impostata su <code>true</code>.</p>
GetObject	"GetObject"
GetObjectAcl	Se vengono fornite le credenziali di accesso necessarie per l'account, l'operazione restituisce una risposta positiva e l'ID, il DisplayName e l'autorizzazione del proprietario dell'oggetto, indicando che il proprietario dispone dell'accesso completo all'oggetto.
GetObjectLegalHold	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
GetObjectRetention	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
GetObjectTagging	<p>Utilizza la <code>tagging</code> sottorisorsa per restituire tutti i tag per un oggetto.</p> <p>Versione</p> <p>Se il <code>versionId</code> parametro query non è specificato nella richiesta, l'operazione restituisce tutti i tag della versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con l' <code>x-amz-delete-marker</code> intestazione della risposta impostata su <code>true</code>.</p>
HeadObject (oggetto intestazione)	"HeadObject (oggetto intestazione)"
RestoreObject	"RestoreObject"
PutObject	"PutObject"
Oggetto CopyObject (Precedentemente denominato oggetto PUT - Copia)	"Oggetto CopyObject"
PutObjectLegalHold	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

Operazione	Implementazione
PutObjectRetention	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
PutObjectTagging	<p>Utilizza la <code>tagging</code> sottorisorsa per aggiungere una serie di tag a un oggetto esistente.</p> <p>Limiti tag oggetto</p> <p>È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole.</p> <p>Aggiornamenti dei tag e comportamento di acquisizione</p> <p>Quando si utilizza PutObjectTagging per aggiornare i tag di un oggetto, StorageGRID non acquisisce nuovamente l'oggetto. Ciò significa che l'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background.</p> <p>Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto.</p> <p>Risoluzione dei conflitti</p> <p>Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.</p> <p>Versione</p> <p>Se il <code>versionId</code> parametro query non è specificato nella richiesta, l'operazione aggiunge tag alla versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con l' <code>x-amz-delete-marker</code> intestazione della risposta impostata su <code>true</code>.</p>
SelectObjectContent	"SelectObjectContent"

StorageGRID supporta le seguenti condizioni, tipi di dati e operatori Amazon S3 Select per ["Comando SelectObjectContent"](#).



Gli elementi non elencati non sono supportati.

Per la sintassi, vedere ["SelectObjectContent"](#). Per ulteriori informazioni su S3 Select, vedere ["Documentazione AWS per S3 Select"](#).

Solo gli account tenant con S3 Select abilitato possono eseguire query SelectObjectContent. Consultare la ["Considerazioni e requisiti per l'utilizzo di S3 Select"](#).

Clausole

- SELEZIONARE l'elenco
- CLAUSOLA FROM
- Clausola WHERE
- Clausola di LIMITAZIONE

Tipi di dati

- bool
- intero
- stringa
- fluttuare
- decimale, numerico
- data e ora

Operatori

Operatori logici

- E.
- NO
- OPPURE

Operatori di confronto

- <
- >
- <=
- >=
- =
- =
- <>

- !=
- TRA
- POLL

Operatori di corrispondenza dei modelli

- MI PIACE
- _
- %

Operatori unitari

- È NULL
- NON È NULL

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

Funzioni di aggregazione

- MEDIA()
- CONTEGGIO(*)
- MAX()
- MIN()
- SOMMA()

Funzioni condizionali

- CASO
- COALESCE
- NULLIF

Funzioni di conversione

- CAST (per il tipo di dati supportato)

Funzioni di data

- DATA_ADD
- DATA_DIFF

- ESTRARRE
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funzioni di stringa

- CHAR_LENGTH, CHARACTER_LENGTH
- ABBASSARE
- SOTTOSTRINGA
- TAGLIARE
- SUPERIORE

Utilizzare la crittografia lato server

La crittografia lato server consente di proteggere i dati a oggetti inattivi. StorageGRID crittografa i dati durante la scrittura dell'oggetto e li decrta quando si accede all'oggetto.

Se si desidera utilizzare la crittografia lato server, è possibile scegliere una delle due opzioni che si escludono a vicenda, in base alla modalità di gestione delle chiavi di crittografia:

- **SSE (crittografia lato server con chiavi gestite da StorageGRID):** Quando si invia una richiesta S3 per memorizzare un oggetto, StorageGRID crittografa l'oggetto con una chiave univoca. Quando si invia una richiesta S3 per recuperare l'oggetto, StorageGRID utilizza la chiave memorizzata per decrittare l'oggetto.
- **SSE-C (crittografia lato server con chiavi fornite dal cliente):** Quando si invia una richiesta S3 per memorizzare un oggetto, viene fornita la propria chiave di crittografia. Quando si recupera un oggetto, si fornisce la stessa chiave di crittografia come parte della richiesta. Se le due chiavi di crittografia corrispondono, l'oggetto viene decrittografato e vengono restituiti i dati dell'oggetto.

Mentre StorageGRID gestisce tutte le operazioni di crittografia e decifrazione degli oggetti, è necessario gestire le chiavi di crittografia fornite.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente.



Se un oggetto viene crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Utilizzare SSE

Per crittografare un oggetto con una chiave univoca gestita da StorageGRID, utilizzare la seguente intestazione di richiesta:

```
x-amz-server-side-encryption
```

L'intestazione della richiesta SSE è supportata dalle seguenti operazioni a oggetti:

- "PutObject"

- "Oggetto CopyObject"
- "CreateMultipartUpload"

Utilizzare SSE-C.

Per crittografare un oggetto con una chiave univoca gestita, vengono utilizzate tre intestazioni di richiesta:

Intestazione della richiesta	Descrizione
x-amz-server-side-encryption-customer-algorithm	Specificare l'algoritmo di crittografia. Il valore dell'intestazione deve essere AES256.
x-amz-server-side-encryption-customer-key	Specificare la chiave di crittografia che verrà utilizzata per crittografare o decrittare l'oggetto. Il valore della chiave deve essere 256 bit, con codifica base64.
x-amz-server-side-encryption-customer-key-MD5	Specificare il digest MD5 della chiave di crittografia in base a RFC 1321, utilizzato per garantire che la chiave di crittografia sia stata trasmessa senza errori. Il valore del digest MD5 deve essere a 128 bit con codifica base64.

Le intestazioni delle richieste SSE-C sono supportate dalle seguenti operazioni a oggetti:

- "GetObject"
- "HeadObject (oggetto intestazione)"
- "PutObject"
- "Oggetto CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Considerazioni sull'utilizzo della crittografia lato server con le chiavi fornite dal cliente (SSE-C)

Prima di utilizzare SSE-C, tenere presente quanto segue:

- È necessario utilizzare https.



StorageGRID rifiuta qualsiasi richiesta effettuata tramite http quando si utilizza SSE-C. per motivi di sicurezza, è necessario considerare qualsiasi chiave inviata accidentalmente utilizzando http come compromessa. Eliminare la chiave e ruotarla in base alle necessità.

- L'ETag nella risposta non è l'MD5 dei dati dell'oggetto.
- È necessario gestire il mapping delle chiavi di crittografia agli oggetti. StorageGRID non memorizza le chiavi di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia che fornisce per ciascun oggetto.
- Se il bucket è abilitato per la versione, ogni versione dell'oggetto deve disporre di una propria chiave di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia utilizzata per ciascuna

versione dell'oggetto.

- Poiché si gestiscono le chiavi di crittografia sul lato client, è necessario gestire anche eventuali protezioni aggiuntive, come la rotazione delle chiavi, sul lato client.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente.

- Se la replica cross-grid o CloudMirror è configurata per il bucket, non è possibile acquisire oggetti SSE-C. L'operazione di acquisizione non riesce.

Informazioni correlate

["Manuale dell'utente di Amazon S3: Utilizzo della crittografia lato server con chiavi fornite dal cliente \(SSE-C\)"](#)

Oggetto CopyObject

È possibile utilizzare la richiesta CopyObject S3 per creare una copia di un oggetto già memorizzato in S3. Un'operazione CopyObject è la stessa dell'esecuzione di GetObject seguito da PutObject.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se sono presenti oggetti di dimensioni superiori a 5 GiB, utilizzare ["caricamento multiparte"](#) invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).



Se è stato eseguito l'aggiornamento da StorageGRID 11,6 o versioni precedenti, l'avviso S3 PUT object size too large verrà attivato se si tenta di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11,7 o 11,8, l'avviso non verrà attivato in questo caso. Tuttavia, per allinearsi allo standard AWS S3, le versioni future di StorageGRID non supporteranno il caricamento di oggetti di dimensioni superiori a 5 GiB.

UTF-8 caratteri nei metadati dell'utente

Se una richiesta include valori UTF-8 (non escapati) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento di StorageGRID non è definito.

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 escapati vengono trattati come caratteri ASCII:

- Le richieste hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 escapati.
- StorageGRID non restituisce l'`x-amz-missing-meta` intestazione se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- Content-Type
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since
- x-amz-meta-, seguito da una coppia nome-valore contenente metadati definiti dall'utente
- x-amz-metadata-directive: Il valore predefinito è COPY, che consente di copiare l'oggetto e i metadati associati.

È possibile specificare REPLACE se sovrascrivere i metadati esistenti durante la copia dell'oggetto o se aggiornare i metadati dell'oggetto.

- x-amz-storage-class
- x-amz-tagging-directive: Il valore predefinito è COPY, che consente di copiare l'oggetto e tutti i tag.

È possibile specificare REPLACE di sovrascrivere i tag esistenti durante la copia dell'oggetto o di aggiornare i tag.

- Intestazioni della richiesta di blocco oggetti S3:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la modalità di versione dell'oggetto e mantenere la data fino alla data. Vedere ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#).

- Intestazioni di richiesta SSE:

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

Vedere [Intestazioni di richiesta per la crittografia lato server](#)

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm

Quando si copia un oggetto, se l'oggetto di origine ha un checksum, StorageGRID non copia tale valore checksum nel nuovo oggetto. Questo comportamento si applica sia che si provi o meno a utilizzare `x-amz-checksum-algorithm` nella richiesta dell'oggetto.

- x-amz-website-redirect-location

Opzioni di classe storage

L'`x-amz-storage-class`intestazione della richiesta è supportata e influisce sul numero di copie degli oggetti create da StorageGRID se la regola ILM corrispondente utilizza il doppio commit o bilanciato "[opzione di acquisizione](#)".

- STANDARD

(Impostazione predefinita) specifica un'operazione di ingest dual-commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced (bilanciamento) torna alla creazione di copie interinali.

- REDUCED_REDUNDANCY

Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione di commit doppio o quando l'opzione di bilanciamento ritorna alla creazione di copie interinali.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l'`REDUCED_REDUNDANCY` opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Utilizzo di x-amz-copy-source in CopyObject

Se il bucket e la chiave di origine, specificati nell'`x-amz-copy-source`intestazione, sono diversi dal bucket e dalla chiave di destinazione, una copia dei dati dell'oggetto di origine viene scritta nella destinazione.

Se l'origine e la destinazione corrispondono e l'`x-amz-metadata-directive`intestazione viene specificata come `REPLACE`, i metadati dell'oggetto vengono aggiornati con i valori dei metadati forniti nella richiesta. In questo caso, StorageGRID non reinserisce l'oggetto. Questo ha due conseguenze importanti:

- Non è possibile utilizzare CopyObject per crittografare un oggetto esistente sul posto o per modificare la

crittografia di un oggetto esistente sul posto. Se si fornisce l' `x-amz-server-side-encryption` intestazione o l' `x-amz-server-side-encryption-customer-algorithm` intestazione, StorageGRID rifiuta la richiesta e restituisce `XNotImplemented`.

- L'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background.

Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto.

Intestazioni di richiesta per la crittografia lato server

Se si utilizza ["usa crittografia lato server"](#), le intestazioni di richiesta fornite dipendono dal fatto che l'oggetto di origine sia crittografato e dal fatto che si intenda crittografare l'oggetto di destinazione.

- Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta CopyObject, in modo che l'oggetto possa essere decrittografato e quindi copiato:
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Specificare la chiave di crittografia fornita al momento della creazione dell'oggetto di origine.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto sorgente.
- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca che si fornisce e si gestisce, includere le seguenti tre intestazioni:
 - `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
 - `x-amz-server-side-encryption-customer-key`: Specificare una nuova chiave di crittografia per l'oggetto di destinazione.
 - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della nuova chiave di crittografia.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a ["utilizzo della crittografia lato server"](#).

- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca gestita da StorageGRID (SSE), includere questa intestazione nella richiesta CopyObject:
 - `x-amz-server-side-encryption`



`server-side-encryption` Impossibile aggiornare il valore dell'oggetto. Eseguire invece una copia con un nuovo `server-side-encryption` valore utilizzando `x-amz-metadata-directive: REPLACE`.

Versione

Se il bucket di origine è in versione, è possibile utilizzare l' `x-amz-copy-source` intestazione per copiare la versione più recente di un oggetto. Per copiare una versione specifica di un oggetto, è necessario specificare esplicitamente la versione da copiare utilizzando la `versionId` sottorisorsa. Se il bucket di destinazione è in versione, la versione generata viene restituita nell' `x-amz-version-id` intestazione della risposta. Se la versione è sospesa per il bucket target, `x-amz-version-id` restituisce un valore "null".

GetObject

È possibile utilizzare la richiesta `GetObject` S3 per recuperare un oggetto da un bucket S3.

Oggetti `GetObject` e multiparte

È possibile utilizzare il `partNumber` parametro di richiesta per recuperare una parte specifica di un oggetto multiparte o segmentato. L' `x-amz-mp-parts-count` elemento di risposta indica il numero di parti dell'oggetto.

È possibile impostare `partNumber` su 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, l' `x-amz-mp-parts-count` elemento di risposta viene restituito solo per gli oggetti segmentati o multiparte.

UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. LE richieste di RECUPERO per un oggetto con caratteri UTF-8 di escape nei metadati definiti dall'utente non restituiscono l' `x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

Intestazione richiesta supportata

È supportata la seguente intestazione della richiesta:

- `x-amz-checksum-mode`: Specificare `ENABLED`

L' `Range` intestazione non è supportata con `x-amz-checksum-mode` per `GetObject`. Quando si include `Range` nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

Versione

Se non viene specificata una `versionId` sottorisorsa, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "non trovato" con l' `x-amz-delete-marker` intestazione della risposta impostata su `true`.

Intestazioni delle richieste per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)

Utilizzare tutte e tre le intestazioni se l'oggetto è crittografato con una chiave univoca fornita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia dell'oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in ["Utilizzare la crittografia lato server"](#).

Comportamento degli oggetti GetObject per Cloud Storage Pool

Se un oggetto è stato memorizzato in ["Pool di cloud storage"](#), il comportamento di una richiesta GetObject dipende dallo stato dell'oggetto. Per ulteriori informazioni, vedere ["HeadObject \(oggetto intestazione\)"](#).



Se un oggetto viene memorizzato in un Cloud Storage Pool e sulla griglia esistono anche una o più copie dell'oggetto, le richieste GetObject tenteranno di recuperare i dati dalla griglia, prima di recuperarli da Cloud Storage Pool.

Stato dell'oggetto	Comportamento di GetObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	200 OK Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK Viene recuperata una copia dell'oggetto.
Oggetto sottoposto a transizione in uno stato non recuperabile	403 Forbidden, InvalidObjectState Utilizzare una "RestoreObject" richiesta per ripristinare l'oggetto in uno stato recuperabile.
Oggetto in fase di ripristino da uno stato non recuperabile	403 Forbidden, InvalidObjectState Attendere il completamento della richiesta RestoreObject.
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Viene recuperata una copia dell'oggetto.

Oggetti multiparte o segmentati in un pool di storage cloud

Se hai caricato un oggetto multiparte o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta `GetObject` potrebbe restituire erroneamente `200 OK` quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono state ancora ripristinate.

In questi casi:

- La richiesta `GetObject` potrebbe restituire alcuni dati ma interrompersi a metà del trasferimento.
- Una richiesta `GetObject` successiva potrebbe restituire `403 Forbidden`.

Replica `GetObject` e cross-grid

Se si utilizza "federazione di grid" ed "replica cross-grid" è attivato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta `GetObject`. La risposta include l'intestazione della risposta specifica di StorageGRID `x-ntap-sg-cgr-replication-status`, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	<ul style="list-style-type: none">• COMPLETATO: La replica è riuscita.• PENDING: L'oggetto non è stato ancora replicato.• ERRORE: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA : L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta la `x-amz-replication-status` testata.

HeadObject (oggetto intestazione)

È possibile utilizzare la richiesta `HeadObject` S3 per recuperare i metadati da un oggetto senza restituire l'oggetto stesso. Se l'oggetto viene memorizzato in un Cloud Storage Pool, è possibile utilizzare `HeadObject` per determinare lo stato di transizione dell'oggetto.

Oggetti HeadObject e multiparte

È possibile utilizzare il `partNumber` parametro di richiesta per recuperare i metadati per una parte specifica di un oggetto multiparte o segmentato. L' `x-amz-mp-parts-count` elemento di risposta indica il numero di parti dell'oggetto.

È possibile impostare `partNumber` su 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, l' `x-amz-mp-parts-count` elemento di risposta viene restituito solo per gli oggetti segmentati o multiparte.

UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. Le richieste

HEAD per un oggetto con caratteri UTF-8 di escape nei metadati definiti dall'utente non restituiscono l' `x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

Intestazione richiesta supportata

È supportata la seguente intestazione della richiesta:

- `x-amz-checksum-mode`

Il `partNumber` parametro e `Range` l'intestazione non sono supportati con `x-amz-checksum-mode` per `HeadObject`. Quando vengono inclusi nella richiesta con `x-amz-checksum-mode` abilitato, `StorageGRID` non restituisce un valore checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

Versione

Se non viene specificata una `versionId` sottorisorsa, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "non trovato" con l' `x-amz-delete-marker` intestazione della risposta impostata su `true`.

Intestazioni delle richieste per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)

Utilizzare tutte e tre queste intestazioni se l'oggetto è crittografato con una chiave univoca fornita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia dell'oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in ["Utilizzare la crittografia lato server"](#).

Risposte `HeadObject` per gli oggetti `Cloud Storage Pool`

Se l'oggetto è memorizzato in ["Pool di cloud storage"](#), vengono restituite le seguenti intestazioni di risposta:

- `x-amz-storage-class`: `GLACIER`
- `x-amz-restore`

Le intestazioni delle risposte forniscono informazioni sullo stato di un oggetto quando viene spostato in un `Cloud Storage Pool`, facoltativamente trasferito in uno stato non recuperabile e ripristinato.

Stato dell'oggetto	Risposta a HeadObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	200 OK (Non viene restituita alcuna intestazione di risposta speciale).
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Fino a quando l'oggetto non viene spostato in uno stato non recuperabile, il valore per viene impostato su un expiry-date tempo lontano in futuro. L'ora esatta della transizione non è controllata dal sistema StorageGRID.</p>
L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche nella griglia	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Il valore per expiry-date è impostato su un certo tempo lontano in futuro.</p> <p>Nota: Se la copia nella griglia non è disponibile (ad esempio, un nodo di archiviazione è inattivo), è necessario eseguire una "RestoreObject" richiesta di ripristino della copia dal pool di archiviazione cloud prima di poter recuperare correttamente l'oggetto.</p>
L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia nella griglia	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Oggetto in fase di ripristino da uno stato non recuperabile	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>

Stato dell'oggetto	Risposta a HeadObject
Oggetto completamente ripristinato nel Cloud Storage Pool	<pre>200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"</pre> <div> `expiry-date`Indica quando l'oggetto nel Cloud Storage Pool verrà riportato a uno stato non recuperabile. </div>

Oggetti multiparte o segmentati nel Cloud Storage Pool

Se hai caricato un oggetto multiparte o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta HeadObject potrebbe restituire erroneamente `x-amz-restore: ongoing-request="false"` quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono state ancora ripristinate.

HeadObject e replica cross-grid

Se si utilizza ["federazione di grid"](#) ed ["replica cross-grid"](#) è attivato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta HeadObject. La risposta include l'intestazione della risposta specifica di StorageGRID `x-ntap-sg-cgr-replication-status`, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	<ul style="list-style-type: none"> • COMPLETATO: La replica è riuscita. • PENDING: L'oggetto non è stato ancora replicato. • ERRORE: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA: L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta la `x-amz-replication-status` testata.

PutObject

È possibile utilizzare la richiesta S3 PutObject per aggiungere un oggetto a un bucket.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se sono presenti oggetti di dimensioni superiori a 5 GiB, utilizzare ["caricamento multiparte"](#) invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).



Se è stato eseguito l'aggiornamento da StorageGRID 11,6 o versioni precedenti, l'avviso S3 PUT object size too large verrà attivato se si tenta di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11,7 o 11,8, l'avviso non verrà attivato in questo caso. Tuttavia, per allinearsi allo standard AWS S3, le versioni future di StorageGRID non supporteranno il caricamento di oggetti di dimensioni superiori a 5 GiB.

Dimensione dei metadati dell'utente

Amazon S3 limita la dimensione dei metadati definiti dall'utente all'interno di ogni intestazione di richiesta PUT a 2 KB. StorageGRID limita i metadati dell'utente a 24 KiB. La dimensione dei metadati definiti dall'utente viene misurata prendendo la somma del numero di byte nella codifica UTF-8 di ogni chiave e valore.

UTF-8 caratteri nei metadati dell'utente

Se una richiesta include valori UTF-8 (non escapati) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento di StorageGRID non è definito.

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 escapati vengono trattati come caratteri ASCII:

- Le richieste PutObject, CopyObject, GetObject e HeadObject hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 di escape.
- StorageGRID non restituisce l'`x-amz-missing-meta` intestazione se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Limiti tag oggetto

È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole.

Proprietà degli oggetti

In StorageGRID, tutti gli oggetti sono di proprietà dell'account del proprietario del bucket, inclusi gli oggetti creati da un account non proprietario o da un utente anonimo.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- Cache-Control
- Content-Disposition
- Content-Encoding

Quando si specifica `aws-chunked` per Content-Encoding StorageGRID non verifica i seguenti elementi:

- StorageGRID non verifica il `chunk-signature` rispetto ai dati del blocco.
- StorageGRID non verifica il valore fornito per `x-amz-decoded-content-length` rispetto all'oggetto.
- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

La codifica di trasferimento a blocchi è supportata se `aws-chunked` si utilizza anche la firma del payload.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente.

Quando si specifica la coppia nome-valore per i metadati definiti dall'utente, utilizzare questo formato generale:

```
x-amz-meta-name: value
```

Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano al momento della creazione dell'oggetto. Ad esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per `creation-time` viene valutato in secondi dal 1 gennaio 1970.



Una regola ILM non può utilizzare sia un **tempo di creazione definito dall'utente** per il tempo di riferimento che l'opzione di acquisizione bilanciata o rigorosa. Quando viene creata la regola ILM viene restituito un errore.

- `x-amz-tagging`
- Intestazioni di richiesta blocco oggetti S3
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`

- `x-amz-object-lock-legal-hold`

Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la modalità di versione dell'oggetto e mantenere la data fino alla data. Vedere ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#).

- Intestazioni di richiesta SSE:

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

Vedere [Intestazioni di richiesta per la crittografia lato server](#)

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `If-Match`
- `If-None-Match`
- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

La `x-amz-website-redirect-location` testata ritorna `XNotImplemented`.

Opzioni di classe storage

L'`x-amz-storage-class` intestazione della richiesta è supportata. Il valore inviato per `x-amz-storage-class` influisce sul modo in cui StorageGRID protegge i dati degli oggetti durante l'acquisizione e non sul numero di copie persistenti dell'oggetto memorizzate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto acquisito utilizza l'opzione di acquisizione rigorosa, l'`x-amz-storage-class` intestazione non ha effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class`:

- **STANDARD** (Impostazione predefinita)
 - **Doppio commit:** Se la regola ILM specifica l'opzione doppio commit per il comportamento di Ingest, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita in un nodo di storage diverso (doppio commit). Quando viene valutato ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento della regola. In caso contrario, potrebbe essere necessario creare nuove copie degli oggetti in posizioni diverse e eliminare le copie intermedie iniziali.

- **Balanced:** Se la regola ILM specifica l'opzione Balanced (bilanciamento) e StorageGRID non può eseguire immediatamente tutte le copie specificate nella regola, StorageGRID esegue due copie intermedie su nodi di storage diversi.

Se StorageGRID è in grado di creare immediatamente tutte le copie dell'oggetto specificate nella regola ILM (posizionamento sincrono), l'`x-amz-storage-class` intestazione non ha effetto.

- **REDUCED_REDUNDANCY**

- **Commit doppio:** Se la regola ILM specifica l'opzione commit doppio per il comportamento di Ingest, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (commit singolo).
- **Balanced:** Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. L'`REDUCED_REDUNDANCY` opzione viene utilizzata in modo ottimale quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso l'utilizzo di `REDUCED_REDUNDANCY` elimina la creazione e la cancellazione non necessarie di una copia degli oggetti extra per ogni operazione di acquisizione.

L'uso dell'`REDUCED_REDUNDANCY` opzione non è consigliato in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.



Avere una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

La specifica `REDUCED_REDUNDANCY` influisce solo sul numero di copie create al momento della prima acquisizione di un oggetto. Non influisce sul numero di copie dell'oggetto create quando l'oggetto viene valutato dalle policy ILM attive e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l'`REDUCED_REDUNDANCY` opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE:** Utilizzare la seguente intestazione se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID.
 - `x-amz-server-side-encryption`

Quando l'`x-amz-server-side-encryption` intestazione non è inclusa nella richiesta PutObject, l'intera griglia "[impostazione di crittografia degli oggetti archiviati](#)" viene omessa dalla risposta PutObject.

- **SSE-C:** Utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca che si fornisce e si gestisce.
 - `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
 - `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per il nuovo oggetto.
 - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a ["utilizzo della crittografia lato server"](#).



Se un oggetto viene crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Versione

Se la versione è abilitata per un bucket, viene generato automaticamente un univoco `versionId` per la versione dell'oggetto che viene memorizzato. Questo `versionId` viene anche restituito nella risposta utilizzando l' `x-amz-version-id` intestazione della risposta.

Se la versione è sospesa, la versione oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, verrà sovrascritta.

Calcoli della firma per l'intestazione autorizzazione

Quando si utilizza l' `Authorization` intestazione per autenticare le richieste, StorageGRID differisce da AWS nei seguenti modi:

- StorageGRID non richiede che `host` le intestazioni siano incluse in `CanonicalHeaders`.
- StorageGRID non richiede di `Content-Type` essere incluso in `CanonicalHeaders`.
- StorageGRID non richiede che `x-amz-*` le intestazioni siano incluse in `CanonicalHeaders`.



Come procedura consigliata generale, includere sempre queste intestazioni all'interno `CanonicalHeaders` per assicurarsi che siano verificate; tuttavia, se si escludono queste intestazioni, StorageGRID non restituisce un errore.

Per ulteriori informazioni, fare riferimento alla ["Calcoli della firma per l'intestazione dell'autorizzazione: Trasferimento del payload in un singolo chunk \(firma AWS versione 4\)"](#).

Informazioni correlate

- ["Gestire gli oggetti con ILM"](#)
- ["Riferimento API Amazon Simple Storage Service: PutObject"](#)

RestoreObject

È possibile utilizzare la richiesta S3 `RestoreObject` per ripristinare un oggetto memorizzato in un Cloud Storage Pool.

Tipo di richiesta supportato

StorageGRID supporta solo le richieste `RestoreObject` per ripristinare un oggetto. Non supporta il `SELECT` tipo di restauro. Selezionare Richieste restituite `XNotImplemented`.

Versione

Facoltativamente, specificare `versionId` per ripristinare una versione specifica di un oggetto in un bucket in versione. Se non si specifica `versionId`, viene ripristinata la versione più recente dell'oggetto

Comportamento di `RestoreObject` negli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in una "[Pool di cloud storage](#)", una richiesta `RestoreObject` presenta il seguente comportamento, in base allo stato dell'oggetto. Per ulteriori informazioni, vedere "[HeadObject \(oggetto intestazione\)](#)".



Se un oggetto viene memorizzato in un Cloud Storage Pool ed esistono anche una o più copie dell'oggetto nella griglia, non è necessario ripristinarlo inviando una richiesta `RestoreObject`. La copia locale può essere recuperata direttamente, utilizzando una richiesta `GetObject`.

Stato dell'oggetto	Comportamento di <code>RestoreObject</code>
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto non presente in un pool di storage cloud	403 Forbidden, InvalidObjectState
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK Non vengono apportate modifiche. Nota: Prima che un oggetto sia stato spostato in uno stato non recuperabile, non è possibile modificare il suo <code>expiry-date</code> .
Oggetto sottoposto a transizione in uno stato non recuperabile	202 Accepted Ripristina una copia recuperabile dell'oggetto in Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Al termine di questo periodo, l'oggetto viene riportato in uno stato non recuperabile. Facoltativamente, utilizzare l' <code>Tier</code> elemento di richiesta per determinare il tempo necessario per completare il processo di ripristino (<code>Expedited</code> , <code>Standard</code> o <code>Bulk</code>). Se non si specifica <code>Tier</code> , viene utilizzato il <code>Standard</code> livello. Importante: Se un oggetto è stato spostato in S3 Glacier Deep Archive o Cloud Storage Pool utilizza l'archiviazione BLOB di Azure, non puoi ripristinarlo utilizzando il <code>Expedited Tier</code> . Viene restituito il seguente errore 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.
Oggetto in fase di ripristino da uno stato non recuperabile	409 Conflict, RestoreAlreadyInProgress

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto completamente ripristinato nel Cloud Storage Pool	<p>200 OK</p> <p>Nota: se un oggetto è stato ripristinato ad uno stato recuperabile, è possibile modificarlo <code>expiry-date</code> rimettendo la richiesta <code>RestoreObject</code> con un nuovo valore per <code>Days</code>. La data di ripristino viene aggiornata in relazione all'ora della richiesta.</p>

SelectObjectContent

È possibile utilizzare la richiesta S3 `SelectObjectContent` per filtrare il contenuto di un oggetto S3 in base a una semplice istruzione SQL.

Per ulteriori informazioni, vedere ["Riferimento API Amazon Simple Storage Service: SelectObjectContent"](#).

Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 Select.
- Si dispone dell' `s3:GetObject` autorizzazione per l'oggetto che si desidera sottoporre a query.
- L'oggetto che si desidera sottoporre a query deve essere in uno dei seguenti formati:
 - **CSV**. Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
 - **Parquet**. Requisiti aggiuntivi per gli oggetti in parquet:
 - S3 Select supporta solo la compressione colonnare con GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti parquet.
 - S3 Select non supporta l'output parquet. Specificare il formato di output come CSV o JSON.
 - La dimensione massima del gruppo di righe non compresso è di 512 MB.
 - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
 - Non è possibile utilizzare TIPI logici INTERVAL, JSON, LIST, TIME o UUID.
- L'espressione SQL ha una lunghezza massima di 256 KB.
- Qualsiasi record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi per le richieste CSV

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

Esempio di sintassi della richiesta di parquet


```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

Esempio di query SQL

Questa query ottiene il nome dello stato, 2010 popolazioni, 2015 popolazioni stimate e la percentuale di cambiamento rispetto ai dati del censimento degli Stati Uniti. I record nel file che non sono stati vengono ignorati.

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

Le prime righe del file da interrogare, SUB-EST2020_ALL.csv, sono simili a quanto segue:

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717
```

Esempio di utilizzo di AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Le prime righe del file di output, changes.csv, sono simili a queste:

```
Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246
```

Esempio di utilizzo di AWS-CLI (Parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

Le prime righe del file di output, Changes.csv, sono le seguenti:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operazioni per caricamenti multiparte

Operazioni per caricamenti multiparte

Questa sezione descrive come StorageGRID supporta le operazioni per gli upload di più parti.

Le seguenti condizioni e note si applicano a tutte le operazioni di caricamento multiparte:

- Non si devono superare i 1.000 caricamenti simultanei di più parti in un singolo bucket, poiché i risultati delle query ListMultipartUploads per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID applica i limiti di dimensione AWS per le parti multipart. I client S3 devono seguire queste linee guida:
 - Ciascuna parte di un caricamento multiparte deve essere compresa tra 5 MiB (5,242,880 byte) e 5 GiB (5,368,709,120 byte).
 - L'ultima parte può essere inferiore a 5 MiB (5,242,880 byte).
 - In generale, le dimensioni delle parti devono essere il più grandi possibile. Ad esempio, utilizzare le dimensioni delle parti di 5 GiB per un oggetto 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce l'overhead dei metadati StorageGRID.
 - Per gli oggetti di dimensioni inferiori a 5 GiB, prendere in considerazione l'utilizzo di un caricamento non multiparte.
- ILM viene valutato per ogni parte di un oggetto multiparte nel momento in cui viene acquisito e per l'oggetto nel suo insieme al completamento del caricamento multiparte, se la regola ILM utilizza il bilanciato o rigoroso ["opzione di acquisizione"](#). Devi essere consapevole di come questo influisca sul posizionamento di oggetti e parti:
 - Se ILM cambia mentre è in corso un caricamento multiparte S3, alcune parti dell'oggetto potrebbero

non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. Qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e spostata nella posizione corretta in un secondo momento.

- Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più grandi sono memorizzati a DC1 GB mentre tutti gli oggetti più piccoli sono memorizzati a DC2 GB, ogni parte da 1 GB di un caricamento multiparte in 10 parti viene memorizzata a DC2 GB al momento dell'acquisizione. Tuttavia, quando ILM viene valutato per l'oggetto nel suo complesso, tutte le parti dell'oggetto vengono spostate in DC1.
- Tutte le operazioni di caricamento multiparte supportano StorageGRID ["valori di coerenza"](#) .
- Quando un oggetto viene acquisito utilizzando il caricamento multiparte, ["Soglia di segmentazione degli oggetti \(1 GiB\)"](#) non viene applicato.
- Se necessario, è possibile utilizzare ["crittografia lato server"](#) con caricamenti multiparte. Per utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID), è necessario includere l'`x-amz-server-side-encryption` intestazione della richiesta solo nella richiesta CreateMultipartUpload. Per utilizzare SSE-C (crittografia lato server con chiavi fornite dal cliente), specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta CreateMultipartUpload e in ogni richiesta UploadPart successiva.
- Un oggetto caricato in più parti è incluso in un ["secchio di rami"](#) se l'acquisizione è stata avviata prima del timestamp Before del bucket di base, indipendentemente dal momento in cui viene completato il caricamento.

Operazione	Implementazione
AbortMultipartUpload	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
CompleteMultipartUpload	Vedere "CompleteMultipartUpload"
CreateMultipartUpload (Precedentemente denominato Initiate Multipart Upload)	Vedere "CreateMultipartUpload"
ListMultipartUploads	Vedere "ListMultipartUploads"
ListParts	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
UploadPart	Vedere "UploadPart"
UploadPartCopy	Vedere "UploadPartCopy"

CompleteMultipartUpload

L'operazione CompleteMultipartUpload completa il caricamento multiparte di un oggetto assemblando le parti caricate in precedenza.



StorageGRID supporta valori non consecutivi in ordine crescente per il `partNumber` parametro di richiesta con `CompleteMultipartUpload`. Il parametro può iniziare con qualsiasi valore.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

L' `x-amz-storage-class` intestazione influisce sul numero di copie di oggetti create da StorageGRID se la regola ILM corrispondente specifica ["Dual commit o opzione di acquisizione bilanciata"](#).

- `STANDARD`

(Impostazione predefinita) specifica un'operazione di ingest dual-commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced (bilanciamento) torna alla creazione di copie interinali.

- `REDUCED_REDUNDANCY`

Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione di commit doppio o quando l'opzione di bilanciamento ritorna alla creazione di copie interinali.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l' `REDUCED_REDUNDANCY` opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.



Se un caricamento multipart non viene completato entro 15 giorni, l'operazione viene contrassegnata come inattiva e tutti i dati associati vengono cancellati dal sistema.



Il `ETag` valore restituito non è una somma di MD5 dei dati, ma segue l'implementazione API Amazon S3 del `ETag` valore per gli oggetti multipart.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `If-Match`
- `If-None-Match`
- `x-amz-sdk-checksum-algorithm`

- `x-amz-trailer`

Versione

Questa operazione completa un caricamento multiparte. Se il controllo delle versioni è attivato per un bucket, la versione dell'oggetto viene creata al termine del caricamento multiparte.

Se la versione è abilitata per un bucket, viene generato automaticamente un univoco `versionId` per la versione dell'oggetto che viene memorizzato. Questo `versionId` viene anche restituito nella risposta utilizzando l' `x-amz-version-id` intestazione della risposta.

Se la versione è sospesa, la versione oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, verrà sovrascritta.



Quando il controllo delle versioni è attivato per un bucket, il completamento di un caricamento multiparte crea sempre una nuova versione, anche se ci sono caricamenti multipli simultanei completati sulla stessa chiave a oggetti. Quando il controllo delle versioni non è abilitato per un bucket, è possibile avviare un caricamento multiparte e fare in modo che un altro caricamento multiparte venga avviato e completato prima sulla stessa chiave a oggetti. Nei bucket senza versione, il caricamento multiparte che completa l'ultimo ha la precedenza.

Replica, notifica o notifica dei metadati non riuscite

Se il bucket in cui si verifica il caricamento multiparte è configurato per un servizio di piattaforma, il caricamento multiparte riesce anche se l'azione di replica o notifica associata non riesce.

Un tenant può attivare la replica o la notifica non riuscita aggiornando i metadati o i tag dell'oggetto. Un tenant può reinviare i valori esistenti per evitare modifiche indesiderate.

Fare riferimento alla ["Risolvere i problemi relativi ai servizi della piattaforma"](#).

CreateMultipartUpload

L'operazione `CreateMultipartUpload` (precedentemente denominata `Initiate Multipart Upload`) avvia un caricamento multiparte per un oggetto e restituisce un ID di caricamento.

L'`x-amz-storage-class` intestazione della richiesta è supportata. Il valore inviato per `x-amz-storage-class` influisce sul modo in cui StorageGRID protegge i dati degli oggetti durante l'acquisizione e non sul numero di copie persistenti dell'oggetto memorizzate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto acquisito utilizza Strict ["opzione di acquisizione"](#), l' `x-amz-storage-class` intestazione non ha alcun effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class`:

- **STANDARD** (Impostazione predefinita)
 - **Dual Commit:** Se la regola ILM specifica l'opzione di acquisizione **Dual Commit**, non appena un oggetto viene acquisito una seconda copia di tale oggetto viene creata e distribuita in un nodo di archiviazione diverso (dual commit). Quando viene valutato ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento della regola. In caso contrario,

potrebbe essere necessario creare nuove copie degli oggetti in posizioni diverse e eliminare le copie intermedie iniziali.

- **Balanced:** Se la regola ILM specifica l'opzione Balanced (bilanciamento) e StorageGRID non può eseguire immediatamente tutte le copie specificate nella regola, StorageGRID esegue due copie intermedie su nodi di storage diversi.

Se StorageGRID è in grado di creare immediatamente tutte le copie dell'oggetto specificate nella regola ILM (posizionamento sincrono), l'`x-amz-storage-class` intestazione non ha effetto.

- **REDUCED_REDUNDANCY**

- **Dual Commit:** Se la regola ILM specifica l'opzione Dual Commit, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (Single Commit).
- **Balanced:** Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. L'`REDUCED_REDUNDANCY` opzione viene utilizzata in modo ottimale quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso l'utilizzo di `REDUCED_REDUNDANCY` elimina la creazione e la cancellazione non necessarie di una copia degli oggetti extra per ogni operazione di acquisizione.

L'uso dell'`REDUCED_REDUNDANCY` opzione non è consigliato in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.



Avere una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

La specifica `REDUCED_REDUNDANCY` influisce solo sul numero di copie create al momento della prima acquisizione di un oggetto. Non influisce sul numero di copie dell'oggetto create quando l'oggetto viene valutato dalle policy ILM attive e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l'`REDUCED_REDUNDANCY` opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- Content-Type
- x-amz-checksum-algorithm

Attualmente, è supportato solo il valore SHA256 per `x-amz-checksum-algorithm`.

- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente

Quando si specifica la coppia nome-valore per i metadati definiti dall'utente, utilizzare questo formato generale:

```
x-amz-meta-_name_: `value`
```

Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano al momento della creazione dell'oggetto. Ad esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per `creation-time` viene valutato in secondi dal 1 gennaio 1970.



L'aggiunta `creation-time` come metadati definiti dall'utente non è consentita se si aggiunge un oggetto a un bucket in cui è abilitata la conformità legacy. Viene restituito un errore.

- Intestazioni della richiesta di blocco oggetti S3:

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la versione dell'oggetto che resta aggiornata.

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

- Intestazioni di richiesta SSE:

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

[Intestazioni di richiesta per la crittografia lato server](#)



Per informazioni sul modo in cui StorageGRID gestisce i caratteri UTF-8, vedere ["PutObject"](#).

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto multiparte con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE**: Utilizzare la seguente intestazione nella richiesta CreateMultipartUpload se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste UploadPart.
 - `x-amz-server-side-encryption`
- **SSE-C**: Utilizzare tutte e tre le intestazioni nella richiesta CreateMultipartUpload (e in ogni richiesta UploadPart successiva) se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.
 - `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
 - `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per il nuovo oggetto.
 - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a ["utilizzo della crittografia lato server"](#).

Intestazioni di richiesta non supportate

La seguente intestazione della richiesta non è supportata:

- `x-amz-website-redirect-location`

La `x-amz-website-redirect-location` testata ritorna `XNotImplemented`.

Versione

Il caricamento multipart consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

ListMultipartUploads

L'operazione ListMultipartUploads elenca i caricamenti multipart in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`

- Authorization

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

UploadPart

L'operazione UploadPart carica una parte in un upload multiparte per un oggetto.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

Intestazioni di richiesta per la crittografia lato server

Se è stata specificata la crittografia SSE-C per la richiesta CreateMultipartUpload, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPart:

- x-amz-server-side-encryption-customer-algorithm: Specificare AES256.
- x-amz-server-side-encryption-customer-key: Specificare la stessa chiave di crittografia fornita nella richiesta CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5: Specificare lo stesso digest MD5 fornito nella richiesta CreateMultipartUpload.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in ["Utilizzare la crittografia lato server"](#).

Se è stato specificato un checksum SHA-256 durante la richiesta CreateMultipartUpload, è necessario includere anche l'intestazione della richiesta seguente in ogni richiesta UploadPart:

- x-amz-checksum-sha256: Specificare il checksum SHA-256 per questa parte.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Versione

Il caricamento multipart consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione `CompleteMultipartUpload`, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

UploadPartCopy

L'operazione `UploadPartCopy` carica una parte di un oggetto copiando i dati da un oggetto esistente come origine dati.

L'operazione `UploadPartCopy` viene implementata con tutto il comportamento dell'API REST Amazon S3. Soggetto a modifiche senza preavviso.

Questa richiesta legge e scrive i dati dell'oggetto specificati in `x-amz-copy-source-range` sistema StorageGRID.

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Intestazioni di richiesta per la crittografia lato server

Se è stata specificata la crittografia SSE-C per la richiesta `CreateMultipartUpload`, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta `UploadPartCopy`:

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specificare la stessa chiave di crittografia fornita nella richiesta `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare lo stesso digest MD5 fornito nella richiesta `CreateMultipartUpload`.

Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta `UploadPartCopy`, in modo che l'oggetto possa essere decrittografato e quindi copiato:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-copy-source-server-side-encryption-customer-key`: Specificare la chiave di crittografia fornita al momento della creazione dell'oggetto di origine.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto sorgente.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in ["Utilizzare la crittografia lato server"](#).

Versione

Il caricamento multipart consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione CompleteMultipartUpload, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

Risposte agli errori

Il sistema StorageGRID supporta tutte le risposte di errore standard dell'API REST S3 applicabili. Inoltre, l'implementazione di StorageGRID aggiunge diverse risposte personalizzate.

Codici di errore S3 API supportati

Nome	Stato HTTP
Accesso negato	403 proibita
BadDigest	400 richiesta errata
BucketAlreadyExists	409 conflitto
BucketNotEmpty	409 conflitto
IncompleteBody	400 richiesta errata
InternalError	500 errore interno del server
InvalidAccessKeyId	403 proibita
Documento invalidato	400 richiesta errata
InvalidBucketName	400 richiesta errata
InvalidBucketState	409 conflitto
InvalidDigest	400 richiesta errata
InvalidEncryptionAlgorithmError	400 richiesta errata
InvalidPart	400 richiesta errata
InvalidPartOrder	400 richiesta errata
InvalidRange	416 intervallo richiesto non riscontrabile

Nome	Stato HTTP
InvalidRequest	400 richiesta errata
InvalidStorageClass	400 richiesta errata
InvalidTag	400 richiesta errata
InvalidURI	400 richiesta errata
KeyTooLong	400 richiesta errata
MalformedXML	400 richiesta errata
MetadataTooLarge	400 richiesta errata
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
MissingRequestBodyError	400 richiesta errata
MissingSecurityHeader	400 richiesta errata
NoSuchBucket	404 non trovato
NoSuchKey	404 non trovato
NoSuchUpload	404 non trovato
Non soddisfatto	501 non implementato
NoSuchBucketPolicy	404 non trovato
ObjectLockConfigurationNotFoundError	404 non trovato
PrecondizioneFailed	412 precondizione non riuscita
RequestTimeTooSkewed	403 proibita
ServiceUnavailable (Servizio non disponibile)	503 Servizio non disponibile
SignatureDoesNotMatch	403 proibita
TooManyBucket	400 richiesta errata

Nome	Stato HTTP
UserKeyMustBeSpecified	400 richiesta errata

Codici di errore personalizzati StorageGRID

Nome	Descrizione	Stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket compatibile legacy	400 richiesta errata
XBucketPolicyParseException	Impossibile analizzare JSON policy bucket ricevuta.	400 richiesta errata
XComplianceConflict	Operazione negata a causa delle impostazioni di conformità legacy.	403 proibita
XComplianceRiduciRedundancyProibita	La ridondanza ridotta non è consentita nel bucket compatibile legacy	400 richiesta errata
XMaxBucketPolicyLengthExceed	La policy supera la lunghezza massima consentita della policy bucket.	400 richiesta errata
XMissingInternalRequestHeader	Manca un'intestazione di una richiesta interna.	400 richiesta errata
Conformità XNoSuchBucketCompliance	Nel bucket specificato non è attivata la compliance legacy.	404 non trovato
XNotAcceptable (XNotAccettabile)	La richiesta contiene una o più intestazioni di accettazione che non possono essere soddisfatte.	406 non accettabile
XNotImplemented	La richiesta fornita implica funzionalità non implementate.	501 non implementato

Operazioni personalizzate di StorageGRID

Operazioni personalizzate di StorageGRID

Il sistema StorageGRID supporta operazioni personalizzate che vengono aggiunte all'API REST S3.

Nella tabella seguente sono elencate le operazioni personalizzate supportate da StorageGRID.

Operazione	Descrizione
"COERENZA del bucket"	Restituisce la coerenza applicata a un determinato bucket.
"METTI la coerenza del bucket"	Imposta la coerenza applicata a un particolare bucket.
"OTTIENI l'ultimo tempo di accesso a bucket"	Restituisce se gli ultimi aggiornamenti dell'ora di accesso sono attivati o disattivati per un bucket specifico.
"TEMPO ULTIMO accesso bucket"	Consente di attivare o disattivare gli ultimi aggiornamenti dell'orario di accesso per un determinato bucket.
"ELIMINA la configurazione di notifica dei metadati del bucket"	Elimina l'XML di configurazione della notifica dei metadati associato a un bucket specifico.
"OTTIENI la configurazione della notifica dei metadati del bucket"	Restituisce l'XML di configurazione della notifica dei metadati associato a un bucket specifico.
"INSERIRE la configurazione della notifica dei metadati del bucket"	Configura il servizio di notifica dei metadati per un bucket.
"OTTIENI l'utilizzo dello storage"	Indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account.
"Obsoleto: CreateBucket con impostazioni di conformità"	Obsoleto e non supportato: Non è più possibile creare nuovi bucket con Compliance abilitata.
"Obsoleto: OTTIENI la compliance del bucket"	Obsoleto ma supportato: Restituisce le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.
"Obsoleto: METTI la compliance del bucket"	Obsoleto ma supportato: Consente di modificare le impostazioni di conformità per un bucket compatibile esistente.

COERENZA del bucket

La richiesta di coerenza GET Bucket consente di determinare la coerenza applicata a un determinato bucket.

La coerenza predefinita è impostata per garantire la lettura dopo scrittura per gli oggetti appena creati.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketConsistency o essere root dell'account.

Esempio di richiesta

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Nella risposta XML, <Consistency> restituirà uno dei seguenti valori:

Coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
read-after-new-write	(Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
disponibile	Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Esempio di risposta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informazioni correlate

METTI la coerenza del bucket

La richiesta di coerenza PUT bucket consente di specificare la coerenza da applicare alle operazioni eseguite su un bucket.

La coerenza predefinita è impostata per garantire la lettura dopo scrittura per gli oggetti appena creati.

Prima di iniziare

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketConsistency o essere root dell'account.

Richiesta

Il `x-ntap-sg-consistency` parametro deve contenere uno dei seguenti valori:

Coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
read-after-new-write	(Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
disponibile	Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Nota: in generale, si dovrebbe usare la coerenza "Read-after-new-write". Se le richieste non funzionano correttamente, modificare il comportamento del client dell'applicazione, se possibile. In alternativa, configurare il client per specificare la coerenza per ogni richiesta API. Impostare la consistenza a livello del bucket solo come ultima risorsa.

Esempio di richiesta

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informazioni correlate

["Coerenza"](#)

OTTIENI l'ultimo tempo di accesso a bucket

La richiesta GET bucket last access time (OTTIENI bucket ultimo accesso) consente di determinare se gli ultimi aggiornamenti dell'orario di accesso sono attivati o disattivati per i singoli bucket.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketLastAccessTime o essere root dell'account.

Esempio di richiesta

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra che gli ultimi aggiornamenti dell'ora di accesso sono attivati per il bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

TEMPO ULTIMO accesso bucket

La richiesta PUT bucket Last access time consente di attivare o disattivare gli ultimi aggiornamenti del tempo di accesso per i singoli bucket. La disattivazione degli ultimi aggiornamenti dell'orario di accesso migliora le prestazioni ed è l'impostazione

predefinita per tutti i bucket creati con la versione 10.3.0 o successiva.

Per completare questa operazione, è necessario disporre dell'autorizzazione `s3:PutBucketLastAccessTime` per un bucket o essere root dell'account.



A partire dalla versione 10.3 di StorageGRID, gli aggiornamenti all'ultimo tempo di accesso sono disattivati per impostazione predefinita per tutti i nuovi bucket. Se si dispone di bucket creati utilizzando una versione precedente di StorageGRID e si desidera che corrispondano al nuovo comportamento predefinito, è necessario disattivare esplicitamente gli ultimi aggiornamenti del tempo di accesso per ciascuno di questi bucket precedenti. È possibile attivare o disattivare gli aggiornamenti per l'ora dell'ultimo accesso utilizzando la richiesta PUT Bucket last access time o dalla pagina dei dettagli di un bucket in Tenant Manager. Vedere ["Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso"](#).

Se gli ultimi aggiornamenti dell'ora di accesso sono disattivati per un bucket, alle operazioni sul bucket viene applicato il seguente comportamento:

- Le richieste `GetObject`, `GetObjectAcl`, `GetObjectTagging` e `HeadObject` non aggiornano l'ora dell'ultimo accesso. L'oggetto non viene aggiunto alle code per la valutazione ILM (Information Lifecycle Management).
- Le richieste `CopyObject` e `PutObjectTagging` che aggiornano solo i metadati aggiornano anche l'ora dell'ultimo accesso. L'oggetto viene aggiunto alle code per la valutazione ILM.
- Se gli aggiornamenti dell'ora dell'ultimo accesso sono disattivati per il bucket di origine, le richieste `CopyObject` non aggiornano l'ora dell'ultimo accesso per il bucket di origine. L'oggetto copiato non viene aggiunto alle code per la valutazione ILM del bucket di origine. Tuttavia, per la destinazione, le richieste `CopyObject` aggiornano sempre l'ora dell'ultimo accesso. La copia dell'oggetto viene aggiunta alle code per la valutazione ILM.
- `CompleteMultipartUpload` richiede l'aggiornamento dell'ora di ultimo accesso. L'oggetto completato viene aggiunto alle code per la valutazione ILM.

Richiedi esempi

In questo esempio viene attivato l'ultimo tempo di accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Questo esempio disattiva l'ultimo tempo di accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

ELIMINA la configurazione di notifica dei metadati del bucket

La richiesta di configurazione DELLA notifica dei metadati DEL bucket DELETE consente di disattivare il servizio di integrazione della ricerca per i singoli bucket eliminando il file XML di configurazione.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:DeleteBucketMetadataNotification per un bucket o essere root dell'account.

Esempio di richiesta

Questo esempio mostra la disattivazione del servizio di integrazione della ricerca per un bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

OTTIENI la configurazione della notifica dei metadati del bucket

La richiesta DI configurazione DELLA notifica dei metadati GET Bucket consente di recuperare l'XML di configurazione utilizzato per configurare l'integrazione della ricerca per i singoli bucket.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketMetadataNotification o essere root dell'account.

Esempio di richiesta

Questa richiesta recupera la configurazione di notifica dei metadati per il bucket denominato bucket.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Il corpo della risposta include la configurazione della notifica dei metadati per il bucket. La configurazione della notifica dei metadati consente di determinare la configurazione del bucket per l'integrazione della ricerca. Ciò consente di determinare quali oggetti vengono indicizzati e a quali endpoint vengono inviati i metadati degli oggetti.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

Ogni configurazione di notifica dei metadati include una o più regole. Ogni regola specifica gli oggetti a cui si applica e la destinazione in cui StorageGRID deve inviare i metadati degli oggetti. Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	<p>Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati.</p> <p>Contiene uno o più elementi della regola.</p>	Sì
Regola	<p>Tag container 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 della regola.</p> <p>Incluso nell'elemento Rule.</p>	No
Stato	<p>Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate.</p> <p>Incluso nell'elemento Rule.</p>	Sì

Nome	Descrizione	Obbligatorio
Prefisso	<p>Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata.</p> <p>Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Destinazione	<p>Tag container per la destinazione di una regola.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Urna	<p>URNA della destinazione in 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"> • es deve essere il terzo elemento. • L'URN deve terminare con l'indice e digitare dove sono memorizzati i metadati, nel formato domain-name/myindex/mytype. <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404.</p> <p>L'urn è incluso nell'elemento Destination.</p>	Sì

Esempio di risposta

L'XML incluso tra i

```
<MetadataNotificationConfiguration></MetadataNotificationConfiguration>
```

tag mostra come è configurata l'integrazione con un endpoint di integrazione della ricerca per il bucket. In questo esempio, i metadati degli oggetti vengono inviati a un indice Elasticsearch denominato e a un tipo `2017 denominato ospitato in un dominio AWS records denominato current.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Informazioni correlate

["Utilizzare un account tenant"](#)

INSERIRE la configurazione della notifica dei metadati del bucket

La richiesta di configurazione DELLA notifica dei metadati PUT bucket consente di attivare il servizio di integrazione della ricerca per i singoli bucket. L'XML di configurazione della notifica dei metadati fornito nel corpo della richiesta specifica gli oggetti i cui metadati vengono inviati all'indice di ricerca di destinazione.

Per completare questa operazione, è necessario disporre dell'autorizzazione `s3:PutBucketMetadataNotification` per un bucket o essere account root.

Richiesta

La richiesta deve includere la configurazione della notifica dei metadati nel corpo della richiesta. Ogni configurazione di notifica dei metadati include una o più regole. Ogni regola specifica gli oggetti a cui si applica e la destinazione in cui StorageGRID deve inviare i metadati degli oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, è possibile inviare metadati per gli oggetti con il prefisso `/images` a una destinazione e oggetti con il prefisso `/videos` a un'altra.

Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, non è consentita una configurazione che includeva una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2`.

Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID. L'endpoint deve

esistere quando viene inoltrata la configurazione della notifica dei metadati o la richiesta non riesce come un 400 Bad Request. il messaggio di errore indica: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

La tabella descrive gli elementi contenuti nel file XML di configurazione per la notifica dei metadati.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfigration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No

Nome	Descrizione	Obbligatorio
Stato	<p>Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Prefisso	<p>Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata.</p> <p>Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Destinazione	<p>Tag container per la destinazione di una regola.</p> <p>Incluso nell'elemento Rule.</p>	Sì
Urna	<p>URNA della destinazione in 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"> • <code>es</code> deve essere il terzo elemento. • L'URN deve terminare con l'indice e digitare dove sono memorizzati i metadati, nel formato <code>domain-name/myindex/mytype</code>. <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404.</p> <p>L'urn è incluso nell'elemento Destination.</p>	Sì

Richiedi esempi

Questo esempio mostra come abilitare l'integrazione della ricerca per un bucket. In questo esempio, i metadati degli oggetti per tutti gli oggetti vengono inviati alla stessa destinazione.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

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

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

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

JSON generato dal servizio di integrazione della ricerca

Quando si attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. La `test` benna non è in versione, quindi l'etichetta ``versionId`` è vuota.

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

Metadati degli oggetti inclusi nelle notifiche dei metadati

La tabella elenca tutti i campi inclusi nel documento JSON che viene inviato all'endpoint di destinazione quando è attivata l'integrazione della ricerca.

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

Tipo	Nome dell'elemento	Descrizione
Informazioni su bucket e oggetti	bucket	Nome del bucket
Informazioni su bucket e oggetti	chiave	Nome chiave oggetto
Informazioni su bucket e oggetti	ID versione	Versione oggetto, per gli oggetti nei bucket con versione
Informazioni su bucket e oggetti	regione	Ad esempio, la regione del bucket <code>us-east-1</code>
Metadati di sistema	dimensione	Dimensione dell'oggetto (in byte) come visibile a un client HTTP
Metadati di sistema	md5	Hash di oggetto
Metadati dell'utente	metadati <i>key:value</i>	Tutti i metadati dell'utente per l'oggetto, come coppie chiave-valore

Tipo	Nome dell'elemento	Descrizione
Tag	tag <i>key:value</i>	Tutti i tag di oggetto definiti per l'oggetto, come coppie chiave-valore



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

Informazioni correlate

["Utilizzare un account tenant"](#)

OTTIENI la richiesta di utilizzo dello storage

La richiesta GET Storage Usage indica la quantità totale di storage in uso da un account e per ciascun bucket associato all'account.

La quantità di spazio di archiviazione utilizzata da un account e dai relativi bucket può essere ottenuta da una richiesta ListBuckets modificata con il `x-ntap-sg-usage` parametro query. L'utilizzo dello storage bucket viene monitorato separatamente dalle richieste DI PUT ed ELIMINAZIONE elaborate dal sistema. Potrebbe verificarsi un ritardo prima che i valori di utilizzo corrispondano ai valori previsti in base all'elaborazione delle richieste, in particolare se il sistema è sottoposto a un carico pesante.

Per impostazione predefinita, StorageGRID tenta di recuperare le informazioni sull'utilizzo utilizzando una coerenza forte-globale. Se non è possibile ottenere una forte coerenza globale, StorageGRID tenta di recuperare le informazioni sull'utilizzo con una forte coerenza del sito.

Per completare questa operazione, è necessario disporre dell'autorizzazione `s3:ListAllMyBucket` o essere root dell'account.

Esempio di richiesta

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra un account con quattro oggetti e 12 byte di dati in due bucket. Ogni bucket contiene due oggetti e sei byte di dati.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Versione

Ogni versione dell'oggetto memorizzata contribuirà ai `ObjectCount` valori e `DataBytes` nella risposta. I marcatori di eliminazione non vengono aggiunti al `ObjectCount` totale.

Informazioni correlate

["Coerenza"](#)

Richieste bucket obsolete per conformità legacy

Richieste bucket obsolete per conformità legacy

Potrebbe essere necessario utilizzare l'API REST di StorageGRID S3 per gestire i bucket creati utilizzando la funzionalità di conformità legacy.

Funzionalità di compliance obsoleta

La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3.

Se in precedenza è stata attivata l'impostazione di conformità globale, l'impostazione di blocco oggetti S3 globale viene attivata in StorageGRID 11.6. Non è più possibile creare nuovi bucket con la conformità abilitata; tuttavia, se necessario, è possibile utilizzare l'API REST di StorageGRID S3 per gestire qualsiasi bucket compatibile esistente.

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Gestire gli oggetti con ILM"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Richieste di conformità obsolete:

- ["Deprecato - CONSENTE DI APPORTARE modifiche alla richiesta di conformità al bucket"](#)

L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML opzionale di PUT bucket Requests per creare un bucket conforme.

- ["Obsoleto - CONFORMITÀ bucket"](#)

La richiesta DI compliance GET Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.

- ["Deprecato - METTERE la compliance del bucket"](#)

La richiesta DI compliance PUT Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket compatibile esistente. Ad esempio, è possibile mettere un bucket esistente in attesa legale o aumentarne il periodo di conservazione.

Obsoleto: CreateBucket richiede modifiche per la conformità

L'elemento XML SGCompliance è obsoleto. In precedenza, è possibile includere questo elemento personalizzato StorageGRID nel corpo di richiesta XML opzionale delle richieste CreateBucket per creare un bucket conforme.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Non è più possibile creare nuovi bucket con Compliance abilitata. Se si tenta di utilizzare le modifiche della richiesta CreateBucket per la conformità per creare un nuovo bucket conforme, viene visualizzato il seguente messaggio di errore:

```
The Compliance feature is deprecated.  
Contact your StorageGRID administrator if you need to create new Compliant  
buckets.
```

Deprecato: OTTIENI una richiesta di conformità bucket

La richiesta DI compliance GET Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Per completare questa operazione, è necessario disporre dell'autorizzazione `s3:GetBucketCompliance` o essere root dell'account.

Esempio di richiesta

Questa richiesta di esempio consente di determinare le impostazioni di conformità per il bucket denominato `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Nella risposta XML, `<SGCompliance>` elenca le impostazioni di conformità in vigore per il bucket. Questa risposta di esempio mostra le impostazioni di compliance per un bucket in cui ciascun oggetto verrà conservato per un anno (525,600 minuti), a partire da quando l'oggetto viene acquisito nella griglia. Attualmente non esiste un blocco legale in questo bucket. Ogni oggetto verrà automaticamente cancellato dopo un anno.


```

HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>

```

Nome	Descrizione
RetentionPeriodMinutes	La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene acquisito nella griglia.
LegalHold	<ul style="list-style-type: none"> • Vero: Questo bucket è attualmente sotto una stretta legale. Gli oggetti in questo bucket non possono essere cancellati fino a quando non viene revocata la conservazione a fini giudiziari, anche se il periodo di conservazione è scaduto. • Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.
Eliminazione automatica	<ul style="list-style-type: none"> • Vero: Gli oggetti in questo bucket verranno cancellati automaticamente allo scadere del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale. • Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.

Risposte agli errori

Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è 404 Not Found, con un codice di errore S3 di XNoSuchBucketCompliance.

Deprecato: INSERIRE la richiesta di conformità del bucket

La richiesta DI compliance PUT Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket compatibile esistente. Ad esempio, è possibile mettere un bucket esistente in attesa legale o aumentarne il periodo di conservazione.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Per completare questa operazione, è necessario disporre dell'autorizzazione `s3:PutBucketCompliance` o essere root dell'account.

È necessario specificare un valore per ogni campo delle impostazioni di compliance quando si invia una richiesta DI compliance PUT bucket.

Esempio di richiesta

Questa richiesta di esempio modifica le impostazioni di conformità per il bucket denominato `mybucket`. In questo esempio, gli oggetti in verranno conservati per due anni (1.051.200 minuti) invece di un anno, a partire dal momento in `mybucket` cui l'oggetto viene inserito nella griglia. Questo bucket non ha alcuna tenuta legale. Ogni oggetto verrà automaticamente cancellato dopo due anni.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrizione
RetentionPeriodMinutes	<p>La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene acquisito nella griglia.</p> <p>Importante quando si specifica un nuovo valore per <code>RetentionPeriodMinutes</code>, è necessario specificare un valore uguale o superiore al periodo di conservazione corrente del bucket. Una volta impostato il periodo di conservazione del bucket, non è possibile diminuire tale valore, ma solo aumentarlo.</p>

Nome	Descrizione
LegalHold	<ul style="list-style-type: none"> • Vero: Questo bucket è attualmente sotto una stretta legale. Gli oggetti in questo bucket non possono essere cancellati fino a quando non viene revocata la conservazione a fini giudiziari, anche se il periodo di conservazione è scaduto. • Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.
Eliminazione automatica	<ul style="list-style-type: none"> • Vero: Gli oggetti in questo bucket verranno cancellati automaticamente allo scadere del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale. • Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.

Coerenza per le impostazioni di conformità

Quando aggiorni le impostazioni di compliance per un bucket S3 con una richiesta DI compliance PUT bucket, StorageGRID tenta di aggiornare i metadati del bucket nella griglia. Per impostazione predefinita, StorageGRID utilizza la coerenza **strong-Global** per garantire che tutti i siti dei data center e tutti i nodi di storage che contengono i metadati del bucket abbiano coerenza di lettura dopo scrittura per le impostazioni di conformità modificate.

Se StorageGRID non riesce a raggiungere la coerenza **strong-Global** perché un sito di data center o più nodi di archiviazione in un sito non sono disponibili, il codice di stato HTTP per la risposta è 503 `Service Unavailable`.

Se si riceve questa risposta, è necessario contattare l'amministratore del grid per assicurarsi che i servizi di storage richiesti siano resi disponibili il prima possibile. Se l'amministratore della griglia non è in grado di rendere disponibile una quantità sufficiente di nodi di archiviazione in ogni sito, il supporto tecnico potrebbe richiedere di riprovare la richiesta non riuscita forzando la coerenza **strong-Site**.



Non forzare mai la coerenza **strong-site** per la conformità del bucket PUT a meno che non sia stato richiesto dal supporto tecnico e a meno che non si capiscano le potenziali conseguenze dell'utilizzo di questo livello.

Quando la coerenza viene ridotta a **strong-Site**, StorageGRID garantisce che le impostazioni di conformità aggiornate abbiano coerenza di lettura dopo scrittura solo per le richieste client all'interno di un sito. Ciò significa che il sistema StorageGRID potrebbe disporre temporaneamente di più impostazioni incoerenti per questo bucket fino a quando non saranno disponibili tutti i siti e i nodi di storage. Le impostazioni incoerenti possono causare comportamenti imprevisti e indesiderati. Ad esempio, se si colloca un bucket in una conservazione legale e si forza una minore coerenza, le precedenti impostazioni di conformità del bucket (ovvero, blocco legale) potrebbero continuare a essere attive in alcuni data center. Di conseguenza, gli oggetti che si ritiene siano in stato di conservazione a fini giudiziari potrebbero essere eliminati allo scadere del periodo di conservazione, dall'utente o mediante eliminazione automatica, se attivata.

Per forzare l'uso della coerenza **strong-Site**, rimettere la richiesta di conformità PUT Bucket e includere l'`Consistency-Control` intestazione della richiesta HTTP, come segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Risposte agli errori

- Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è 404 Not Found.
- Se `RetentionPeriodMinutes` nella richiesta è inferiore al periodo di conservazione corrente del bucket, il codice di stato HTTP è 400 Bad Request.

Informazioni correlate

"[Deprecato: APPORTARE modifiche alla richiesta di conformità al bucket](#)"

Gestire le policy di accesso

Utilizzare le policy di accesso

StorageGRID utilizza il linguaggio delle policy di Amazon Web Services (AWS) per consentire ai tenant S3 di controllare l'accesso ai bucket e agli oggetti all'interno di tali bucket. Il sistema StorageGRID implementa un sottoinsieme del linguaggio dei criteri delle API REST S3. I criteri di accesso per l'API S3 sono scritti in JSON.

Panoramica dei criteri di accesso

StorageGRID supporta tre tipi di criteri di accesso:

- **Criteri bucket**, che sono gestiti utilizzando le operazioni API `GetBucketPolicy`, `PutBucketPolicy` e `DeleteBucketPolicy` S3 o l'API `Tenant Manager` o `Tenant Management`. Le policy del bucket sono collegate ai bucket, quindi sono configurate per controllare l'accesso degli utenti nell'account del proprietario del bucket o altri account al bucket e agli oggetti in esso contenuti. Una policy di bucket si applica a un solo bucket ed eventualmente a più gruppi.
- **Criteri di gruppo**, configurati utilizzando l'API di gestione `tenant Manager` o `tenant`. I criteri di gruppo sono associati a un gruppo dell'account, quindi sono configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Una policy di gruppo si applica a un solo gruppo e possibilmente a più bucket.
- **Criteri di sessione**, inclusi come parte della richiesta `AssumeRole`. I criteri di sessione si applicano solo alla sessione specificata, definendo ulteriormente le autorizzazioni di cui dispone l'utente, oltre a quelle concesse dai criteri di gruppo e di bucket.



Non vi è alcuna differenza di priorità tra i criteri di gruppo, bucket e sessione.

Le policy di gruppo e bucket di StorageGRID seguono una grammatica specifica definita da Amazon. All'interno di ogni policy è presente una serie di dichiarazioni di policy, ciascuna delle quali contiene i seguenti elementi:

- ID dichiarazione (Sid) (opzionale)
- Effetto
- Principal/NotPrincipal

- Risorsa/NotResource
- Azione/Notazione
- Condizione (opzionale)

Le istruzioni dei criteri vengono create utilizzando questa struttura per specificare le autorizzazioni: Grant <Effect> per consentire/negare a <Principal> di eseguire <Action> su <Resource> quando viene applicato <Condition>.

Ciascun elemento di policy viene utilizzato per una funzione specifica:

Elemento	Descrizione
SID	L'elemento Sid è opzionale. Il Sid deve essere utilizzato solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID.
Effetto	Utilizzare l'elemento Effect per stabilire se le operazioni specificate sono consentite o rifiutate. È necessario identificare le operazioni consentite (o negate) su bucket o oggetti utilizzando le parole chiave dell'elemento Action supportate.
Principal/NotPrincipal	<p>È possibile consentire a utenti, gruppi e account di accedere a risorse specifiche ed eseguire azioni specifiche. Se nella richiesta non è inclusa alcuna firma S3, l'accesso anonimo è consentito specificando il carattere jolly (*) come principale. Per impostazione predefinita, solo l'account root ha accesso alle risorse di proprietà dell'account.</p> <p>È sufficiente specificare l'elemento Principal in una policy bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito.</p>
Risorsa/NotResource	L'elemento Resource identifica bucket e oggetti. Puoi consentire o negare le autorizzazioni per bucket e oggetti utilizzando il nome risorsa Amazon (ARN) per identificare la risorsa.
Azione/Notazione	Gli elementi Action e Effect sono i due componenti delle autorizzazioni. Quando un gruppo richiede una risorsa, gli viene concesso o negato l'accesso alla risorsa. L'accesso viene negato a meno che non si assegnino specificamente autorizzazioni, ma è possibile utilizzare la funzione di negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio.
Condizione	L'elemento Condition è opzionale. Le condizioni consentono di creare espressioni per determinare quando applicare un criterio.

Nell'elemento Action, è possibile utilizzare il carattere jolly (*) per specificare tutte le operazioni o un sottoinsieme di operazioni. Ad esempio, questa azione corrisponde a permessi come s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

Nell'elemento Resource, è possibile utilizzare i caratteri jolly () e (?). Mentre l'asterisco (*) corrisponde a 0 o più caratteri, il punto interrogativo (?) corrisponde a qualsiasi singolo carattere.

Nell'elemento Principal, i caratteri jolly non sono supportati, ad eccezione dell'impostazione dell'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, impostare il carattere jolly (*) come valore Principal.

```
"Principal": ""
```

```
"Principal": {"AWS": ""}
```

Nell'esempio seguente, l'istruzione utilizza gli elementi Effect, Principal, Action e Resource. In questo esempio viene illustrata un'istruzione completa dei criteri bucket che utilizza l'effetto "Consenti" per assegnare ai Principals, al gruppo admin `federated-group/admin` e al gruppo Finance `federated-group/finance`, le autorizzazioni per eseguire l'azione `s3:ListBucket` sul bucket denominato `mybucket` e l'azione `s3:GetObject` su tutti gli oggetti all'interno di tale bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

Il criterio bucket ha un limite di dimensione di 20,480 byte e il criterio di gruppo ha un limite di dimensione di 5,120 byte.

Coerenza delle policy

Per impostazione predefinita, gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Quando un criterio di gruppo diventa coerente, le modifiche possono richiedere altri 15 minuti, a causa della memorizzazione nella cache dei criteri. Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri bucket sono fortemente coerenti.

Come richiesto, è possibile modificare le garanzie di coerenza per gli aggiornamenti delle policy bucket. Ad esempio, è possibile rendere disponibile una modifica a un criterio bucket in caso di fuori servizio di un sito.

In questo caso, è possibile impostare l'`Consistency-Control`intestazione nella richiesta PutBucketPolicy oppure utilizzare la richiesta di coerenza PUT Bucket. Quando un criterio bucket diventa coerente, le modifiche possono richiedere altri 8 secondi per diventare effettive, a causa del caching delle policy.



Se si imposta la coerenza su un valore diverso per risolvere una situazione temporanea, assicurarsi di riportare l'impostazione del livello del bucket al valore originale al termine dell'operazione. In caso contrario, tutte le richieste bucket future utilizzeranno l'impostazione modificata.

Che cos'è la politica di sessione?

Una policy di sessione è una policy di accesso che limita temporaneamente le autorizzazioni disponibili durante una sessione specifica, ad esempio quando un utente assume l'incarico di un gruppo. Una policy di sessione può consentire solo un sottoinsieme di autorizzazioni e non può concedere autorizzazioni aggiuntive. Il gruppo stesso potrebbe avere permessi più ampi.

Utilizzare ARN nelle dichiarazioni delle policy

Nelle dichiarazioni delle policy, l'ARN viene utilizzato negli elementi Principal e Resource.

- Utilizzare questa sintassi per specificare la risorsa S3 ARN:

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

- Utilizzare questa sintassi per specificare l'ARN della risorsa di identità (utenti e gruppi):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Altre considerazioni:

- È possibile utilizzare l'asterisco (*) come carattere jolly per far corrispondere zero o più caratteri all'interno della chiave oggetto.
- I caratteri internazionali, che possono essere specificati nella chiave oggetto, devono essere codificati utilizzando JSON UTF-8 o le sequenze di escape JSON. La codifica in percentuale non è supportata.

"Sintassi URN RFC 2141"

Il corpo della richiesta HTTP per l'operazione PutBucketPolicy deve essere codificato con charset=UTF-8.

Specificare le risorse in un criterio

Nelle istruzioni policy, è possibile utilizzare l'elemento Resource per specificare il bucket o l'oggetto per cui le autorizzazioni sono consentite o negate.

- Ogni dichiarazione di policy richiede un elemento Resource. In un criterio, le risorse sono indicate dall'elemento Resource, o in alternativa, NotResource per esclusione.
- Specificare le risorse con un ARN di risorsa S3. Ad esempio:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- È inoltre possibile utilizzare le variabili dei criteri all'interno della chiave a oggetti. Ad esempio:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Il valore della risorsa può specificare un bucket che non esiste ancora quando viene creata una policy di gruppo.

Specificare le entità in un criterio

Utilizzare l'elemento Principal per identificare l'account utente, gruppo o tenant a cui è consentito/negato l'accesso alla risorsa dall'istruzione policy.

- Ogni dichiarazione di policy in una policy bucket deve includere un elemento Principal. Le dichiarazioni di policy in una policy di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principale.
- In un criterio, i principal sono indicati dall'elemento "Principal" o in alternativa "NotPrincipal" per l'esclusione.
- Le identità basate sull'account devono essere specificate utilizzando un ID o un ARN:

```
"Principal": { "AWS": "account_id" }  
"Principal": { "AWS": "identity_arn" }
```

- In questo esempio viene utilizzato l'ID account tenant 27233906934684427525, che include l'account root e tutti gli utenti dell'account:

```
"Principal": { "AWS": "27233906934684427525" }
```

- È possibile specificare solo l'account root:


```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- È possibile specificare un utente federato specifico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-user/Alex" }
```

- È possibile specificare uno specifico gruppo federated ("Manager"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-group/Managers" }
```

- È possibile specificare un'entità anonima:

```
"Principal": "*" 
```

- Per evitare ambiguità, è possibile utilizzare l'UUID utente invece del nome utente:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

Ad esempio, supponiamo che Alex abbandoni l'organizzazione e che il nome utente `Alex` venga eliminato. Se un nuovo Alex entra a far parte dell'organizzazione e viene assegnato lo stesso `Alex` nome utente, il nuovo utente potrebbe inavvertitamente ereditare le autorizzazioni concesse all'utente originale.

- Il valore principale può specificare un nome utente/gruppo che non esiste ancora quando viene creata una policy bucket.

Specificare le autorizzazioni in un criterio

In un criterio, l'elemento `Action` viene utilizzato per consentire/negare le autorizzazioni a una risorsa. È possibile specificare una serie di autorizzazioni in un criterio, indicate dall'elemento `"Action"` o, in alternativa, `"NotAction"` per l'esclusione. Ciascuno di questi elementi viene associato a specifiche operazioni REST API S3.

Le tabelle elencano le autorizzazioni applicabili ai bucket e le autorizzazioni applicabili agli oggetti.



Amazon S3 ora utilizza l'autorizzazione `S3:PutReplicationConfiguration` per entrambe le azioni `PutBucketReplication` e `DeleteBucketReplication`. StorageGRID utilizza autorizzazioni separate per ciascuna azione, che corrispondono alla specifica originale di Amazon S3.



Un'eliminazione viene eseguita quando si utilizza un `put` per sovrascrivere un valore esistente.

Autorizzazioni applicabili ai bucket

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:CreateBucket	CreateBucket	Sì. Nota: Utilizzare solo nei criteri di gruppo.
s3:Deletebucket	DeleteBucket	
s3:DeleteBucketMetadataNotification	ELIMINA la configurazione di notifica dei metadati del bucket	Sì
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Sì, separare le autorizzazioni per PUT ed DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	OTTIENI compliance bucket (obsoleta)	Sì
s3:GetBucketConsistency	COERENZA del bucket	Sì
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	OTTIENI l'ultimo tempo di accesso a bucket	Sì
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	OTTIENI la configurazione della notifica dei metadati del bucket	Sì
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBucket	<ul style="list-style-type: none"> ListBucket OTTIENI l'utilizzo dello storage 	<p>Sì, per OTTIENI utilizzo storage.</p> <p>Nota: Utilizzare solo nei criteri di gruppo.</p>
s3:ListBucket	<ul style="list-style-type: none"> ListObjects (oggetti elenco) HeadBucket RestoreObject 	
s3:ListBucketMultipartUploads	<ul style="list-style-type: none"> ListMultipartUploads RestoreObject 	
s3:ListBucketVersions	SCARICA le versioni di bucket	
s3:PutBucketCompliance	METTERE la compliance del bucket (obsoleta)	Sì
s3:PutBucketConsistency	METTI la coerenza del bucket	Sì
s3:PutBucketCORS	<ul style="list-style-type: none"> DeleteBucketCors† PutBucketCors 	
s3:PutEncryptionConfiguration	<ul style="list-style-type: none"> DeleteBucketEncryption PutBucketEncryption 	
s3:PutBucketLastAccessTime	TEMPO ULTIMO accesso bucket	Sì
s3:PutBucketMetadataNotification	INSERIRE la configurazione della notifica dei metadati del bucket	Sì
s3:PutBucketNotification	PutBucketNotificationConfiguration	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> CreateBucket con l' `x-amz-bucket-object-lock-enabled: true` intestazione della richiesta (richiede anche l'autorizzazione S3:CreateBucket) PutObjectLockConfiguration 	
s3:PutBucketPolicy	PutBucketPolicy	
s3:PutBucketTagging	<ul style="list-style-type: none"> DeleteBucketTagging† PutBucketTagging 	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	<ul style="list-style-type: none"> DeleteBucketLifecycle† PutBucketLifecycleConfiguration 	
s3:PutReplicationConfiguration	PutBucketReplication	Sì, separare le autorizzazioni per PUT ed DELETE

Autorizzazioni applicabili agli oggetti

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:AbortMultipartUpload	<ul style="list-style-type: none"> AbortMultipartUpload RestoreObject 	
s3:BypassGovernanceRetention	<ul style="list-style-type: none"> DeleteObject (Elimina oggetto) DeleteObjects PutObjectRetention 	
s3>DeleteObject	<ul style="list-style-type: none"> DeleteObject (Elimina oggetto) DeleteObjects RestoreObject 	
s3>DeleteObjectTagging	DeleteObjectTagging	
s3>DeleteObjectVersionTagging	DeleteObjectTagging (una versione specifica dell'oggetto)	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:DeleteObjectVersion	DeleteObject (una versione specifica dell'oggetto)	
s3:GetObject	<ul style="list-style-type: none"> • GetObject • HeadObject (oggetto intestazione) • RestoreObject • SelectObjectContent 	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GetObject (una versione specifica dell'oggetto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	<ul style="list-style-type: none"> • PutObject • Oggetto CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy 	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (una versione specifica dell'oggetto)	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:PutOverwriteObject	<ul style="list-style-type: none"> • PutObject • Oggetto CopyObject • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload 	Sì
s3:RestoreObject (Riavvia oggetto)	RestoreObject	

Utilizza l'autorizzazione PutOverwriteObject

l'autorizzazione s3:PutOverwriteObject è un'autorizzazione StorageGRID personalizzata che si applica alle operazioni che creano o aggiornano oggetti. L'impostazione di questa autorizzazione determina se il client può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o il tagging degli oggetti S3.

Le impostazioni possibili per questa autorizzazione includono:

- **Allow:** Il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega:** Il client non può sovrascrivere un oggetto. Se impostata su Nega, l'autorizzazione PutOverwriteObject funziona come segue:
 - Se un oggetto esistente viene trovato nello stesso percorso:
 - I dati dell'oggetto, i metadati definiti dall'utente o il tag S3 non possono essere sovrascritti.
 - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
 - Se è attivata la versione S3, l'impostazione Nega impedisce alle operazioni PutObjectTagging o DeleteObjectTagging di modificare il TagSet per un oggetto e le relative versioni non correnti.
 - Se non viene trovato un oggetto esistente, questa autorizzazione non ha effetto.
- Quando questa autorizzazione non è presente, l'effetto è lo stesso di se Allow è stato impostato.



Se l'attuale policy S3 consente la sovrascrittura e l'autorizzazione PutOverwriteObject è impostata su Nega, il client non può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o i tag degli oggetti. Inoltre, se è selezionata la casella di controllo **Impedisci modifica client (Configurazione > Impostazioni di sicurezza > Rete e oggetti)**, tale impostazione sovrascrive l'impostazione dell'autorizzazione PutOverwriteObject.

Specificare le condizioni in un criterio

Le condizioni definiscono quando una policy sarà in vigore. Le condizioni sono costituite da operatori e coppie chiave-valore.

Le condizioni utilizzano coppie chiave-valore per la valutazione. Un elemento Condition può contenere più condizioni e ciascuna condizione può contenere più coppie chiave-valore. Il blocco Condition utilizza il seguente formato:

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

Nell'esempio seguente, la condizione ipaddress utilizza la chiave SourceIp Condition.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

Operatori delle condizioni supportati

Gli operatori delle condizioni sono classificati come segue:

- Stringa
- Numerico
- Booleano
- Indirizzo IP
- Controllo nullo

Condizionare gli operatori	Descrizione
StringEquals	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole).
StringNotEquals	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole).
StringEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora maiuscole/minuscole).
StringNotEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora maiuscole/minuscole).
StringLike	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole). Può includere caratteri jolly * e ?.
StringNotLike	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole). Può includere caratteri jolly * e ?.

Condizionare gli operatori	Descrizione
Valori numerici Equals	Confronta una chiave con un valore numerico in base alla corrispondenza esatta.
NumericNotEquals	Confronta una chiave con un valore numerico in base alla corrispondenza negata.
NumericGreaterThan	Confronta un tasto con un valore numerico basato sulla corrispondenza "maggiore di".
NumericGreaterThanEquals	Confronta una chiave con un valore numerico basato sulla corrispondenza "maggiore o uguale".
NumericLessThan	Confronta una chiave con un valore numerico basato sulla corrispondenza "minore di".
NumericLessThanEquals	Confronta una chiave con un valore numerico basato sulla corrispondenza "minore di o uguale".
Bool	Confronta una chiave con un valore booleano basato sulla corrispondenza "true o false".
Indirizzo IP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP.
NotIpAddress	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata.
Null	Controlla se è presente una chiave di condizione nel contesto della richiesta corrente.
Se esiste	Aggiunto a qualsiasi operatore di condizione, eccetto la condizione Null, per verificare l'assenza di quella chiave di condizione. Restituisce TRUE se la chiave di condizione non è presente.

Chiavi di condizione supportate

Tasti Condition	Azioni	Descrizione
aws: SourceIp	Operatori IP	<p>Viene confrontato con l'indirizzo IP da cui è stata inviata la richiesta. Può essere utilizzato per operazioni bucket o a oggetti.</p> <p>Nota: se la richiesta S3 è stata inviata tramite il servizio Load Balancer sui nodi Admin e Gateway, viene confrontato con l'indirizzo IP a monte del servizio Load Balancer.</p> <p>Nota: Se si utilizza un bilanciamento del carico non trasparente di terze parti, questo viene confrontato con l'indirizzo IP del bilanciamento del carico. Qualsiasi X-Forwarded-For intestazione verrà ignorata perché la sua validità non può essere accertata.</p>
aws:nome utente	Risorsa/identità	Viene confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni bucket o a oggetti.
s3:delimitatore	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Verrà eseguito un confronto con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions.
S3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl s3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging S3:PutObjectAcl s3:PutObjectTagging S3:PutObjectVersionAcl s3:PutObjectVersionTagging	Richiede che l'oggetto esistente abbia la chiave e il valore tag specifici.

Tasti Condition	Azioni	Descrizione
s3: tasti max	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Verrà eseguito un confronto con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions.
s3:modalità-blocco-oggetto	s3:PutObject	Confronta con il object-lock-mode espanso dall'intestazione della richiesta nelle richieste PutObject, CopyObject e CreateMultipartUpload.
s3:modalità-blocco-oggetto	s3:PutObjectRetention	Confronta con il object-lock-mode espanso dal corpo XML nella richiesta PutObjectRetention.
s3:giorni-rimanenti-conservazione-blocco-oggetto	s3:PutObject	Viene confrontato con la data di scadenza specificata nell' `x-amz-object-lock-retain-until-date` intestazione della richiesta o calcolata dal periodo di conservazione predefinito del bucket per assicurarsi che questi valori rientrino nell'intervallo consentito per le seguenti richieste: <ul style="list-style-type: none"> • PutObject • Oggetto CopyObject • CreateMultipartUpload
s3:giorni-rimanenti-conservazione-blocco-oggetto	s3:PutObjectRetention	Viene confrontato con la data di scadenza specificata nella richiesta PutObjectRetention per garantire che rientri nell'intervallo consentito.
s3:prefisso	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Verrà eseguito un confronto con il parametro prefix specificato in una richiesta ListObjects o ListObjectVersions.
S3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Richiede una chiave e un valore tag specifici quando la richiesta dell'oggetto include il tagging.
algoritmo-cliente-di-crittografia-lato-server-s3:x-amz	s3:PutObject	Confronta con il sse-customer-algorithm o al copy-source-sse-customer-algorithm espanso dall'intestazione della richiesta nelle richieste PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy e CompleteMultipartUpload.

Specificare le variabili in un criterio

È possibile utilizzare le variabili nei criteri per popolare le informazioni sui criteri quando sono disponibili. È possibile utilizzare le variabili dei criteri nell' `Resource` elemento e nei confronti delle stringhe nell' `Condition` elemento.

In questo esempio, la variabile `${aws:username}` fa parte dell'elemento Resource:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In questo esempio, la variabile `${aws:username}` fa parte del valore di condizione nel blocco di condizione:

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variabile	Descrizione
<code>\${aws:SourceIp}</code>	Utilizza la chiave SourceIp come variabile fornita.
<code>\${aws:username}</code>	Utilizza la chiave Username come variabile fornita.
<code>\${s3:prefix}</code>	Utilizza la chiave di prefisso specifica del servizio come variabile fornita.
<code>\${s3:max-keys}</code>	Utilizza la chiave max-keys specifica del servizio come variabile fornita.
<code>\${*}</code>	Carattere speciale. Utilizza il carattere come carattere * letterale.
<code>\${?}</code>	Carattere speciale. Utilizza il carattere come carattere letterale ?.
<code>\${\$}</code>	Carattere speciale. Utilizza il carattere come carattere letterale.

Creare policy che richiedono una gestione speciale

A volte un criterio può concedere autorizzazioni pericolose per la sicurezza o pericolose per operazioni continue, come il blocco dell'utente root dell'account. L'implementazione dell'API REST di StorageGRID S3 è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Negare automaticamente le autorizzazioni all'account root	Bucket	Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3	Stesso
Negare automaticamente le autorizzazioni all'utente/gruppo	Gruppo	Valido e applicato	Stesso
Consenti a un gruppo di account esterno qualsiasi autorizzazione	Bucket	Principal non valido	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio
Consentire a un account root esterno o a un utente qualsiasi autorizzazione	Bucket	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio	Stesso
Consenti a tutti i permessi per tutte le azioni	Bucket	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) per l'account root esterno e gli utenti	Stesso
Negare a Everyone le autorizzazioni per tutte le azioni	Bucket	Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3	Stesso
Principal è un utente o un gruppo inesistente	Bucket	Principal non valido	Valido
La risorsa è un bucket S3 inesistente	Gruppo	Valido	Stesso
Principal è un gruppo locale	Bucket	Principal non valido	Valido

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Il criterio concede a un account non proprietario (inclusi gli account anonimi) le autorizzazioni per l'inserimento degli oggetti.	Bucket	Valido. Gli oggetti sono di proprietà dell'account creatore e la policy bucket non si applica. L'account creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL a oggetti.	Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la policy bucket.

Protezione WORM (Write-Once-Read-Many)

È possibile creare bucket WORM (write-once-Read-many) per proteggere i dati, i metadati degli oggetti definiti dall'utente e il tagging degli oggetti S3. I bucket WORM vengono configurati in modo da consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione del contenuto esistente. Utilizzare uno degli approcci descritti di seguito.

Per garantire che le sovrascritture vengano sempre negate, è possibile:

- Da Grid Manager, vai su **Configurazione > Sicurezza > Impostazioni di sicurezza > Rete e oggetti** e seleziona la casella di controllo **Impedisci modifiche client**.
- Applicare le seguenti regole e criteri S3:
 - Aggiungere un'operazione di NEGAZIONE PutOverwriteObject al criterio S3.
 - Aggiungere un'operazione di NEGAZIONE DeleteObject al criterio S3.
 - Aggiungere un'operazione PutObject ALLOW al criterio S3.



L'impostazione di DeleteObject su NEGA in un criterio S3 non impedisce a ILM di eliminare oggetti quando esiste una regola come "zero copie dopo 30 giorni".



Anche quando tutte queste regole e policy vengono applicate, non si proteggono dalle scritture simultanee (vedi situazione A). Si proteggono dalle sovrascritture sequenziali completate (vedere situazione B).

Situazione A: Scritture simultanee (non protette)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

Situazione B: Sovrascritture sequenziali completate (con protezione)

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

Informazioni correlate

- ["Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID"](#)
- ["Esempio di policy bucket"](#)
- ["Criteri di gruppo di esempio"](#)
- ["Esempio di policy di sessione"](#)
- ["Gestire gli oggetti con ILM"](#)
- ["Utilizzare un account tenant"](#)

Esempio di policy di sessione

Utilizzare l'esempio seguente per creare una policy di sessione StorageGRID .

Esempio: impostare una policy di sessione che consenta il recupero degli oggetti

In questo esempio, al principale della sessione è consentito recuperare oggetti solo dal bucket1. Tutte le altre azioni vengono implicitamente negate, ad eccezione delle azioni specifiche StorageGRID, come l'utilizzo di ["s3:PutOverwriteObject"](#) permesso. La policy di sessione può essere fornita come file JSON durante la chiamata all'API AssumeRole.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

Esempio di policy bucket

Utilizza gli esempi di questa sezione per creare policy di accesso StorageGRID per i bucket.

I criteri del bucket specificano le autorizzazioni di accesso per il bucket a cui è associata la policy. È possibile configurare un criterio bucket utilizzando l'API S3 PutBucketPolicy tramite uno dei seguenti strumenti:

- ["Manager tenant"](#).
- AWS CLI utilizzando il seguente comando (vedere la ["Operazioni sui bucket"](#)):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Esempio: Consentire a tutti l'accesso in sola lettura a un bucket

In questo esempio, a tutti, incluso anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni

GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni verranno negate. Si noti che questo criterio potrebbe non essere particolarmente utile perché nessuno, ad eccezione dell'account root, dispone delle autorizzazioni di scrittura nel bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}
```

Esempio: Consentire a tutti gli utenti di un account l'accesso completo e a tutti gli utenti di un altro account l'accesso in sola lettura a un bucket

In questo esempio, a tutti gli utenti di un account specificato è consentito l'accesso completo a un bucket, mentre a tutti gli utenti di un altro account specificato è consentito solo elencare il bucket ed eseguire operazioni GetObject sugli oggetti nel bucket che iniziano con il `shared/` prefisso della chiave dell'oggetto.



In StorageGRID, gli oggetti creati da un account non proprietario (inclusi gli account anonimi) sono di proprietà dell'account proprietario del bucket. La policy bucket si applica a questi oggetti.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

Esempio: Consentire a tutti l'accesso in sola lettura a un bucket e l'accesso completo per gruppo specifico

In questo esempio, a tutti gli utenti, incluso anonimo, è consentito elencare il bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket, mentre solo gli utenti appartenenti al gruppo Marketing nell'account specificato possono accedere completamente.


```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Esempio: Consentire a tutti l'accesso in lettura e scrittura a un bucket se il client si trova nell'intervallo IP

In questo esempio, Everyone, incluso l'anonimato, è autorizzato a elencare il bucket ed eseguire qualsiasi operazione oggetto su tutti gli oggetti nel bucket, a condizione che le richieste provengano da un intervallo IP specificato (da 54.240.143.0 a 54.240.143.255, eccetto 54.240.143.188). Tutte le altre operazioni verranno rifiutate e tutte le richieste al di fuori dell'intervallo IP verranno rifiutate.

```

{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "IpAddress": { "aws:SourceIp": "54.240.143.0/24" },
        "NotIpAddress": { "aws:SourceIp": "54.240.143.188" }
      }
    }
  ]
}

```

Esempio: Consentire l'accesso completo a un bucket esclusivamente da un utente federato specificato

In questo esempio, all'utente federato Alex è consentito l'accesso completo al `examplebucket` bucket e ai relativi oggetti. A tutti gli altri utenti, tra cui 'root', vengono esplicitamente negate tutte le operazioni. Si noti tuttavia che a 'root' non vengono mai negate le autorizzazioni per `put/get/DeleteBucketPolicy`.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Esempio: Autorizzazione PutOverwriteObject

In questo esempio, l'`Deny` effetto di PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e l'etichettatura degli oggetti S3.

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

Criteri di gruppo di esempio

Utilizzare gli esempi di questa sezione per creare criteri di accesso StorageGRID per i gruppi.

I criteri di gruppo specificano le autorizzazioni di accesso per il gruppo a cui è associato il criterio. Non vi è alcun Principal elemento nella politica perché è implicita. I criteri di gruppo vengono configurati utilizzando il tenant Manager o l'API.

Esempio: Impostare i criteri di gruppo utilizzando Tenant Manager

Quando si aggiunge o si modifica un gruppo in Tenant Manager, è possibile selezionare una policy di gruppo per determinare quali autorizzazioni di accesso S3 avranno i membri di questo gruppo. Vedere ["Creare gruppi per un tenant S3"](#).

- **Nessun accesso S3:** Opzione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
- **Accesso di sola lettura:** Gli utenti di questo gruppo hanno accesso di sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
- **Accesso completo:** Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
- **Ransomware Mitigation:** Questa policy di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti.

Gli utenti di tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.

- **Personalizzato:** Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

Esempio: Consentire l'accesso completo del gruppo a tutti i bucket

In questo esempio, a tutti i membri del gruppo è consentito l'accesso completo a tutti i bucket di proprietà dell'account tenant, a meno che non sia esplicitamente negato dalla policy bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Esempio: Consentire l'accesso di gruppo in sola lettura a tutti i bucket

In questo esempio, tutti i membri del gruppo hanno accesso in sola lettura alle risorse S3, a meno che non sia esplicitamente negato dalla policy del bucket. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag.

```

{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}

```

Esempio: Consenti ai membri del gruppo di accedere completamente solo alla loro "cartella" in un bucket

In questo esempio, i membri del gruppo possono solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Tenere presente che le autorizzazioni di accesso da altre policy di gruppo e la policy del bucket devono essere prese in considerazione quando si determina la privacy di queste cartelle.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Operazioni S3 registrate nei registri di audit

I messaggi di audit vengono generati dai servizi StorageGRID e memorizzati in file di log di testo. È possibile rivedere i messaggi di audit specifici per S3 nel registro di audit per ottenere dettagli sulle operazioni di bucket e oggetti.

Operazioni bucket registrate nei registri di audit

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- HeadBucket
- ListObjects (oggetti elenco)
- ListObjectVersions
- METTI la compliance del bucket
- PutBucketTagging
- PutBucketVersioning

Operazioni a oggetti registrate nei registri di audit

- CompleteMultipartUpload
- Oggetto CopyObject
- DeleteObject (Elimina oggetto)
- GetObject
- HeadObject (oggetto intestazione)
- PutObject
- RestoreObject
- SelectObject (oggetto)
- UploadPart (quando una regola ILM utilizza un'acquisizione bilanciata o rigorosa)
- UploadPartCopy (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)

Informazioni correlate

- ["Accedere al file di log di audit"](#)
- ["Messaggi di audit di scrittura del client"](#)
- ["Messaggi di audit in lettura del client"](#)

Utilizza Swift REST API (fine del ciclo di vita)

Utilizzare l'API REST di Swift

Il supporto per l'API Swift è terminato e verrà rimosso in una versione futura.



I dettagli Swift sono stati rimossi da questa versione del sito della documentazione. Vedere ["StorageGRID 11,8: Utilizza l'API REST Swift"](#).

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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