



## **USA StorageGRID**

### StorageGRID

NetApp

October 03, 2025

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-115/tenant/web-browser-requirements.html> on October 03, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Sommario

USA StorageGRID .....	1
Utilizzare un account tenant .....	1
Utilizzo di Tenant Manager .....	1
Gestione dell'accesso al sistema per gli utenti tenant .....	15
Gestione degli account tenant S3 .....	37
Gestione dei servizi della piattaforma S3 .....	66
Utilizzare S3 .....	108
Supporto per l'API REST S3 .....	108
Configurazione di account e connessioni tenant .....	112
Come StorageGRID implementa l'API REST S3 .....	118
Operazioni e limitazioni supportate dall'API REST S3 .....	125
Operazioni REST API di StorageGRID S3 .....	177
Policy di accesso a bucket e gruppi .....	200
Configurazione della sicurezza per l'API REST .....	226
Operazioni di monitoraggio e controllo .....	229
Vantaggi delle connessioni HTTP attive, inattive e simultanee .....	232
USA Swift .....	235
Supporto API di OpenStack Swift in StorageGRID .....	235
Configurazione di account e connessioni tenant .....	238
Operazioni supportate da Swift REST API .....	243
Operazioni API Swift REST di StorageGRID .....	256
Configurazione della sicurezza per l'API REST .....	260
Operazioni di monitoraggio e controllo .....	263

# USA StorageGRID

## Utilizzare un account tenant

Scopri come utilizzare un account tenant StorageGRID.

- ["Utilizzo di Tenant Manager"](#)
- ["Gestione dell'accesso al sistema per gli utenti tenant"](#)
- ["Gestione degli account tenant S3"](#)
- ["Gestione dei servizi della piattaforma S3"](#)

### Utilizzo di Tenant Manager

Il tenant manager consente di gestire tutti gli aspetti di un account tenant StorageGRID.

È possibile utilizzare Tenant Manager per monitorare l'utilizzo dello storage di un account tenant e per gestire gli utenti con la federazione delle identità o creando gruppi e utenti locali. Per gli account tenant S3, è anche possibile gestire le chiavi S3, gestire i bucket S3 e configurare i servizi della piattaforma.

### Utilizzando un account tenant StorageGRID

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

Ogni account tenant dispone di gruppi federati o locali, utenti, bucket S3 o container Swift e oggetti.

Facoltativamente, 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 anche possibile utilizzare i bucket S3 e le policy bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario creare account tenant separati. Vedere le istruzioni per l'implementazione delle applicazioni client S3.

- **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.

### Creazione di account tenant

Gli account tenant vengono creati da un amministratore di grid StorageGRID utilizzando il gestore di grid. Quando si crea un account tenant, l'amministratore della griglia specifica le seguenti informazioni:

- Nome visualizzato per il tenant (l'ID account del tenant viene assegnato automaticamente e non può essere modificato).

- Se l'account tenant utilizzerà S3 o Swift.
- Per gli account tenant S3: Se l'account tenant è autorizzato a utilizzare i servizi della piattaforma. Se è consentito l'utilizzo dei servizi della piattaforma, la griglia deve essere configurata per supportarne l'utilizzo.
- Facoltativamente, una quota di storage per l'account tenant, ovvero il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant. La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).
- Se la federazione delle identità è attivata per il sistema StorageGRID, il gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant.
- Se l'SSO (Single Sign-on) non è in uso per il sistema StorageGRID, se l'account tenant utilizzerà la propria origine di identità o condividerà l'origine di identità della griglia e la password iniziale per l'utente root locale del tenant.

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.

### Configurazione dei tenant S3

Una volta creato un account tenant S3, è possibile accedere a tenant Manager per eseguire le seguenti attività:

- Impostazione della federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) o creazione di gruppi e utenti locali
- Gestione delle chiavi di accesso S3
- Creazione e gestione di bucket S3, inclusi bucket conformi
- Utilizzo dei servizi della piattaforma (se abilitati)
- Monitoraggio dell'utilizzo dello storage



Sebbene sia possibile creare e gestire i bucket S3 con Tenant Manager, è necessario disporre di chiavi di accesso S3 e utilizzare l'API REST S3 per acquisire e gestire gli oggetti.

### Configurazione dei tenant Swift

Una volta creato un account tenant Swift, gli utenti con l'autorizzazione Root Access possono accedere a Tenant Manager per eseguire attività come le seguenti:

- Impostazione della federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) e creazione di gruppi e utenti locali
- Monitoraggio dell'utilizzo dello storage



Gli utenti Swift devono disporre dell'autorizzazione Root Access per accedere a Tenant Manager. Tuttavia, l'autorizzazione Root Access non consente agli utenti di autenticarsi nell'API SWIFT REST per creare container e acquisire oggetti. Gli utenti devono disporre dell'autorizzazione di amministratore Swift per autenticarsi nell'API DI Swift REST.

### Informazioni correlate

["Amministrare StorageGRID"](#)

["Utilizzare S3"](#)

## Requisiti del browser Web

È necessario utilizzare un browser Web supportato.

Browser Web	Versione minima supportata
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Impostare la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024
Ottimale	1280

## Accesso al tenant manager

Per accedere a Tenant Manager, immettere l'URL del tenant nella barra degli indirizzi di un browser Web supportato.

### Di cosa hai bisogno

- È necessario disporre delle credenziali di accesso.
- Per accedere a tenant Manager, è necessario disporre di un URL 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 contiene sempre il nome di dominio completo (FQDN) o l'indirizzo IP utilizzato per accedere a un nodo di amministrazione e può includere facoltativamente anche un numero di porta, l'ID dell'account tenant a 20 cifre o entrambi.

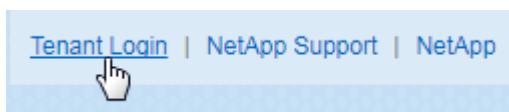
- Se l'URL non include l'ID account a 20 cifre del tenant, è necessario disporre di questo ID account.
- È necessario utilizzare un browser Web supportato.
- I cookie devono essere attivati nel browser Web.
- È necessario disporre di autorizzazioni di accesso specifiche.

## 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 visualizzata dipende dall'URL immesso e dall'utilizzo di SSO (Single Sign-on) da parte dell'organizzazione. Viene visualizzata una delle seguenti schermate:

- Pagina di accesso a Grid Manager. Fare clic sul collegamento **accesso tenant** in alto a destra.



- La pagina di accesso del tenant manager. Il campo **ID account** potrebbe essere già completato, come mostrato di seguito.

 A screenshot of the 'StorageGRID® Tenant Manager' login page. The page has a light blue header with the title. On the left, there is a large NetApp logo. The main area contains three input fields: 'Account ID' with the value '39105156032765926037', 'Username' (empty), and 'Password' (empty). Below these fields is a 'Sign in' button.

- 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. Fare clic su **Accedi**.

Viene visualizzata la dashboard di Tenant Manager.

- La pagina SSO dell'organizzazione, se SSO è attivato nella griglia. Ad esempio:

Sign in with your organizational account

someone@example.com

Password

Sign in

Immettere le credenziali SSO standard e fare clic su **Sign in** (Accedi).

- La pagina di accesso SSO di Tenant Manager.

StorageGRID® Sign in

Recent S3 tenant

Account ID 27469746059057031822

For Grid Manager, leave this field blank.

Sign in

- 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.
- Fare clic su **Accedi**.
- Accedi con le credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Viene visualizzata la dashboard di Tenant Manager.

- Se hai ricevuto una password iniziale da qualcun altro, modifica la password per proteggere il tuo account. Selezionare **Username > Change Password**.



Se SSO è attivato per il sistema StorageGRID, non è possibile modificare la password da Gestore tenant.

#### Informazioni correlate

["Amministrare StorageGRID"](#)

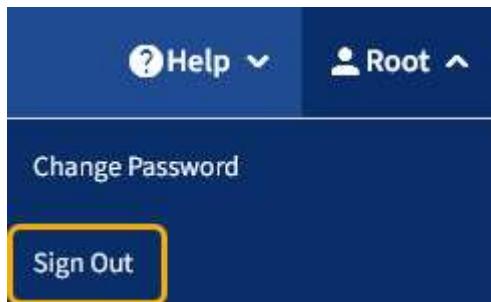
["Requisiti del browser Web"](#)

## Disconnessione dal tenant manager

Una volta terminata la collaborazione con il tenant manager, è necessario disconnettersi 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**.

Opzione	Descrizione
SSO non in uso	Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso del tenant manager.  <b>Nota:</b> se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.
SSO 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 <b>account recenti</b> e viene visualizzato l'ID account* del tenant.  <b>Nota:</b> se SSO è attivato e si è anche connessi a Grid Manager, è necessario disconnettersi da Grid Manager per disconnettersi da SSO.

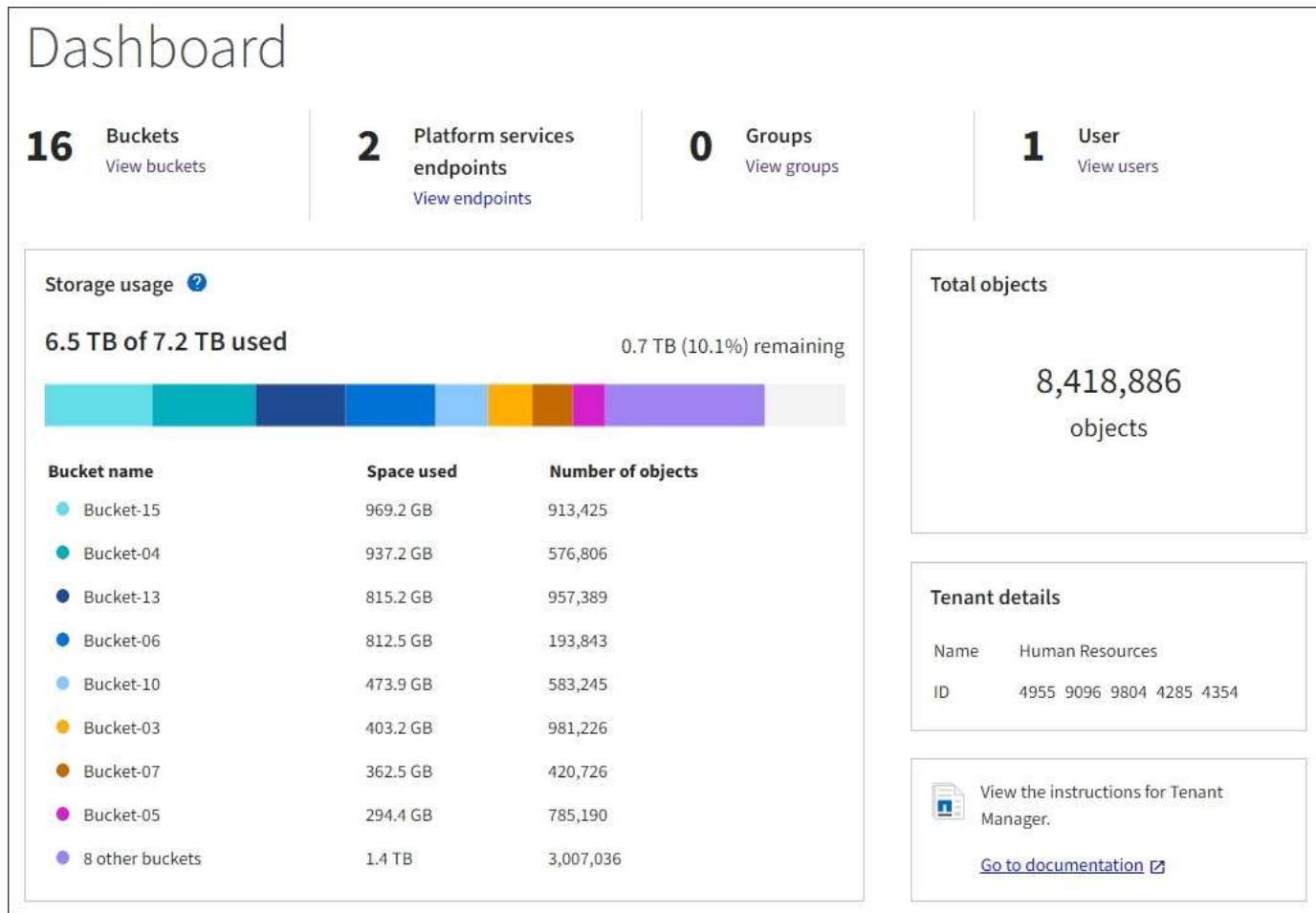
## Informazioni sulla dashboard di Tenant Manager

La dashboard di Tenant Manager offre una panoramica della configurazione di un account tenant e della quantità di spazio utilizzato dagli oggetti nei bucket (S3) o nei container (Swift) del tenant. Se il tenant dispone di una quota, la dashboard mostra la quantità di quota utilizzata e la quantità rimanente. In caso di errori relativi all'account tenant, gli errori vengono visualizzati nella dashboard.



I valori di spazio utilizzato sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi.

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



### Riepilogo account tenant

La parte superiore della dashboard contiene le seguenti informazioni:

- Il numero di bucket o container configurati, gruppi e utenti
- Il numero di endpoint dei servizi della piattaforma, se configurati

È possibile selezionare i collegamenti per visualizzare i dettagli.

Il lato destro della dashboard contiene le seguenti informazioni:

- Il numero totale di oggetti per il tenant.

Per un account S3, se non è stato acquisito alcun oggetto e si dispone dell'autorizzazione Root Access, vengono visualizzate le linee guida per iniziare invece del numero totale di oggetti.

- Il nome e l'ID dell'account tenant.
- Un link alla documentazione di StorageGRID.

### 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 di 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.

## Avvisi sull'utilizzo delle quote

Se gli avvisi sull'utilizzo delle quote sono stati attivati in Grid Manager, 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**. Per ulteriori informazioni, consultare il riferimento agli avvisi nelle istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.



Only 0.6% of the quota is remaining. If the quota is exceeded, you can no longer upload new objects.

Se si supera la quota, non è possibile caricare nuovi oggetti.



The quota has been met. You cannot upload new objects.



Per visualizzare ulteriori dettagli e gestire regole e notifiche per gli avvisi, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

## Errori degli endpoint

Se hai utilizzato Grid Manager per configurare uno o più endpoint da utilizzare con i servizi della piattaforma, il 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 visualizzare i dettagli relativi a un errore di endpoint, selezionare gli endpoint per visualizzare la pagina degli endpoint.

## Informazioni correlate

["Risoluzione dei problemi relativi agli errori degli endpoint dei servizi della piattaforma"](#)

["Monitor risoluzione dei problemi"](#)

## Informazioni sull'API di gestione del 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 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.

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

## Fasi

1. Accedi al tenant manager.
2. Selezionare **Help > API Documentation** dall'intestazione di Tenant Manager.

## 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 eseguire l'autenticazione della sessione utente.

L'API di gestione tenant supporta lo schema di autenticazione del token del bearer. Per l'accesso del tenant, immettere 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 su come migliorare la sicurezza dell'autenticazione, consultare "Protecting Against Cross-Site Request Forgery".



Se per il sistema StorageGRID è attivato il Single Sign-on (SSO), è necessario eseguire diversi passaggi per l'autenticazione. Consultare "Authenticating in to the API if single sign-on is enabled" nelle istruzioni per l'amministrazione di StorageGRID.

- **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.
- **Containers** — operazioni su bucket S3 o container Swift, come segue:

Protocollo	Permesso consentito
S3	<ul style="list-style-type: none"> <li>• Creazione di bucket conformi e non conformi</li> <li>• Modifica delle impostazioni di compliance legacy</li> <li>• Impostazione del controllo di coerenza per le operazioni eseguite sugli oggetti</li> <li>• Creazione, aggiornamento ed eliminazione della configurazione CORS di un bucket</li> <li>• Attivazione e disattivazione degli ultimi aggiornamenti dell'orario di accesso per gli oggetti</li> <li>• Gestione delle impostazioni di configurazione per i servizi della piattaforma, tra cui replica CloudMirror, notifiche e integrazione della ricerca (notifica dei metadati)</li> <li>• Eliminazione di bucket vuoti</li> </ul>
Rapido	Impostazione del livello di coerenza utilizzato per i container

- **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.

- **Groups** — operazioni per gestire gruppi di tenant locali e recuperare gruppi di 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.
- **Regions** — 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 per determinare la modalità di configurazione del blocco oggetti S3 globale (compliance) per il sistema StorageGRID.
- **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	filter by group type
string (query)	
limit	maximum number of results
integer (query)	
marker	marker-style pagination offset (value is Group's URN)
string (query)	
includeMarker	if set, the marker element is also returned
boolean (query)	
order	pagination order (desc requires marker)
string (query)	

### Responses

Response content type

application/json

#### Code Description

200

Example Value Model

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

## Invio di richieste API



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

## Fasi

1. Fare clic sull'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, fare clic su **Model** per conoscere i requisiti di ciascun campo.

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

#### Informazioni correlate

["Protezione contro la contraffazione delle richieste \(CSRF\)"](#)

["Amministrare StorageGRID"](#)

#### 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 3 dell'API.

```
https://hostname_or_ip_address/api/v3/authorize
```

La versione principale dell'API di gestione tenant viene bloccata quando vengono apportate modifiche **non compatibili** con le versioni precedenti. La versione minore dell'API di gestione tenant viene ridotta 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 il software StorageGRID viene installato per la prima volta, viene attivata solo la versione più recente dell'API di gestione del tenant. Tuttavia, quando StorageGRID viene aggiornato a una nuova release di funzionalità, si continua ad avere accesso alla versione API precedente per almeno una release di funzionalità StorageGRID.

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

#### Determinazione delle versioni API supportate nella release corrente

Utilizzare la seguente richiesta API per restituire un elenco delle versioni principali dell'API supportate:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

## Specificare una versione API per una richiesta

È possibile specificare la versione dell'API utilizzando un parametro path (/api/v3) o un'intestazione (Api-Version: 3). Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v3/grid/accounts
curl -H "Api-Version: 3" 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 csrfToken parametro a `true` durante l'autenticazione. L'impostazione predefinita è `false`.

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

Quando è vero, un `GridCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a Grid Manager e a. `AccountCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a 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:

- Il `x-Csrf-Token` Header, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo con codifica a modulo: A. `csrfToken` parametro del corpo della richiesta codificato dal modulo.

Per ulteriori esempi e dettagli, consultare la documentazione API online.



Anche le richieste che dispongono di un set di cookie token CSRF applicheranno "Content-Type: application/json" Intestazione per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

## Gestione dell'accesso al sistema per gli utenti tenant

Gli utenti possono accedere a un account tenant importando i gruppi da un'origine di identità federata e assegnando le autorizzazioni di gestione. È inoltre possibile creare utenti e gruppi di tenant locali, a meno che non sia attivo il Single Sign-on (SSO) per l'intero sistema StorageGRID.

- "[Utilizzo della federazione delle identità](#)"
- "[Gestione dei gruppi](#)"
- "[Gestione degli utenti locali](#)"

### Utilizzo della 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.

- "[Configurazione di un'origine di identità federata](#)"
- "[Forzare la sincronizzazione con l'origine dell'identità](#)"
- "[Disattivazione della federazione delle identità](#)"

#### Configurazione di un'origine di identità federata

È possibile configurare la federazione delle identità se si desidera che gruppi e utenti tenant vengano gestiti in un altro sistema, ad esempio Active Directory, OpenLDAP o Oracle Directory Server.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

- È necessario utilizzare Active Directory, OpenLDAP o Oracle Directory Server come provider di identità. Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare il supporto tecnico.
- 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.

## 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.

## Fasi

1. Selezionare **ACCESS MANAGEMENT > Identity Federation**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione LDAP service type (tipo di servizio LDAP), selezionare **Active Directory, OpenLDAP o Other**.

Se si seleziona **OpenLDAP**, configurare il server OpenLDAP. Consultare le linee guida per la configurazione di un server OpenLDAP.

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.
  - **User Unique Name** (Nome univoco utente): Il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a. `sAMAccountName` Per Active Directory e. `uid` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
  - **UUID utente**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a. `objectGUID` Per Active Directory e. `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Ogni valore dell'utente per l'attributo specificato deve essere un numero esadecimale a 32 cifre in formato a 16 byte o stringa, dove i trattini vengono ignorati.
  - **Group unique name** (Nome univoco gruppo): Il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a. `sAMAccountName` Per Active Directory e. `cn` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
  - **UUID gruppo**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a. `objectGUID` Per Active Directory e. `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale a 32 cifre nel formato a 16 byte o stringa, dove i trattini vengono ignorati.
5. Nella sezione Configure LDAP server (Configura server LDAP), immettere le informazioni richieste per il server LDAP e la connessione di rete.
  - **Nome host**: Nome host del server o 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 oppure uid
- objectGUID, entryUUID, o. nsuniqueid
- cn
- memberOf oppure isMemberOf

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

- **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:** Il 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.

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

- **Utilizzare STARTTLS (consigliato):** Utilizzare STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l’opzione consigliata.
- **Usa LDAPS:** L’opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. Questa opzione è supportata per motivi di compatibilità.
- **Non utilizzare TLS:** Il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto.

Questa opzione non è supportata se il server Active Directory applica 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:** Utilizzare il certificato CA 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.

## 8. Selezionare **Test di connessione** per convalidare le impostazioni di connessione per il server LDAP.

Se la connessione è valida, nell’angolo superiore destro della pagina viene visualizzato un messaggio di conferma.

## 9. Se la connessione è valida, selezionare **Salva**.

La seguente schermata mostra valori di configurazione di esempio per un server LDAP che utilizza Active Directory.

## LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	OpenLDAP	Other
------------------	----------	-------

### Configure LDAP server (All fields are required)

Hostname

Port

Username

Password

Group Base DN

User Base DN

#### Informazioni correlate

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

["Linee guida per la configurazione di un server OpenLDAP"](#)

#### Linee guida per la configurazione di un server OpenLDAP

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

## MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo nella Guida per l'amministratore di OpenLDAP.

## 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.

Consultare le informazioni sulla manutenzione inversa dell'appartenenza al gruppo nella Guida per l'amministratore di OpenLDAP.

## 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.

### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- L'origine dell'identità salvata deve essere abilitata.

### Fasi

#### 1. Selezionare **ACCESS MANAGEMENT > Identity Federation**.

Viene visualizzata la pagina Identity Federation (federazione identità). Il pulsante **Sync server** si trova nella parte superiore destra della pagina.



Se l'origine dell'identità salvata non è abilitata, il pulsante **Sync server** non sarà attivo.

#### 2. Selezionare **Server di sincronizzazione**.

Viene visualizzato un messaggio di conferma che indica che la sincronizzazione è stata avviata correttamente.

## Informazioni correlate

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

## Disattivazione della federazione delle identità

Se è stato configurato un servizio di federazione delle identità per questo tenant, è possibile disattivare temporaneamente o permanentemente la federazione delle identità per gruppi e utenti tenant. Quando la federazione delle identità è disattivata, non vi è alcuna comunicazione tra il sistema StorageGRID e l'origine delle identità. Tuttavia, tutte le impostazioni configurate vengono conservate, consentendo di riattivare facilmente la federazione delle identità in futuro.

### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

### 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 all'account tenant 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 viene eseguita.

### Fasi

1. Selezionare **ACCESS MANAGEMENT > Identity Federation**.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).
3. Selezionare **Salva**.

### Informazioni correlate

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

### Gestione dei gruppi

Assegnare le autorizzazioni ai gruppi di utenti per controllare quali attività possono essere eseguite dagli utenti del tenant. È possibile importare gruppi federati da un'origine di identità, ad esempio Active Directory o OpenLDAP, oppure creare gruppi locali.



Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti locali non potranno accedere a Gestione tenant, anche se possono accedere alle risorse S3 e Swift, in base alle autorizzazioni di 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 a un gruppo le seguenti autorizzazioni. Tenere presente che i tenant S3 e Swift dispongono di permessi di gruppo diversi. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

Permesso	Descrizione
Accesso root	<p>Fornisce l'accesso completo al tenant Manager e all'API di gestione del tenant.</p> <p><b>Nota:</b> gli utenti Swift devono disporre dell'autorizzazione di accesso root per accedere all'account tenant.</p>
Amministratore	<p>Solo tenant Swift. Fornisce l'accesso completo ai container e agli oggetti Swift per questo account tenant</p> <p><b>Nota:</b> gli utenti di Swift devono disporre dell'autorizzazione di amministratore di Swift per eseguire qualsiasi operazione con l'API DI Swift REST.</p>
Gestisci le tue credenziali S3	<p>Solo tenant S3. Consente agli utenti di creare e rimuovere le proprie chiavi di accesso S3. Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu <b>STORAGE (S3) &gt; My S3 access keys</b>.</p>
Gestire tutti i bucket	<ul style="list-style-type: none"> <li>• S3 tenant: Consente agli utenti di utilizzare tenant Manager e l'API di gestione tenant per creare ed eliminare i bucket S3 e per gestire le impostazioni di tutti i bucket S3 nell'account tenant, indipendentemente dalle policy di gruppo o bucket S3.</li> </ul> <p>Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu <b>Bucket</b>.</p> <ul style="list-style-type: none"> <li>• Tenant Swift: Consente agli utenti Swift di controllare il livello di coerenza per i container Swift utilizzando l'API di gestione tenant.</li> </ul> <p><b>Nota:</b> è possibile assegnare l'autorizzazione Gestisci tutti i bucket solo ai gruppi Swift dall'API di gestione tenant. Non è possibile assegnare questa autorizzazione ai gruppi Swift utilizzando il tenant Manager.</p>

Permesso	Descrizione
Gestire gli endpoint	<p>Solo tenant S3. Consente agli utenti di utilizzare il gestore tenant o l'API di gestione tenant per creare o modificare gli endpoint, che vengono utilizzati come destinazione per i servizi della piattaforma StorageGRID.</p> <p>Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu <b>Platform Services Endpoint</b>.</p>

## Informazioni correlate

["Utilizzare S3"](#)

["USA Swift"](#)

### Creazione di gruppi per un tenant S3

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

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.
- Se si intende importare un gruppo federated, la federazione delle identità è stata configurata e il gruppo federated esiste già nell'origine delle identità configurata.

#### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.

Name	ID	Type	Access mode
Applications	22cc2e27-88ee-4461-a8c6-30b550beeeec0	Local	Read-write
Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

2. Selezionare **Crea gruppo**.

3. 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.

4. 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.
- **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

5. Selezionare **continua**.

6. Selezionare una modalità di accesso. 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.

- **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 del tenant Manager o del tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

7. Selezionare le autorizzazioni di gruppo per questo gruppo.

Consultare le informazioni sulle autorizzazioni di gestione del tenant.

8. Selezionare **continua**.

9. Selezionare un criterio di gruppo per determinare le autorizzazioni di accesso S3 di cui avranno i membri di questo gruppo.

- **Nessun accesso S3**: Impostazione 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.
- **Personalizzato**: Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo. Consultare le istruzioni per l'implementazione di un'applicazione client S3 per informazioni dettagliate sui criteri di gruppo, tra cui la sintassi del linguaggio e gli esempi.

10. 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.

In questo esempio, i membri del gruppo possono solo elencare e accedere a una cartella corrispondente al proprio nome utente (prefisso della 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": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

11. Selezionare il pulsante visualizzato, a seconda che si stia creando un gruppo federato o un gruppo locale:

- Gruppo federato: **Crea gruppo**
- Gruppo locale: **Continua**

Se si sta creando un gruppo locale, il passaggio 4 (Aggiungi utenti) viene visualizzato dopo aver selezionato **continua**. Questo passaggio non viene visualizzato per i gruppi federati.

12. Selezionare la casella di controllo per ciascun utente che si desidera aggiungere al gruppo, quindi selezionare **Crea gruppo**.

In alternativa, è possibile salvare il gruppo senza aggiungere utenti. È possibile aggiungere utenti al gruppo in un secondo momento oppure selezionarlo quando si aggiungono nuovi utenti.

13. Selezionare **fine**.

Il gruppo creato viene visualizzato nell'elenco dei gruppi. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### Informazioni correlate

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

["Utilizzare S3"](#)

#### Creazione di gruppi per un tenant Swift

È possibile gestire le autorizzazioni di accesso per un account tenant Swift importando gruppi federati o creando gruppi locali. Almeno un gruppo deve disporre

dell'autorizzazione Swift Administrator, necessaria per gestire i container e gli oggetti per un account tenant Swift.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.
- Se si intende importare un gruppo federated, la federazione delle identità è stata configurata e il gruppo federated esiste già nell'origine delle identità configurata.

#### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beeeec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

2. Selezionare **Crea gruppo**.

3. 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.

4. 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.
- **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

5. Selezionare **continua**.

6. Selezionare una modalità di accesso. 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.

- **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 del tenant Manager o del tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

7. Impostare l'autorizzazione di gruppo.

- Selezionare la casella di controllo **Root Access** se gli utenti devono accedere all'API di gestione tenant o tenant Manager. (Impostazione predefinita)
- Deselezionare la casella di controllo **Root Access** se gli utenti non hanno bisogno dell'accesso all'API di gestione tenant o tenant. Ad esempio, deselectare la casella di controllo per le applicazioni che non richiedono l'accesso al tenant. Quindi, assegnare l'autorizzazione **Swift Administrator** per consentire a questi utenti di gestire container e oggetti.

8. Selezionare **continua**.

9. Selezionare la casella di controllo **Swift Administrator** se l'utente deve poter utilizzare l'API SWIFT REST.

Gli utenti Swift devono disporre dell'autorizzazione Root Access per accedere a Tenant Manager. Tuttavia, l'autorizzazione Root Access non consente agli utenti di autenticarsi nell'API SWIFT REST per creare container e acquisire oggetti. Gli utenti devono disporre dell'autorizzazione di amministratore Swift per autenticarsi nell'API DI Swift REST.

10. Selezionare il pulsante visualizzato, a seconda che si stia creando un gruppo federato o un gruppo locale:

- Gruppo federato: **Crea gruppo**
- Gruppo locale: **Continua**

Se si sta creando un gruppo locale, il passaggio 4 (Aggiungi utenti) viene visualizzato dopo aver selezionato **continua**. Questo passaggio non viene visualizzato per i gruppi federati.

11. Selezionare la casella di controllo per ciascun utente che si desidera aggiungere al gruppo, quindi selezionare **Crea gruppo**.

In alternativa, è possibile salvare il gruppo senza aggiungere utenti. È possibile aggiungere utenti al gruppo in un secondo momento oppure selezionarlo quando si creano nuovi utenti.

12. Selezionare **fine**.

Il gruppo creato viene visualizzato nell'elenco dei gruppi. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

**Informazioni correlate**

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

["USA Swift"](#)

**Visualizzazione e modifica dei dettagli del gruppo**

Quando si visualizzano i dettagli di un gruppo, è possibile modificare il nome visualizzato del gruppo, le autorizzazioni, i criteri e gli utenti che appartengono al gruppo.

**Di cosa hai bisogno**

- È necessario accedere a tenant Manager utilizzando un browser supportato.

- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.

## Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare il nome del gruppo di cui si desidera visualizzare o modificare i dettagli.

In alternativa, è possibile selezionare **azioni > Visualizza dettagli gruppo**.

Viene visualizzata la pagina dei dettagli del gruppo. L'esempio seguente mostra la pagina dei dettagli del gruppo S3.

## Overview

Display name:	<a href="#">Applications</a>
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

[Group permissions](#)[S3 group policy](#)[Users](#)

### Manage group permissions

Select an access mode for this group and select one or more permissions.

**Access mode** [?](#)

Select whether users can change settings and perform operations or whether they can only view settings and features.

 Read-write  Read-only**Group permissions** [?](#)

Select the tenant account permissions you want to assign to this group.

 **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

 **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

 **Manage Endpoints**

Allows users to configure endpoints for platform services.

 **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

[Save changes](#)

### 3. Apportare le modifiche necessarie alle impostazioni del gruppo.



Per assicurarsi che le modifiche vengano salvate, selezionare **Save changes** (Salva modifiche) dopo aver apportato le modifiche in ciascuna sezione. Una volta salvate le modifiche, nell'angolo superiore destro della pagina viene visualizzato un messaggio di conferma.

- a. In alternativa, selezionare il nome visualizzato o l'icona di modifica per aggiornare il nome visualizzato.

Non è possibile modificare il nome univoco di un gruppo. Non è possibile modificare il nome visualizzato per un gruppo federated.

- b. Facoltativamente, aggiornare le autorizzazioni.
- c. Per i criteri di gruppo, apportare le modifiche appropriate al tenant S3 o Swift.
  - Se si modifica un gruppo per un tenant S3, selezionare un criterio di gruppo S3 diverso. Se si seleziona un criterio S3 personalizzato, aggiornare la stringa JSON come richiesto.
  - Se si modifica un gruppo per un tenant Swift, selezionare o deselectare la casella di controllo **Swift Administrator**.

Per ulteriori informazioni sull'autorizzazione amministratore Swift, consultare le istruzioni per la creazione di gruppi per un tenant Swift.

- d. Facoltativamente, aggiungere o rimuovere utenti.

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

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### Informazioni correlate

["Creazione di gruppi per un tenant S3"](#)

["Creazione di gruppi per un tenant Swift"](#)

#### Aggiunta di utenti a un gruppo locale

È possibile aggiungere utenti a un gruppo locale in base alle esigenze.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.

#### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare il nome del gruppo locale a cui si desidera aggiungere utenti.

In alternativa, è possibile selezionare **azioni > Visualizza dettagli gruppo**.

Viene visualizzata la pagina dei dettagli del gruppo.

## Overview

Display name:	<a href="#">Applications</a>
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

[Group permissions](#)[S3 group policy](#)[Users](#)

### Manage group permissions

Select an access mode for this group and select one or more permissions.

**Access mode** [?](#)

Select whether users can change settings and perform operations or whether they can only view settings and features.

 Read-write  Read-only**Group permissions** [?](#)

Select the tenant account permissions you want to assign to this group.

 **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

 **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

 **Manage Endpoints**

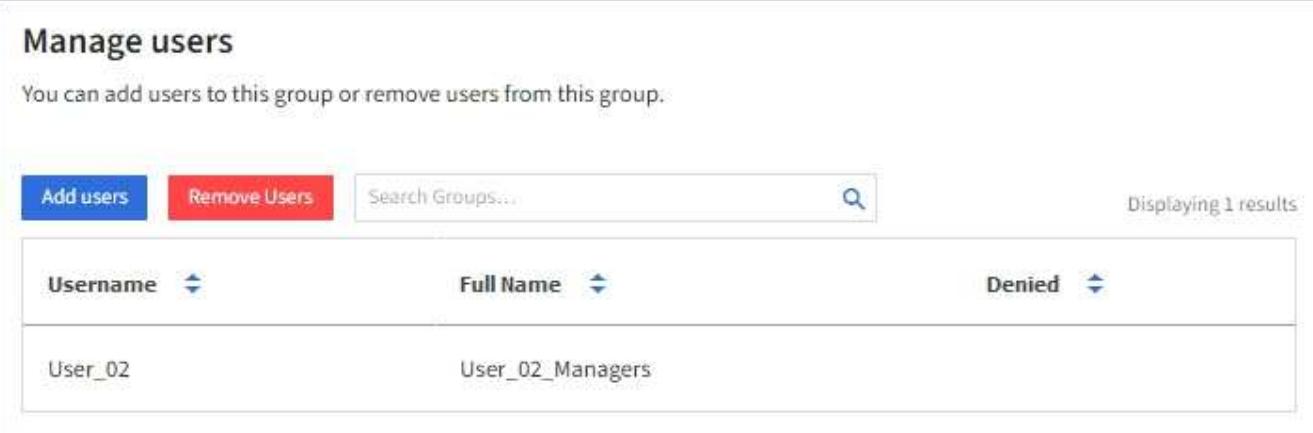
Allows users to configure endpoints for platform services.

 **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

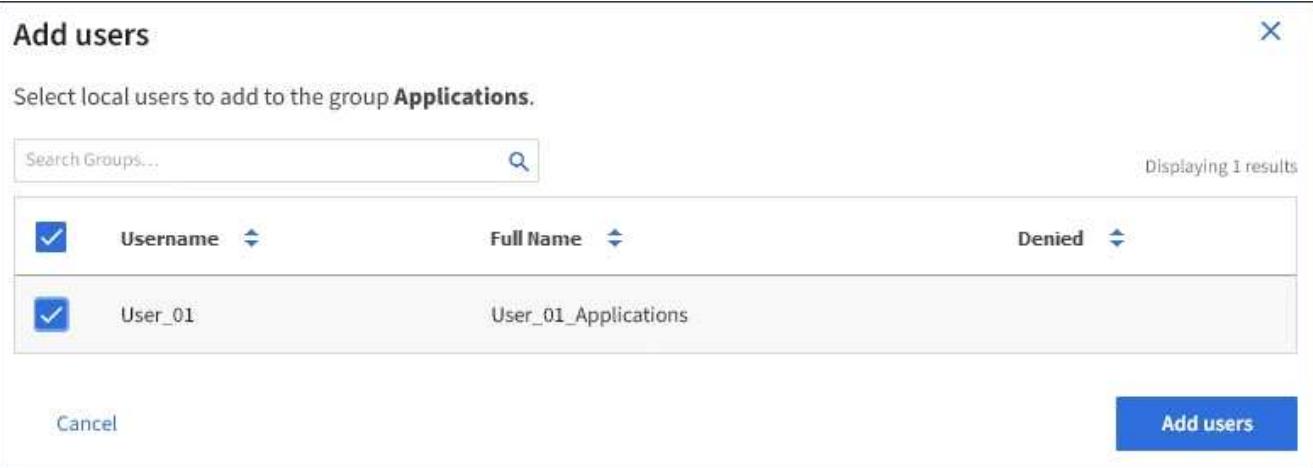
[Save changes](#)

3. Selezionare **Manage Users** (Gestisci utenti), quindi selezionare **Add users** (Aggiungi utenti).



The screenshot shows the 'Manage users' interface. At the top, there are buttons for 'Add users' (blue) and 'Remove Users' (red). Below them is a search bar with 'Search Groups...' and a magnifying glass icon. To the right, it says 'Displaying 1 results'. The main area has three columns: 'Username', 'Full Name', and 'Denied'. A user named 'User\_02' is listed with the full name 'User\_02\_Managers' and the status 'Denied'.

4. Selezionare gli utenti che si desidera aggiungere al gruppo, quindi selezionare **Aggiungi utenti**.



The screenshot shows the 'Add users' dialog box. It says 'Select local users to add to the group **Applications**'. Below is a search bar with 'Search Groups...' and a magnifying glass icon. It also says 'Displaying 1 results'. The list shows a user 'User\_01' with the full name 'User\_01\_Applications'. A checkbox next to the user's name is checked. At the bottom, there are 'Cancel' and 'Add users' buttons.

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### Modifica del nome di un gruppo

È possibile modificare il nome visualizzato di un gruppo. Non è possibile modificare il nome univoco di un gruppo.

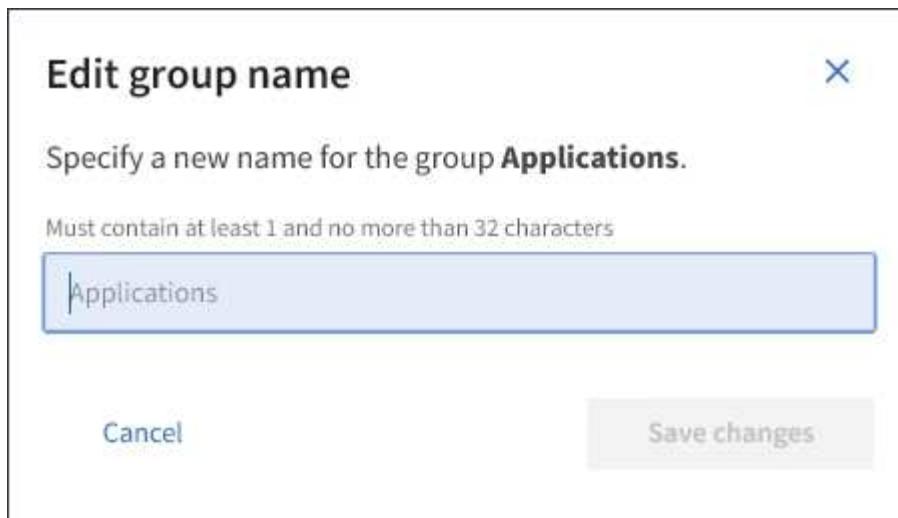
#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.

#### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare la casella di controllo del gruppo di cui si desidera modificare il nome visualizzato.
3. Selezionare **azioni > Modifica nome gruppo**.

Viene visualizzata la finestra di dialogo **Edit group name** (Modifica nome gruppo).



4. Se si sta modificando un gruppo locale, aggiornare il nome visualizzato in base alle necessità.

Non è possibile modificare il nome univoco di un gruppo. Non è possibile modificare il nome visualizzato per un gruppo federated.

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

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### Informazioni correlate

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

#### Duplicazione di un gruppo

È possibile creare nuovi gruppi più rapidamente duplicando un gruppo esistente.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.

#### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare la casella di controllo relativa al gruppo che si desidera duplicare.
3. Selezionare **Duplica gruppo**. Per ulteriori dettagli sulla creazione di un gruppo, consulta le istruzioni per la creazione di gruppi per un tenant S3 o Swift.
4. 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.

5. 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.
- **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

6. Selezionare **continua**.
7. Se necessario, modificare le autorizzazioni per questo gruppo.
8. Selezionare **continua**.
9. Se si desidera duplicare un gruppo per un tenant S3, selezionare un criterio diverso dai pulsanti di opzione **Add S3 policy** (Aggiungi criterio S3). Se è stato selezionato un criterio personalizzato, aggiornare la stringa JSON come richiesto.
10. Selezionare **Crea gruppo**.

#### Informazioni correlate

["Creazione di gruppi per un tenant S3"](#)

["Creazione di gruppi per un tenant Swift"](#)

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

#### Eliminazione di un gruppo

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

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso root.

#### Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.

# Groups

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

2 groups

Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous 1 Next →

2. Selezionare le caselle di controllo dei gruppi che si desidera eliminare.

3. Selezionare **azioni** > **Elimina gruppo**.

Viene visualizzato un messaggio di conferma.

4. Selezionare **Delete group** (Elimina gruppo) per confermare che si desidera eliminare i gruppi indicati nel messaggio di conferma.

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Informazioni correlate

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

## Gestione degli utenti locali

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

## Di cosa hai bisogno

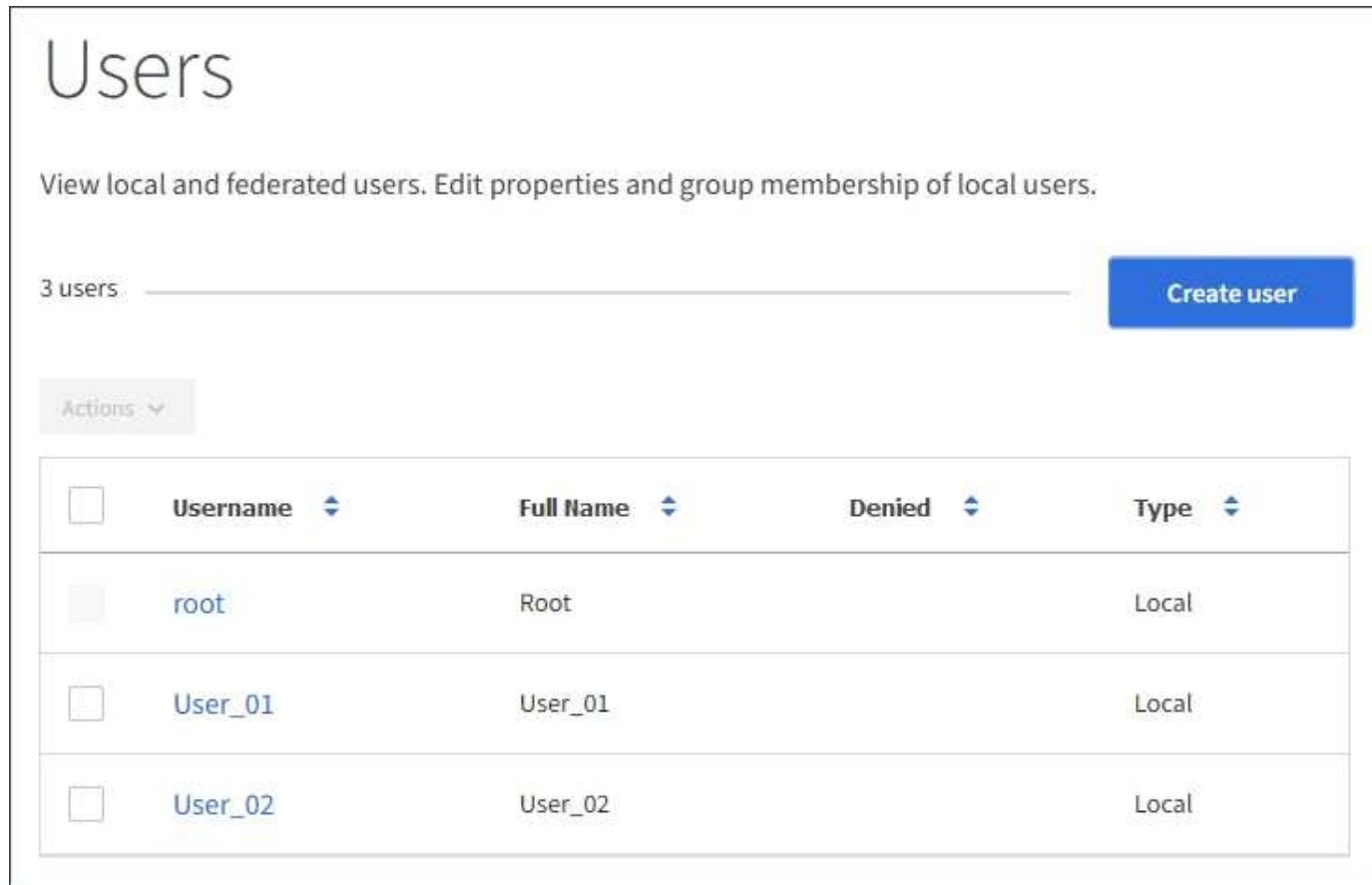
- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti in lettura/scrittura che disponga dell'autorizzazione di accesso root.



Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti locali non potranno accedere al Manager tenant o all'API di gestione tenant, anche se possono utilizzare le applicazioni client S3 o Swift per accedere alle risorse del tenant, in base alle autorizzazioni di gruppo.

## Accesso alla pagina utenti

Selezionare **ACCESS MANAGEMENT > Users**.



<input type="checkbox"/>	Username	Full Name	Denied	Type
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

### Creazione di utenti locali

È possibile creare utenti locali e assegnarli 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.

Gli utenti Swift che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o di accesso al container Swift.

### Fasi

1. Selezionare **Crea utente**.

2. Compilare i seguenti campi.

- **Nome completo:** Il nome completo dell'utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
- **Username:** Il nome che l'utente utilizzerà per accedere. I nomi utente devono essere univoci e non possono essere modificati.
- **Password:** Una password che viene utilizzata quando l'utente effettua l'accesso.
- **Conferma password:** Digitare la stessa password immessa nel campo Password.
- **Nega accesso:** Se si seleziona **Sì**, l'utente non potrà accedere all'account tenant, anche se potrebbe

ancora appartenere a uno o più gruppi.

Ad esempio, è possibile utilizzare questa funzione per sospendere temporaneamente la capacità di accesso di un utente.

### 3. Selezionare **continua**.

### 4. Assegnare l'utente a uno o più gruppi locali.

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.

### 5. Selezionare **Crea utente**.

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Modifica dei dettagli dell'utente

Quando si modificano i dettagli di un utente, è possibile modificare il nome completo e la password dell'utente, aggiungerlo a gruppi diversi e impedire all'utente di accedere al tenant.

### Fasi

#### 1. Nell'elenco Users (utenti), selezionare il nome dell'utente di cui si desidera visualizzare o modificare i dettagli.

In alternativa, è possibile selezionare la casella di controllo dell'utente, quindi selezionare **azioni > Visualizza dettagli utente**.

#### 2. Apportare le modifiche necessarie alle impostazioni utente.

- Modificare il nome completo dell'utente in base alle necessità selezionando il nome completo o l'icona di modifica  Nella sezione Panoramica.

Non è possibile modificare il nome utente.

- Nella scheda **Password**, modificare la password dell'utente in base alle necessità.
- Nella scheda **Access**, consentire all'utente di accedere (selezionare **No**) o impedire all'utente di accedere (selezionare **Sì**) in base alle necessità.
- Nella scheda **gruppi**, aggiungere l'utente ai gruppi o rimuoverlo dai gruppi in base alle necessità.
- In base alle esigenze di ciascuna sezione, selezionare **Save Changes** (Salva modifiche).

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Duplicazione degli utenti locali

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

### Fasi

#### 1. Nell'elenco Users (utenti), selezionare l'utente che si desidera duplicare.

#### 2. Selezionare **Duplica utente**.

#### 3. Modificare i seguenti campi per il nuovo utente.

- **Nome completo:** Il nome completo dell’utente, ad esempio il nome e il cognome di una persona o il nome di un’applicazione.
- **Username:** Il nome che l’utente utilizzerà per accedere. I nomi utente devono essere univoci e non possono essere modificati.
- **Password:** Una password che viene utilizzata quando l’utente effettua l’accesso.
- **Conferma password:** Digitare la stessa password immessa nel campo Password.
- **Nega accesso:** Se si seleziona **Sì**, l’utente non potrà accedere all’account tenant, anche se potrebbe ancora appartenere a uno o più gruppi.

Ad esempio, è possibile utilizzare questa funzione per sospendere temporaneamente la capacità di accesso di un utente.

4. Selezionare **continua**.

5. Selezionare uno o più gruppi locali.

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.

6. Selezionare **Crea utente**.

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### **Eliminazione degli utenti locali**

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

Utilizzando Tenant Manager, è possibile eliminare gli utenti locali, ma non quelli federati. Per eliminare gli utenti federati, è necessario utilizzare l’origine delle identità federate.

#### **Fasi**

1. Nell’elenco Users (utenti), selezionare la casella di controllo dell’utente locale che si desidera eliminare.
2. Selezionare **azioni > Elimina utente**.
3. Nella finestra di dialogo di conferma, selezionare **Delete user** (Elimina utente) per confermare che si desidera eliminare l’utente dal sistema.

Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### **Informazioni correlate**

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

## **Gestione degli account tenant S3**

È possibile utilizzare Tenant Manager per gestire le chiavi di accesso S3 e per creare e gestire i bucket S3.

- ["Gestione delle chiavi di accesso S3"](#)
- ["Gestione dei bucket S3"](#)

## Gestione delle 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.

### A proposito di questa attività

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.

### Creazione di chiavi di accesso S3 personalizzate

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

### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Gestisci credenziali S3.

### 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 quelle necessarie ed eliminare le chiavi non 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 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 protezione nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare una 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

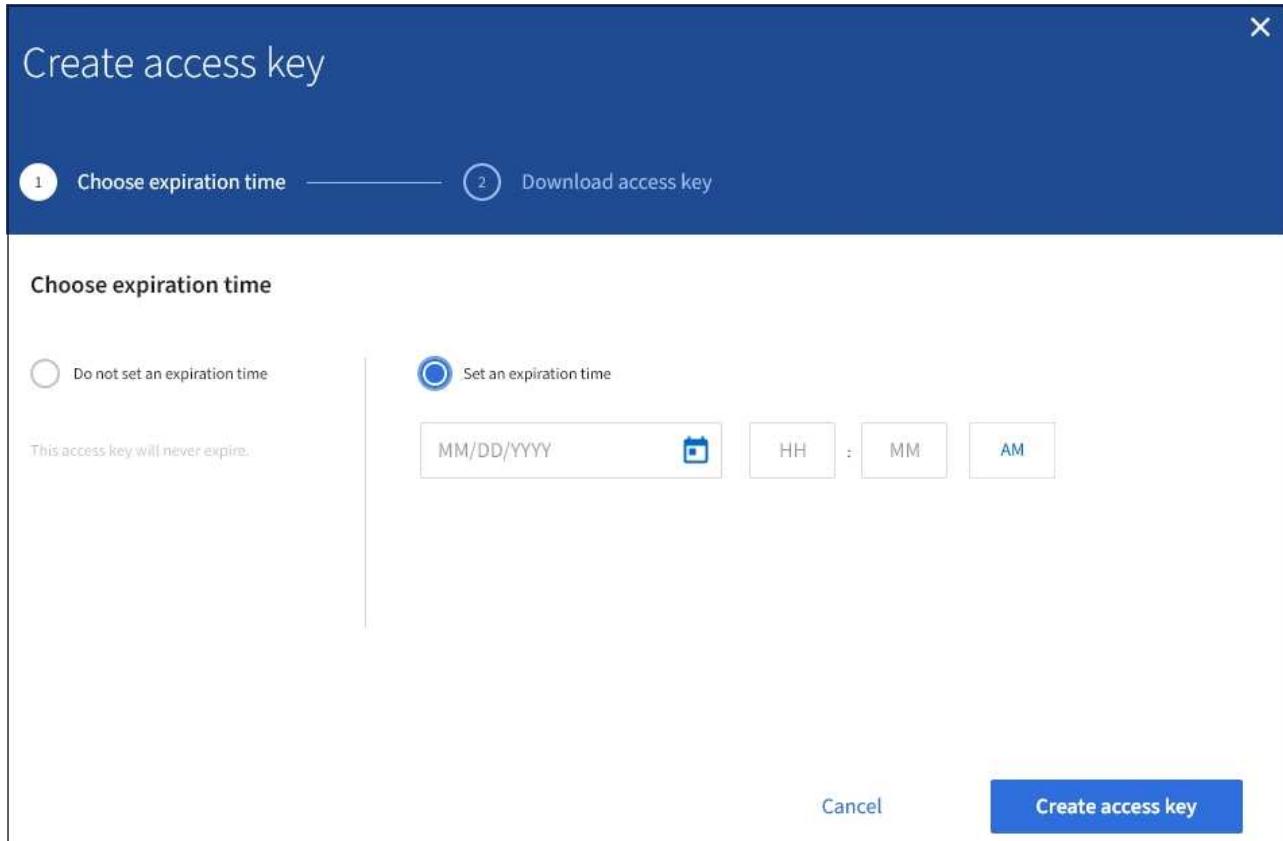
### 1. Selezionare **STORAGE (S3) > My access key**.

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.



### 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.

Create access key X

1 Choose expiration time 2 Download access key

**Download access key**

To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.

**Info** You will not be able to view the Access key ID or Secret access key after you close this dialog.

**Access key ID**  
SHTBQKDRVHQ34YKKUAWX Copy

**Secret access key**  
UGu9+XeACtnOWQYFdbzmgmgVXXDvCkSOzT1OsZ9K Copy

Download .csv Finish

6. Selezionare **fine**.

La nuova chiave è elencata nella pagina i miei tasti di accesso. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### Informazioni correlate

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

#### Visualizzazione delle chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, 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. In base alle esigenze, è possibile creare nuove chiavi o eliminare chiavi che non vengono più utilizzate.

#### Di cosa hai bisogno

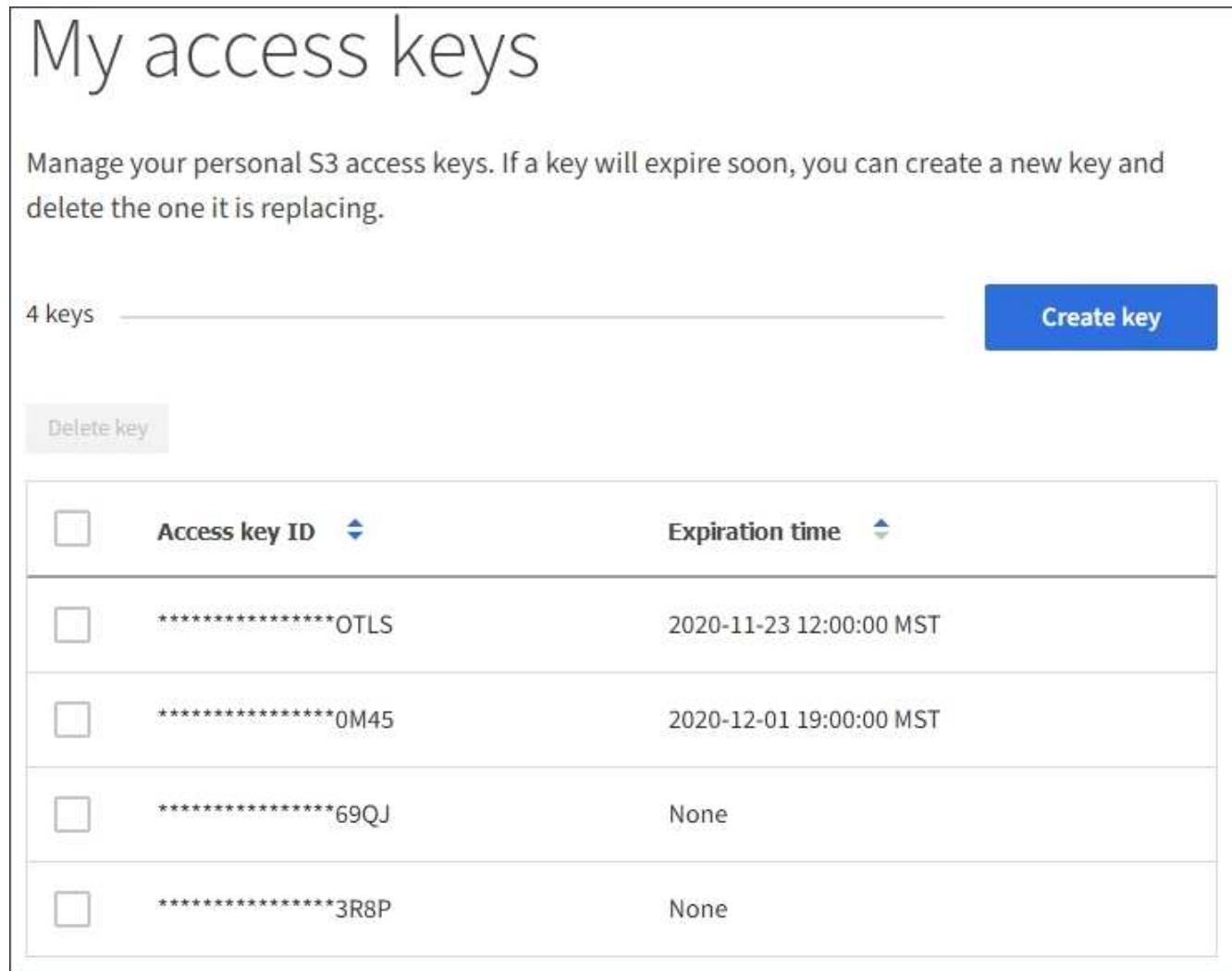
- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Gestisci credenziali S3.

**i** 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.



<input type="checkbox"/>	Access key ID	Expiration time
<input type="checkbox"/>	*****OTLS	2020-11-23 12:00:00 MST
<input type="checkbox"/>	*****0M45	2020-12-01 19:00:00 MST
<input type="checkbox"/>	*****69QJ	None
<input type="checkbox"/>	*****3R8P	None

### 2. Ordinare le chiavi in base a **scadenza** o **ID chiave di accesso**.

### 3. Se necessario, creare nuove chiavi ed eliminarle manualmente 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.

## Informazioni correlate

["Creazione di chiavi di accesso S3 personalizzate"](#)

["Eliminazione delle proprie chiavi di accesso S3"](#)

**Eliminazione delle 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.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Gestisci 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

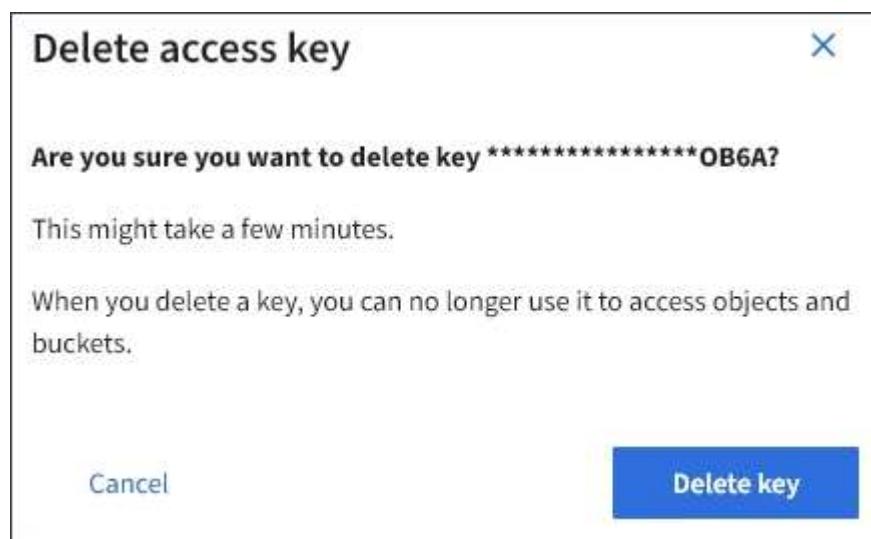
##### 1. Selezionare **STORAGE (S3) > My access key**.

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

##### 2. Selezionare la casella di controllo per ogni chiave di accesso che si desidera rimuovere.

##### 3. Selezionare **Delete key** (Elimina chiave).

Viene visualizzata una finestra di dialogo di conferma.



##### 4. Selezionare **Delete key** (Elimina chiave).

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### Informazioni correlate

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

[Creazione delle 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.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'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 non 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.

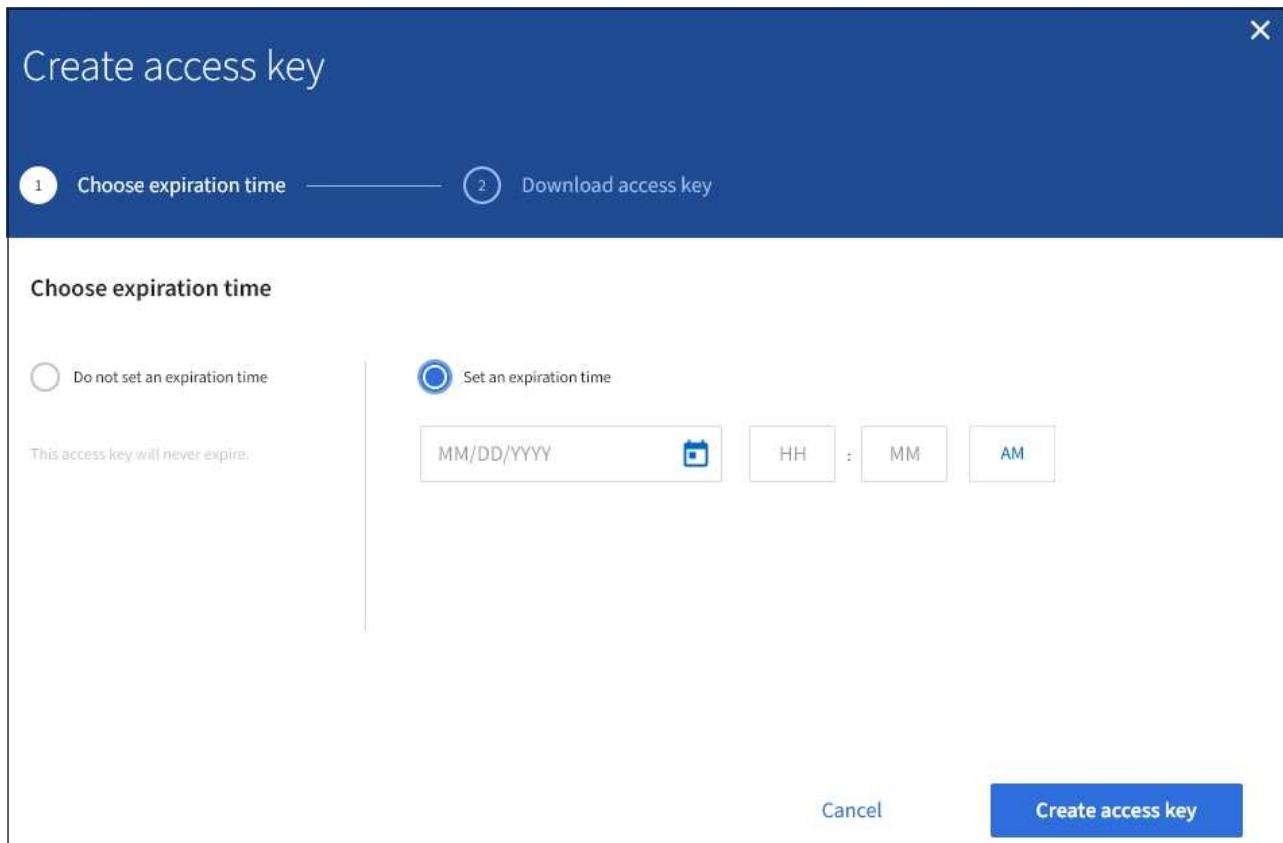
Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

- 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 una 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 **ACCESS MANAGEMENT > Users**.
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 una 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.



##### 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.

Create access key X

1 Choose expiration time 2 Download access key

**Download access key**

To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.

**Info** You will not be able to view the Access key ID or Secret access key after you close this dialog.

**Access key ID**  
SHTBQKDRVHQ34YKKUAWX Copy

**Secret access key**  
UGu9+XeACtnOWQYFdbzmgmgVXXDvCkSOzT1OsZ9K Copy

Download .csv Finish

7. Selezionare **fine**.

La nuova chiave è elencata nella scheda Access Keys della pagina User Details (Dettagli utente). Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

#### Informazioni correlate

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

#### Visualizzazione delle 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.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

i 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

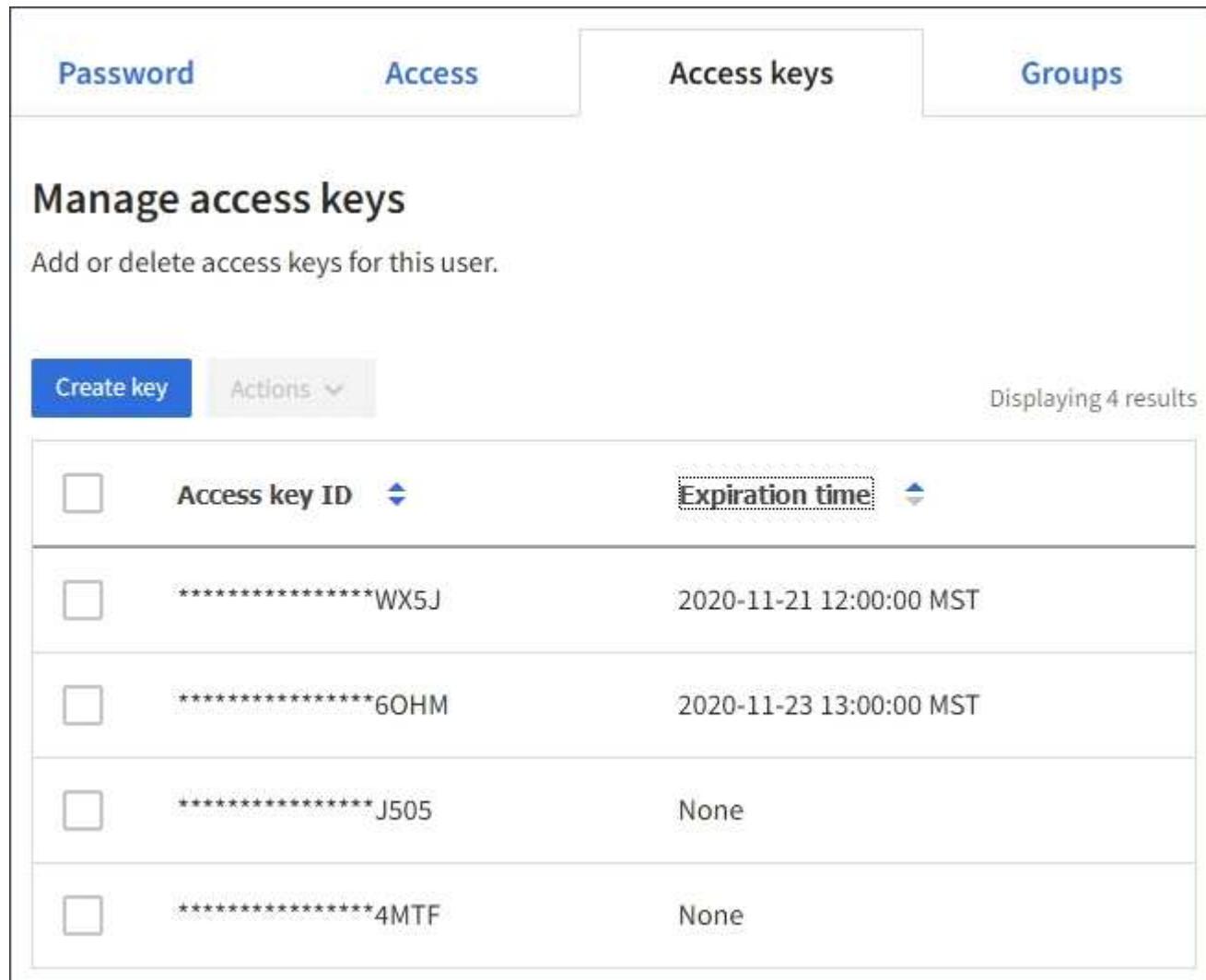
### 1. Selezionare **ACCESS MANAGEMENT > Users**.

Viene visualizzata la pagina **Users** (utenti) che elenca gli utenti esistenti.

### 2. Selezionare l'utente di cui si desidera visualizzare le chiavi di accesso S3.

Viene visualizzata la pagina **User Details** (Dettagli utente).

### 3. Selezionare **Access keys**.



Access key ID	Expiration time
*****WX5J	2020-11-21 12:00:00 MST
*****60HM	2020-11-23 13:00:00 MST
*****J505	None
*****4MTF	None

### 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

["Creazione delle chiavi di accesso S3 di un altro utente"](#)

## "Eliminazione delle chiavi di accesso S3 di un altro utente"

### Eliminazione delle 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.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario disporre dell'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 **ACCESS MANAGEMENT > Users**.

Viene visualizzata la pagina **Users** (utenti) che elenca gli utenti esistenti.

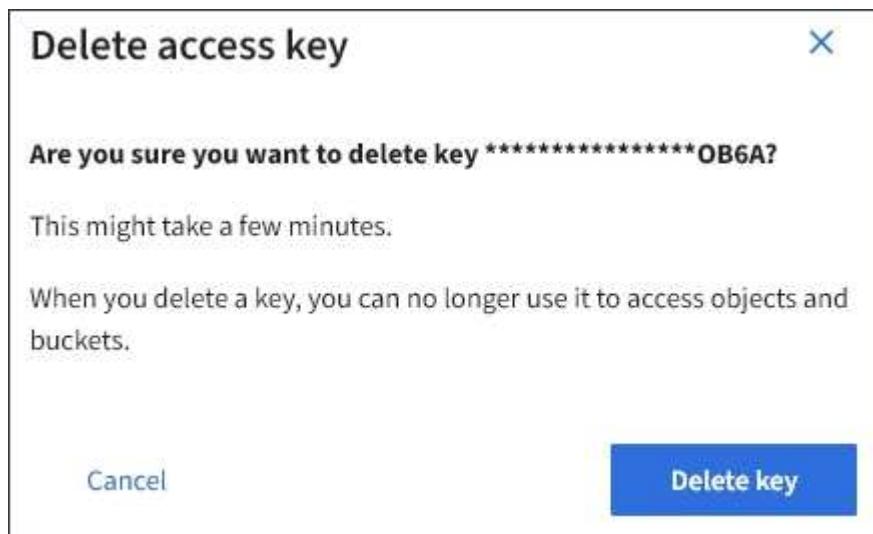
##### 2. Selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

Viene visualizzata la pagina **User Details** (Dettagli utente).

##### 3. Selezionare **Access keys**, quindi selezionare la casella di controllo per ogni chiave di accesso che si desidera eliminare.

##### 4. Selezionare **azioni > Elimina tasto selezionato**.

Viene visualizzata una finestra di dialogo di conferma.



##### 5. Selezionare **Delete key** (Elimina chiave).

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

## Informazioni correlate

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

## Gestione dei bucket S3

Se si utilizza un tenant S3 con le autorizzazioni appropriate, è possibile creare, visualizzare ed eliminare bucket S3, aggiornare le impostazioni del livello di coerenza, configurare Cross-Origin Resource Sharing (CORS), attivare e disattivare le impostazioni dell'ultimo aggiornamento dell'ora di accesso e gestire i servizi della piattaforma S3.

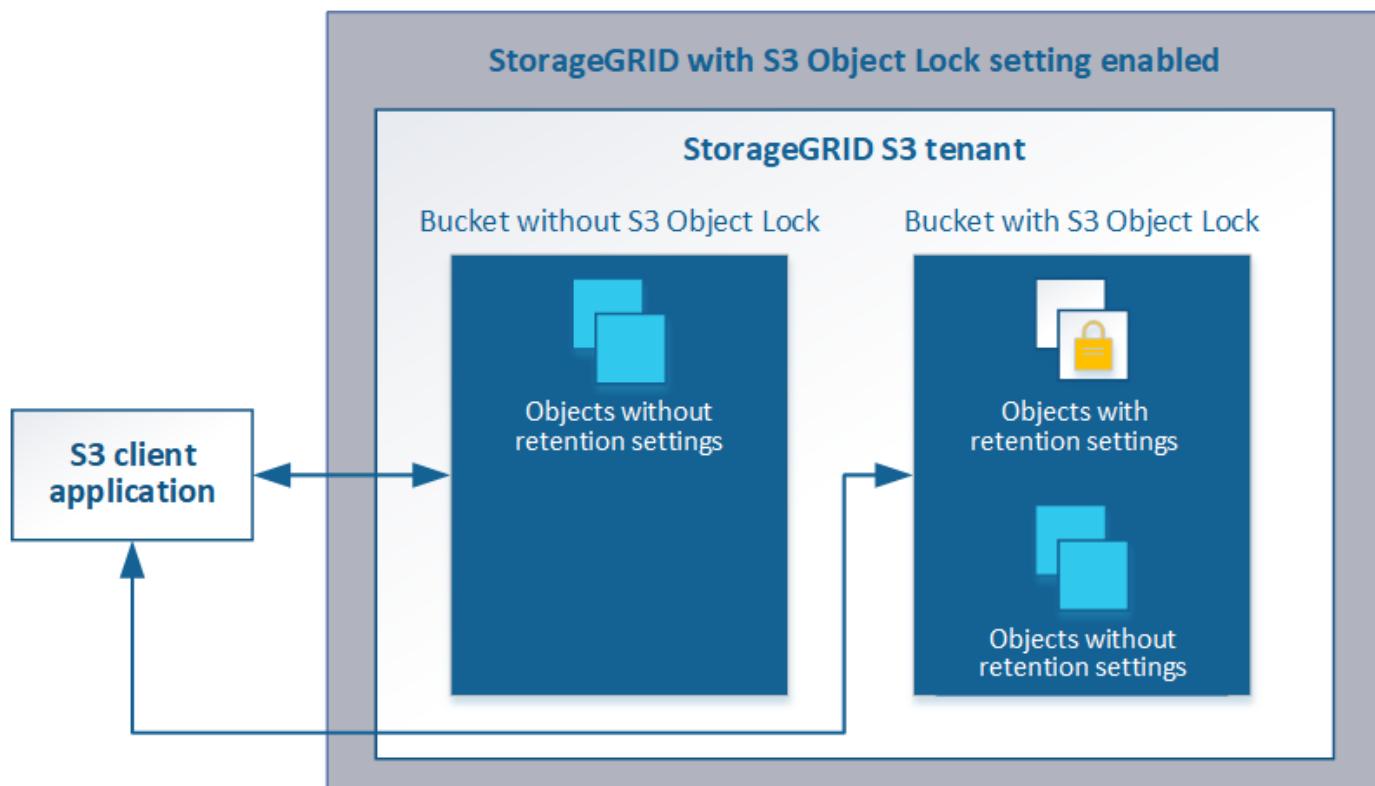
### Utilizzo di S3 Object Lock

È possibile utilizzare la funzione blocco oggetti S3 in StorageGRID se gli oggetti devono essere conformi ai requisiti normativi per la conservazione.

### 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).

Come mostrato nella figura, quando l'impostazione globale S3 Object Lock è attivata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock attivato, le applicazioni client S3 possono specificare le impostazioni di conservazione per qualsiasi versione di oggetto in quel bucket. Una versione dell'oggetto deve avere le impostazioni di conservazione specificate per essere protetta da S3 Object Lock.



La funzione blocco oggetto StorageGRID S3 offre una singola modalità di conservazione equivalente alla modalità di conformità Amazon S3. Per impostazione predefinita, una versione dell'oggetto protetto non può essere sovrascritta o eliminata da alcun utente. La funzione blocco oggetti di StorageGRID S3 non supporta una modalità di governance e non consente agli utenti con autorizzazioni speciali di ignorare le impostazioni di conservazione o di eliminare gli oggetti protetti.

Se in un bucket è attivato il blocco oggetti S3, l'applicazione client S3 può specificare una o entrambe le seguenti impostazioni di conservazione a livello di oggetto durante la creazione o l'aggiornamento di un oggetto:

- **Mantieni-fino-data:** Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere modificato o cancellato. Come richiesto, è possibile aumentare la data di conservazione di un oggetto fino alla data odierna, ma non è possibile diminuarla.
- **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.

Per ulteriori informazioni su queste impostazioni, consultare "Using S3 Object lock" in ["Operazioni e limitazioni supportate dall'API REST S3"](#).

### Gestione dei 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, consultare l'articolo della Knowledge base di NetApp.

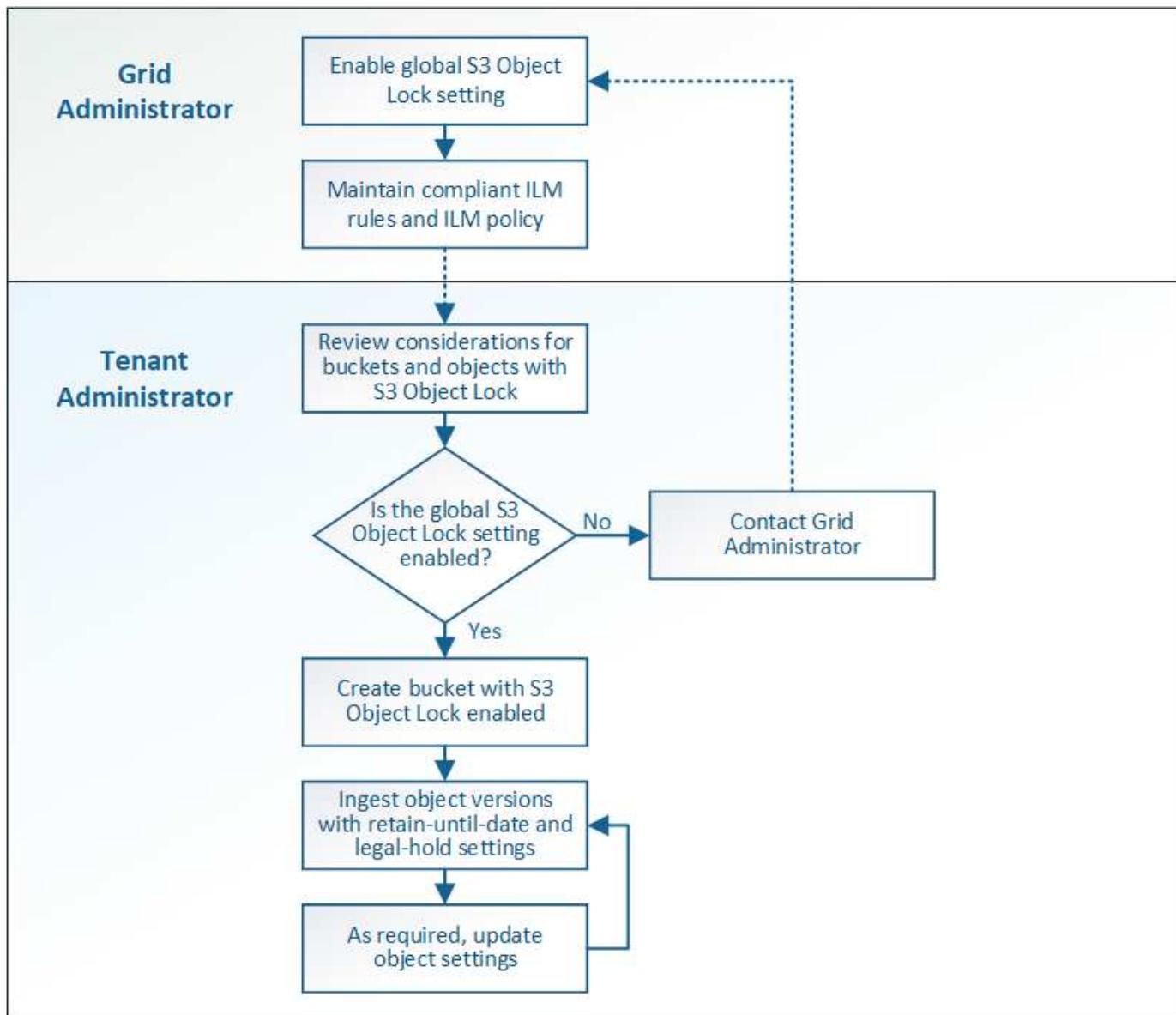
["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

### Workflow di blocco oggetti S3

Il diagramma del flusso di lavoro mostra i passaggi di alto livello per l'utilizzo della funzione blocco oggetti S3 in StorageGRID.

Prima di poter creare bucket con blocco oggetti S3 attivato, l'amministratore della griglia deve attivare l'impostazione di blocco oggetti S3 globale per l'intero sistema StorageGRID. L'amministratore della griglia deve inoltre garantire che il criterio ILM (Information Lifecycle Management) sia "compliant"; deve soddisfare i requisiti dei bucket con S3 Object Lock abilitato. Per ulteriori informazioni, contattare l'amministratore della griglia o consultare le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

Una volta attivata l'impostazione globale S3 Object Lock, è possibile creare bucket con S3 Object Lock attivato. È quindi possibile utilizzare l'applicazione client S3 per specificare facoltativamente le impostazioni di conservazione per ciascuna versione dell'oggetto.



#### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

#### Requisiti per il blocco oggetti S3

Prima di abilitare il blocco oggetti S3 per un bucket, esaminare i requisiti per gli oggetti e i bucket di blocco oggetti S3 e il ciclo di vita degli oggetti nei bucket con il blocco oggetti S3 attivato.

#### 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.

Questo esempio di Tenant Manager mostra un bucket con blocco oggetti S3 attivato.

# Buckets

Create buckets and manage bucket settings.



Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

- Se si intende utilizzare il blocco oggetti S3, è necessario attivare il blocco oggetti S3 quando si crea il bucket. Non è possibile attivare il blocco oggetti S3 per un bucket esistente.
- La versione del bucket è richiesta con S3 Object Lock. Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket.
- Dopo aver creato un bucket con S3 Object Lock attivato, non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per quel bucket.
- Un bucket StorageGRID con blocco oggetti S3 attivato non ha un periodo di conservazione predefinito. L'applicazione client S3 può invece specificare una data di conservazione e un'impostazione di conservazione legale per ogni versione di oggetto aggiunta a quel bucket.
- La configurazione del ciclo di vita del bucket è supportata per i bucket S3 Object Lifecycle.
- 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

- L'applicazione client S3 deve specificare le impostazioni di conservazione per ciascun oggetto che deve essere protetto da S3 Object Lock.
- È possibile aumentare la data di conservazione per una versione a oggetti, ma non è mai possibile diminuire questo valore.
- Se si riceve la notifica di un'azione legale o di un'indagine normativa in sospeso, è possibile conservare le informazioni pertinenti ponendo un blocco legale su una versione dell'oggetto. Quando una versione dell'oggetto è sottoposta a un blocco legale, non è possibile eliminare tale oggetto da StorageGRID, anche se ha raggiunto la data di conservazione. Non appena la conservazione legale viene revocata, la versione dell'oggetto può essere eliminata se è stata raggiunta la data di conservazione.
- S3 Object Lock richiede l'utilizzo di bucket con versione. 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 tre fasi:

### 1. Acquisizione oggetto

- Quando si aggiunge una versione dell'oggetto a un bucket con S3 Object Lock attivato, l'applicazione client S3 può specificare facoltativamente le impostazioni di conservazione per l'oggetto (conservazione fino alla data, conservazione legale o entrambe). StorageGRID genera quindi metadati per l'oggetto, che includono un UUID (Unique Object Identifier) e la data e l'ora di acquisizione.
- Dopo l'acquisizione di una versione a oggetti con impostazioni di conservazione, i relativi dati e i metadati S3 definiti dall'utente non possono essere modificati.
- StorageGRID memorizza i metadati dell'oggetto indipendentemente dai dati dell'oggetto. Conserva tre copie di tutti i metadati degli oggetti in ogni sito.

## 2. Conservazione degli oggetti

- StorageGRID memorizza più copie dell'oggetto. Il numero e il tipo esatti di copie e le posizioni di storage sono determinati dalle regole conformi nel criterio ILM attivo.

## 3. Eliminazione di oggetti

- È possibile eliminare un oggetto una volta raggiunta la data di conservazione.
- Non è possibile eliminare un oggetto sottoposto a conservazione a fini giudiziari.

### Creazione di un bucket S3

È possibile utilizzare Tenant Manager per creare bucket S3 per i dati dell'oggetto. Quando si crea un bucket, è necessario specificare il nome e l'area del bucket. Se per il sistema StorageGRID è attivata l'impostazione blocco oggetti S3 globale, è possibile attivare il blocco oggetti S3 per il bucket.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che disponga dell'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Se si prevede di creare un bucket con blocco oggetti S3, l'impostazione globale blocco oggetti S3 deve essere stata attivata per il sistema StorageGRID ed è necessario esaminare i requisiti per i bucket e gli oggetti blocco oggetti S3.

#### ["Utilizzo di S3 Object Lock"](#)

### Fasi

#### 1. Selezionare **STORAGE (S3) > Bucket**.

Viene visualizzata la pagina bucket che elenca i bucket già creati.

# Buckets

Create buckets and manage bucket settings.

0 buckets

[Create bucket](#)

Actions ▾

Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
No buckets found					
<a href="#">Create bucket</a>					

## 2. Selezionare **Crea bucket**.

Viene visualizzata la procedura guidata Create bucket.

### Create bucket

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name [?](#)

Region [?](#)

[Cancel](#) [Create bucket](#)



Se l'impostazione globale S3 Object Lock (blocco oggetti S3) è attivata, Create bucket (Crea bucket) include una seconda fase per la gestione del blocco oggetti S3 per il bucket.

## 3. Immettere un nome univoco per il bucket.



Non è possibile modificare il nome del bucket dopo averlo creato.

I nomi dei bucket devono essere conformi alle seguenti regole:

- Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).
- Deve essere conforme al DNS.
- Deve contenere almeno 3 e non più di 63 caratteri.
- 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 ulteriori informazioni, consultare la documentazione di Amazon Web Services (AWS).

#### 4. Selezionare la regione per questo bucket.

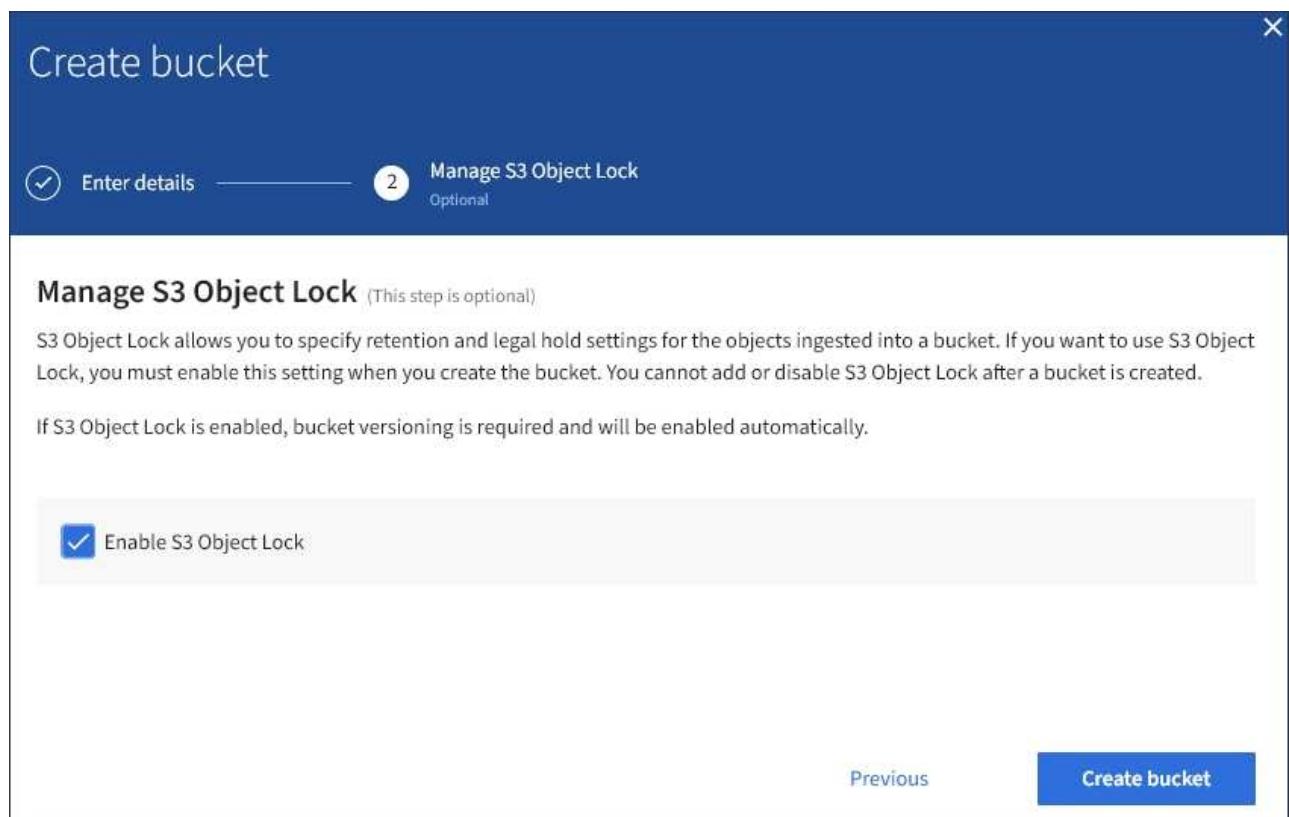
L'amministratore di StorageGRID gestisce le regioni disponibili. L'area di un bucket può influire sulla policy di protezione dei dati applicata agli oggetti. Per impostazione predefinita, tutti i bucket vengono creati in us-east-1 regione.



Non è possibile modificare la regione dopo aver creato il bucket.

#### 5. Selezionare **Crea bucket** o **continua**.

- Se l'impostazione globale S3 Object Lock (blocco oggetti S3) non è attivata, selezionare **Create bucket** (Crea bucket). Il bucket viene creato e aggiunto alla tabella nella pagina Bucket.
- Se l'impostazione globale S3 Object Lock (blocco oggetti S3) è attivata, selezionare **Continue** (continua). Fase 2, viene visualizzato il messaggio Manage S3 Object Lock (Gestisci blocco oggetti S3).



6. Facoltativamente, selezionare la casella di controllo per attivare il blocco oggetti S3 per questo bucket.

S3 Object Lock deve essere attivato per il bucket prima che un'applicazione client S3 possa specificare le impostazioni di conservazione fino alla data e conservazione legale per gli oggetti aggiunti al bucket.



Non è possibile attivare o disattivare il blocco oggetti S3 dopo aver creato il bucket.



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

7. Selezionare **Crea bucket**.

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

#### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Informazioni sull'API di gestione del tenant"](#)

["Utilizzare S3"](#)

#### Visualizzazione dei dettagli del bucket S3

È possibile visualizzare un elenco delle impostazioni dei bucket e dei bucket nell'account tenant.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.

#### Fasi

1. Selezionare **STORAGE (S3) > Bucket**.

Viene visualizzata la pagina bucket che elenca tutti i bucket per l'account tenant.

Buckets						
Create buckets and manage bucket settings.						
2 buckets						
<a href="#">Actions</a> <a href="#">▼</a>						<a href="#">Create bucket</a>
<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

[← Previous](#) **1** [Next →](#)

## 2. Esaminare le informazioni relative a ciascun bucket.

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

- Name (Nome): Il nome univoco del bucket, che non può essere modificato.
- S3 Object Lock (blocco oggetti S3): Se S3 Object Lock (blocco oggetti S3) è attivato per questo bucket.

Questa colonna non viene visualizzata se l'impostazione di blocco oggetti S3 globale è disattivata.

Questa colonna mostra anche informazioni relative a qualsiasi bucket compatibile legacy.

- Regione: La regione del bucket, che non può essere modificata.
- Object Count (Conteggio oggetti): Il numero di oggetti in questo bucket.
- Spazio utilizzato: La dimensione logica di tutti gli oggetti in questo bucket. La dimensione logica non include lo spazio effettivo richiesto per le copie replicate o codificate in cancellazione o per i metadati degli oggetti.
- Data di creazione: Data e ora di creazione del bucket.



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.

## 3. Per visualizzare e gestire le impostazioni di un bucket, selezionare il nome del bucket.

Viene visualizzata la pagina dei dettagli del bucket.

Questa pagina consente di visualizzare e modificare le impostazioni per le opzioni del bucket, l'accesso al bucket e i servizi della piattaforma.

Consultare le istruzioni per la configurazione di ogni impostazione o servizio di piattaforma.

Buckets > bucket-02

## Overview

Name:	bucket-02
Region:	us-east-1
S3 Object Lock:	Disabled
Date created:	2020-11-04 14:51:59 MST

**Bucket options** **Bucket access** **Platform services**

Consistency level	Read-after-new-write	▼
Last access time updates	Disabled	▼

### Informazioni correlate

["Modifica del livello di coerenza"](#)

["Attivazione o disattivazione degli ultimi aggiornamenti dell'orario di accesso"](#)

["Configurazione di Cross-Origin Resource Sharing \(CORS\)"](#)

["Configurazione della replica di CloudMirror"](#)

["Configurazione delle notifiche degli eventi"](#)

["Configurazione del servizio di integrazione della ricerca"](#)

### Modifica del livello di coerenza

Se si utilizza un tenant S3, è possibile utilizzare il tenant Manager o l'API di gestione tenant per modificare il controllo di coerenza per le operazioni eseguite sugli oggetti nei bucket S3.

### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che disponga dell'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

### A proposito di questa attività

Il livello di coerenza crea un compromesso tra la disponibilità degli oggetti e la coerenza di tali oggetti nei

diversi nodi e siti di storage. In generale, è necessario utilizzare il livello di coerenza **Read-after-new-write** per i bucket. Se il livello di coerenza **Read-after-new-write** non soddisfa i requisiti dell'applicazione client, è possibile modificare il livello di coerenza impostando il livello di coerenza del bucket o utilizzando **Consistency-Control** intestazione. Il **Consistency-Control** l'intestazione sovrascrive il livello di coerenza del bucket.



Quando si modifica il livello di coerenza di un bucket, solo gli oggetti acquisiti dopo la modifica vengono garantiti per soddisfare il livello rivisto.

## Fasi

1. Selezionare **STORAGE (S3) > Bucket**.
2. Selezionare il nome del bucket dall'elenco.

Viene visualizzata la pagina dei dettagli del bucket.

3. Selezionare **Opzioni bucket > livello di coerenza**.

Bucket options      Bucket access      Platform services

**Consistency level**      Read-after-new-write (default) ^

Change the consistency control for operations performed on the objects in the bucket. Consistency level makes a trade-off between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

In general, use the **Read-after-new-write** consistency level for your buckets. Then, if objects do not meet availability or consistency requirements, change the client application's behavior, or set the **Consistency-Control** header for an individual API request, which overrides the bucket setting.

All  
 Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.

Strong-global  
 Guarantees read-after-write consistency for all client requests across all sites.

Strong-site  
 Guarantees read-after-write consistency for all client requests within a site.

Read-after-new-write (default)  
 Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

Note: If your application attempts HEAD operations on keys that do not exist, set the Consistency Level to **Available**, unless you require AWS S3 consistency guarantees. Otherwise, a high number of 500 Internal Server errors can result if one or more Storage Nodes are unavailable.

Available  
 Behaves the same as the **Read-after-new-write** consistency level, but only provides eventual consistency for HEAD operations. Offers higher availability for HEAD operations than **Read-after-new-write** if Storage Nodes are unavailable. Differs from AWS S3 consistency guarantees for HEAD operations only.

**Save changes**

4. Selezionare un livello di coerenza per le operazioni eseguite sugli oggetti in questo bucket.

Livello di 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.

Livello di coerenza	Descrizione
Sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
Read-after-new-write (valore predefinito)	<p>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. Corrisponde alle garanzie di coerenza di Amazon S3.</p> <p><b>Nota:</b> se l'applicazione tenta di ESEGUIRE operazioni SU chiavi non esistenti, impostare il livello di coerenza su <b>disponibile</b>, a meno che non si richiedano garanzie di coerenza Amazon S3. In caso contrario, se uno o più nodi di storage non sono disponibili, possono verificarsi un numero elevato di errori 500 nel server interno.</p>
Disponibile (eventuale coerenza per le operazioni TESTA)	Si comporta come il livello di coerenza <b>Read-after-new-write</b> , ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a <b>Read-after-new-write</b> se i nodi storage non sono disponibili. Differisce dalle garanzie di coerenza di Amazon S3 solo per le operazioni HEAD.

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

#### Informazioni correlate

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

#### Attivazione o disattivazione degli 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 sono valide solo per i sistemi StorageGRID che includono almeno una regola ILM che utilizza l'opzione **tempo di ultimo accesso** nelle istruzioni di posizionamento. È possibile ignorare queste istruzioni se il sistema StorageGRID non include tale regola.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che disponga dell'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

**Last Access Time** è una delle opzioni disponibili per le istruzioni di posizionamento **Reference Time** per una regola ILM. L'impostazione del tempo di riferimento per una regola su tempo ultimo accesso consente agli amministratori della griglia di specificare che gli oggetti devono essere posizionati in determinate posizioni di storage in base all'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.



Consultare le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

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 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	Si	Sì	Sì	Sì

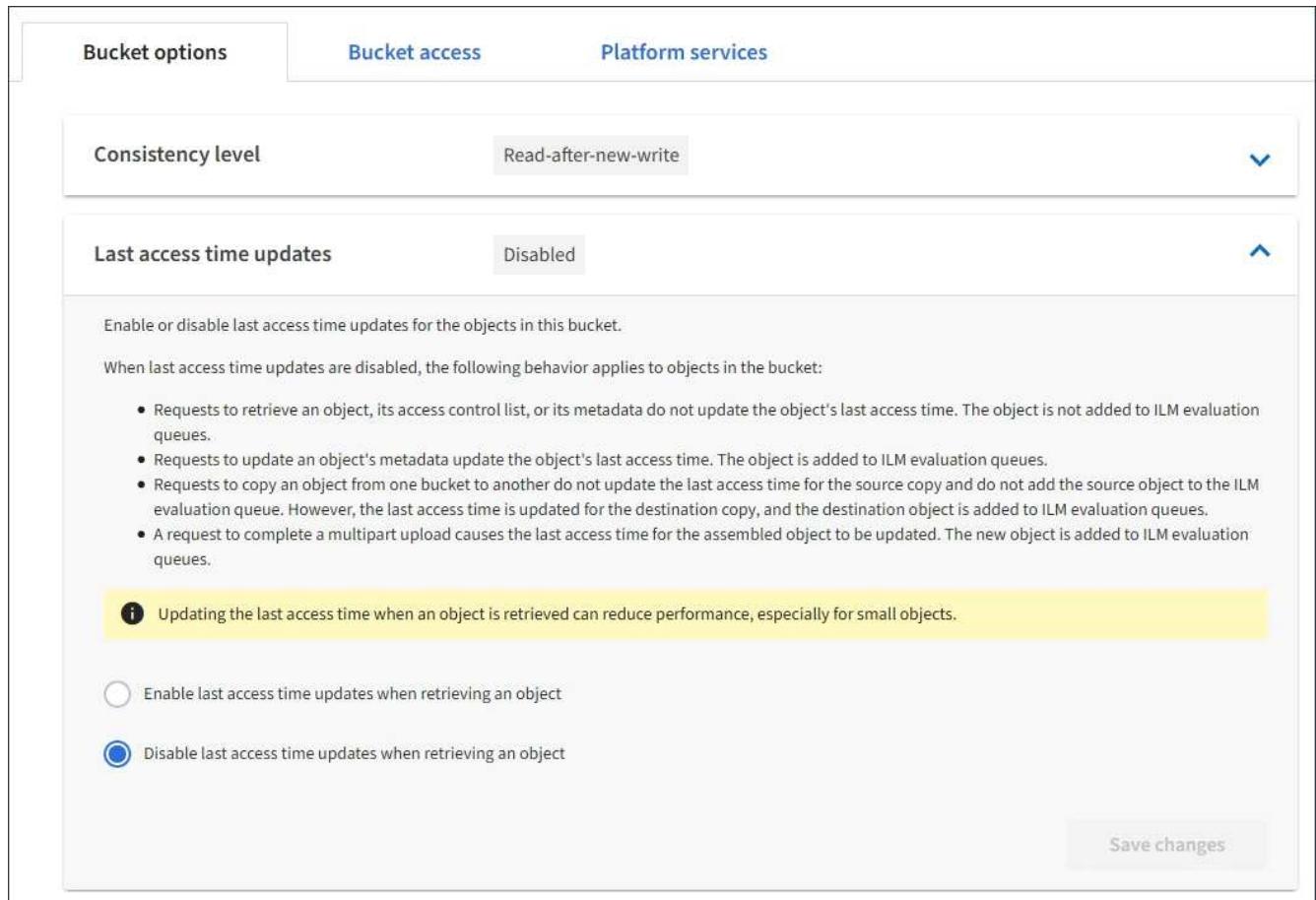
Richiesta di copia di un oggetto da un bucket all'altro	<ul style="list-style-type: none"> <li>• No, per la copia di origine</li> <li>• Sì, per la copia di destinazione</li> </ul>	<ul style="list-style-type: none"> <li>• No, per la copia di origine</li> <li>• Sì, per la copia di destinazione</li> </ul>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

## Fasi

1. Selezionare **STORAGE (S3) > Bucket**.
2. Selezionare il nome del bucket dall'elenco.

Viene visualizzata la pagina dei dettagli del bucket.

3. Selezionare **Opzioni bucket > ultimi aggiornamenti dell'ora di accesso**.
4. Selezionare il pulsante di opzione appropriato per attivare o disattivare gli ultimi aggiornamenti dell'orario di accesso.



The screenshot shows the 'Bucket options' tab selected in the top navigation bar. The 'Last access time updates' section is open, showing the 'Disabled' button is selected. A note below explains: 'Enable or disable last access time updates for the objects in this bucket. When last access time updates are disabled, the following behavior applies to objects in the bucket:'. A list of behaviors follows, and a note at the bottom says: 'Updating the last access time when an object is retrieved can reduce performance, especially for small objects.' The 'Save changes' button is visible at the bottom right.

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

## Informazioni correlate

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

## "Gestire gli oggetti con ILM"

### Configurazione di Cross-Origin Resource Sharing (CORS)

È possibile configurare Cross-Origin Resource Sharing (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.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che disponga dell'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

#### A proposito di questa attività

Cross-Origin Resource Sharing (CORS) è un meccanismo di sicurezza che consente alle applicazioni web client di un dominio di accedere alle risorse di un dominio diverso. Si supponga, ad esempio, di utilizzare un bucket S3 denominato `Images` per memorizzare le immagini. Configurando CORS per `Images` bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito web <http://www.example.com>.

#### Fasi

1. Utilizzare un editor di testo per creare l'XML richiesto per abilitare CORS.

Questo esempio mostra l'XML utilizzato per abilitare il CORS per un bucket S3. Questo XML consente a qualsiasi dominio di inviare richieste GET al bucket, ma consente solo il `http://www.example.com` Dominio per inviare richieste DI 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 Amazon Web Services \(AWS\): Guida per sviluppatori Amazon Simple Storage Service"](#).

2. In Tenant Manager, selezionare **STORAGE (S3) > Bucket**.

3. Selezionare il nome del bucket dall'elenco.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **bucket access > 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 e selezionare **Save changes** (Salva modifiche).

Cross-Origin Resource Sharing (CORS) Disabled

Configure Cross-Origin Resource Sharing (CORS) for an S3 bucket if you want that bucket and objects in that bucket to be accessible to web applications in other domains.

Enable CORS Clear

```
<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>
```

**Save changes**

7. Per modificare l'impostazione CORS per il bucket, aggiornare l'XML di configurazione CORS nella casella di testo o selezionare **Clear** per ricominciare. Quindi selezionare **Save Changes** (Salva modifiche).

8. Per disattivare il CORS per il bucket, deselectare la casella di controllo **Enable CORS** (attiva CORS), quindi selezionare **Save Changes** (Salva modifiche).

#### Eliminazione di un bucket S3

È possibile utilizzare Tenant Manager per eliminare un bucket S3 vuoto.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che disponga dell'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

## A proposito di questa attività

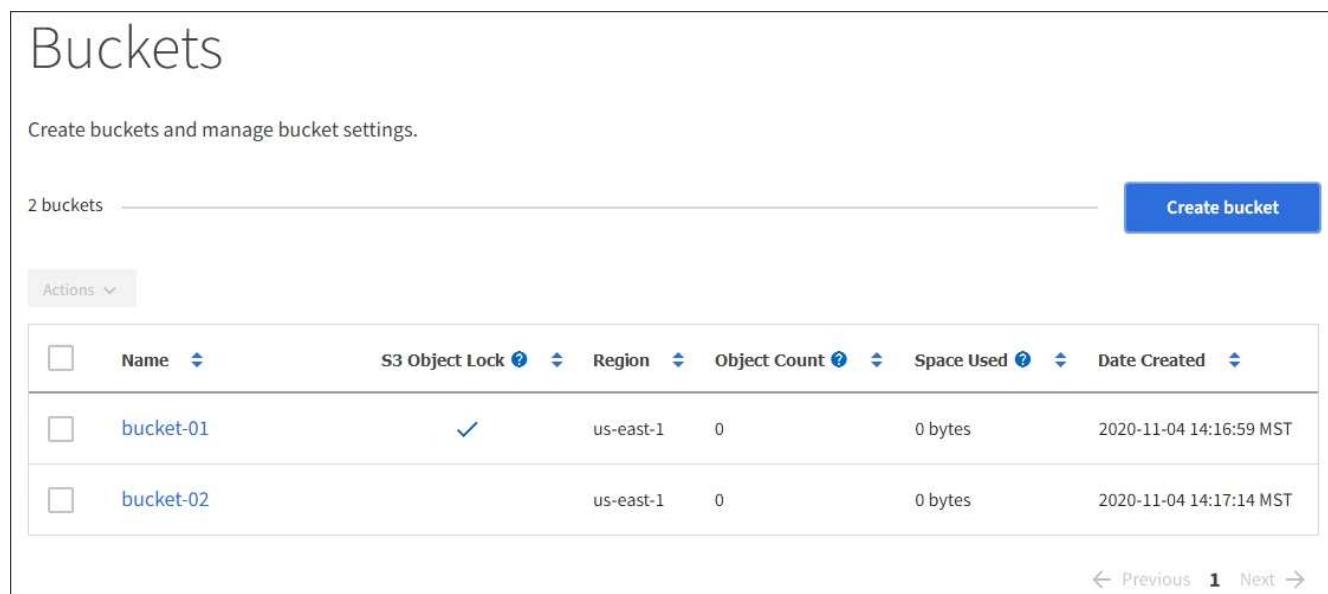
Queste istruzioni descrivono come eliminare un bucket S3 utilizzando il Tenant Manager. È inoltre possibile eliminare i bucket S3 utilizzando l'API di gestione tenant o l'API REST S3.

Non è possibile eliminare un bucket S3 se contiene oggetti o versioni di oggetti non correnti. Per informazioni sull'eliminazione degli oggetti con versione S3, vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni.

## Fasi

### 1. Selezionare **STORAGE (S3) > Bucket**.

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



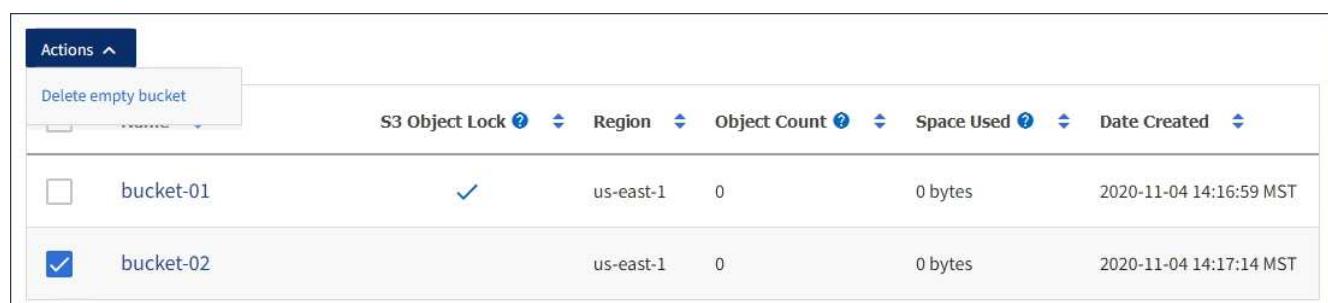
The screenshot shows the AWS S3 Buckets page. At the top, it says "Buckets" and "Create buckets and manage bucket settings." Below that, it shows "2 buckets" and a "Create bucket" button. A "Actions" dropdown menu is open for the second bucket, "bucket-02". The table below lists the buckets with columns: Name, S3 Object Lock, Region, Object Count, Space Used, and Date Created. The second row (bucket-02) has a checked checkbox in the Actions column. The bottom of the page shows navigation links: "← Previous", "1", and "Next →".

Actions	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

### 2. Selezionare la casella di controllo per il bucket vuoto che si desidera eliminare.

Il menu Actions (azioni) è attivato.

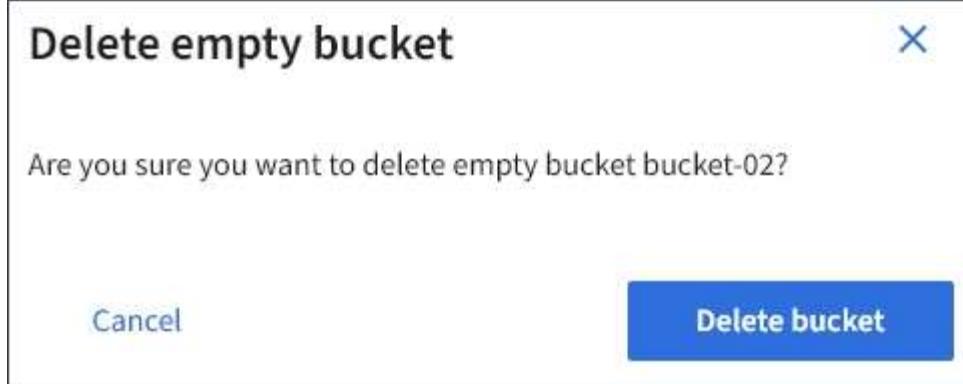
### 3. Dal menu Actions (azioni), selezionare **Delete empty bucket** (Elimina bucket vuoto).



The screenshot shows the AWS S3 Buckets page with the "Actions" dropdown menu open for bucket-02. The "Delete empty bucket" option is highlighted. The table below lists the buckets with columns: Name, S3 Object Lock, Region, Object Count, Space Used, and Date Created. The second row (bucket-02) has a checked checkbox in the Actions column. The bottom of the page shows navigation links: "← Previous", "1", and "Next →".

Actions	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

Viene visualizzato un messaggio di conferma.



4. Se si è certi di voler eliminare il bucket, selezionare **Delete bucket** (Elimina bucket).

StorageGRID conferma che il bucket è vuoto, quindi lo elimina. Questa operazione potrebbe richiedere alcuni minuti.

Se il bucket non è vuoto, viene visualizzato un messaggio di errore. È necessario eliminare tutti gli oggetti prima di poter eliminare il bucket.



Unable to delete the bucket because it is not empty. You must delete all objects before you can delete this bucket.

#### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

### Gestione dei servizi della piattaforma S3

Se l'utilizzo dei servizi della piattaforma è consentito per l'account tenant S3, è possibile utilizzare i servizi della piattaforma per sfruttare i servizi esterni e configurare la replica, le notifiche e l'integrazione della ricerca di CloudMirror per i bucket S3.

- ["Quali sono i servizi della piattaforma"](#)
- ["Considerazioni sull'utilizzo dei servizi della piattaforma"](#)
- ["Configurazione degli endpoint dei servizi di piattaforma"](#)
- ["Configurazione della replica di CloudMirror"](#)
- ["Configurazione delle notifiche degli eventi"](#)
- ["Utilizzando il servizio di integrazione della ricerca"](#)

#### Quali sono i servizi della piattaforma

I servizi della piattaforma StorageGRID possono aiutarti a implementare una strategia di cloud ibrido.

Se l'utilizzo dei servizi della piattaforma è consentito per l'account tenant, è possibile configurare i seguenti servizi per qualsiasi bucket S3:

- **Replica di CloudMirror:** Il servizio di replica di StorageGRID CloudMirror viene utilizzato per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

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.

- **Notifiche:** Le notifiche degli eventi per bucket vengono utilizzate per inviare notifiche su azioni specifiche eseguite su oggetti a un servizio Amazon Simple Notification Service™ (SNS) esterno specificato.

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.



Sebbene la notifica degli eventi possa essere configurata su un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (inclusi lo stato Mantieni fino alla data e conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

- **Search Integration service:** Il servizio di integrazione della ricerca viene utilizzato per inviare metadati di oggetti S3 a un indice Elasticsearch specificato, dove è possibile cercare o analizzare i metadati utilizzando il servizio esterno.

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 su un bucket con S3 Object Lock attivato, i metadati S3 Object Lock (inclusi Retain until Date e Legal Hold status) degli oggetti non saranno inclusi nei messaggi di notifica.

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 il servizio CloudMirror e le notifiche su un bucket StorageGRID S3 in modo da eseguire il mirroring di oggetti specifici al servizio di storage semplice Amazon, inviando una notifica relativa a ciascun oggetto a un'applicazione di monitoraggio 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 gli endpoint esterni configurati utilizzando Tenant Manager o l'API di gestione tenant. Ogni endpoint rappresenta una destinazione esterna, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento SNS (Simple Notification Service) o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

Dopo aver creato un endpoint, 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:

1. Se si desidera che tutti gli oggetti le cui chiavi iniziano con /images Per essere replicati in un bucket Amazon S3, è necessario aggiungere una configurazione di replica al bucket di origine.
2. Se si desidera anche inviare notifiche quando questi oggetti vengono memorizzati nel bucket, è necessario aggiungere una configurazione di notifica.
3. Infine, 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
Replica di CloudMirror	<ul style="list-style-type: none"><li>• OTTIENI la replica bucket</li><li>• METTI la replica del bucket</li></ul>
Notifiche	<ul style="list-style-type: none"><li>• OTTIENI notifica bucket</li><li>• NOTIFICA DEL bucket</li></ul>
Integrazione della ricerca	<ul style="list-style-type: none"><li>• OTTIENI la configurazione della notifica dei metadati del bucket</li><li>• INSERIRE la configurazione della notifica dei metadati del bucket</li></ul> <p>Queste operazioni sono personalizzate per StorageGRID.</p>

Per informazioni dettagliate sull'implementazione di queste API da parte di StorageGRID, consultare le istruzioni per l'implementazione delle applicazioni client S3.

#### Informazioni correlate

["Utilizzare S3"](#)

["Informazioni sul servizio di replica CloudMirror"](#)

["Informazioni sulle notifiche per i bucket"](#)

["Informazioni sul servizio di integrazione della ricerca"](#)

["Considerazioni sull'utilizzo dei servizi della piattaforma"](#)

#### Informazioni sul servizio di replica CloudMirror

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

La replica di CloudMirror funziona indipendentemente dal criterio ILM attivo 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.

Se 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 AWS 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.

In StorageGRID, è possibile replicare gli oggetti in un singolo bucket in più bucket di destinazione. A tale scopo, specificare la destinazione di ciascuna regola nel file XML di configurazione della replica. Non è possibile replicare un oggetto in più bucket contemporaneamente.

Inoltre, è possibile configurare la replica di CloudMirror su bucket con versione o senza versione e specificare un bucket con versione o senza versione come destinazione. 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.

Il comportamento di eliminazione per il servizio di replica CloudMirror è lo stesso del comportamento di eliminazione del servizio CRR (Cross Region Replication) fornito da Amazon S3: 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 marker di eliminazione nel bucket di destinazione né elimina l'oggetto di destinazione.

Man mano che gli oggetti vengono replicati nel bucket di destinazione, StorageGRID li contrassegna come "replicas". Un bucket StorageGRID di destinazione non esegue nuovamente la replica degli oggetti contrassegnati come replicate, proteggendo l'utente da loop di replica accidentali. Questo contrassegno di replica è interno a StorageGRID e non impedisce di sfruttare AWS CRR quando si utilizza un bucket Amazon S3 come destinazione.

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

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.

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.

## Informazioni correlate

["Configurazione della replica di CloudMirror"](#)

## Informazioni sulle notifiche per i bucket

Puoi attivare la notifica degli eventi per un bucket S3 se desideri che StorageGRID invii notifiche relative a eventi specifici a un servizio di notifica semplice Amazon di destinazione.

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

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 sequencer Digitare il messaggio dell'evento per determinare l'ordine degli eventi per un particolare oggetto, come descritto nella documentazione di Amazon S3.

## Notifiche e messaggi supportati

La notifica degli eventi StorageGRID segue l'API Amazon S3 con le seguenti limitazioni:

- Non è possibile configurare una notifica per i seguenti tipi di eventi. Questi tipi di evento sono **non supportati**.
  - s3:ReducedRedundancyLostObject
  - s3:ObjectRestore:Completed
- 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 nella tabella:

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

## Informazioni correlate

["Configurazione delle notifiche degli eventi"](#)

## Informazioni sul 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 automaticamente e in modo asincrono i metadati dell'oggetto S3 a un endpoint di destinazione ogni volta che un oggetto o i relativi metadati 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.

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 vengono generate sotto forma di un documento JSON denominato con il nome del bucket, il nome dell'oggetto e l'ID della versione, se presenti. 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 sull'indice.

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

- Viene creato un oggetto.
- Un oggetto viene eliminato, anche quando gli oggetti vengono eliminati 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.

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 il *Interoperability Matrix Tool* per determinare le versioni supportate di Elasticsearch.

#### Informazioni correlate

["Tool di matrice di interoperabilità NetApp"](#)

["XML di configurazione per l'integrazione della ricerca"](#)

["Metadati degli oggetti inclusi nelle notifiche dei metadati"](#)

["JSON generato dal servizio di integrazione della ricerca"](#)

## "Configurazione del servizio di integrazione della ricerca"

### Considerazioni sull'utilizzo dei servizi della piattaforma

Prima di implementare i servizi della piattaforma, esaminare i consigli e le considerazioni per l'utilizzo di questi servizi.

### Considerazioni sull'utilizzo dei servizi della piattaforma

Considerazione	Dettagli
Monitoraggio degli endpoint di destinazione	È necessario monitorare la disponibilità di ciascun endpoint di destinazione. Se la connettività all'endpoint di destinazione viene persa per un periodo di tempo prolungato ed esiste un grande backlog di richieste, le richieste client aggiuntive (come LE richieste PUT) a StorageGRID non avranno esito positivo. È necessario riprovare queste richieste non riuscite quando l'endpoint diventa raggiungibile.
Rallentamento dell'endpoint di destinazione	<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>
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>

Considerazione	Dettagli
Eliminazioni di oggetti basate su ILM	<p>Per far corrispondere il comportamento di eliminazione dei servizi CRR e SNS di AWS, CloudMirror e le richieste di notifica degli eventi non vengono inviate quando un oggetto nel bucket di origine viene cancellato 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>

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

Considerazione	Dettagli
Stato della replica	StorageGRID non supporta <code>x-amz-replication-status</code> intestazione.
Dimensione dell'oggetto	La dimensione massima per gli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è di 5 TB, che corrisponde alla dimensione massima degli oggetti supportata da StorageGRID.
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><b>Nota:</b> 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 alcuna richiesta DI tag DEGLI oggetti PUT o DELETE che fornisca 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 tag aggiornato a un ID di versione specifico.</p> <p>Al contrario, il servizio CloudMirror replica le richieste DI tagging DEGLI oggetti PUT o ELIMINA le richieste di tagging degli oggetti 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 multipart e. ETag valori	Quando si esegue il mirroring degli oggetti caricati utilizzando un caricamento multipart, il servizio CloudMirror non conserva le parti. Di conseguenza, il ETag il valore dell'oggetto mirrorato sarà diverso da ETag valore dell'oggetto originale.
Oggetti crittografati con SSE-C (crittografia lato server con chiavi fornite dal cliente)	Il servizio CloudMirror non supporta gli oggetti crittografati con SSE-C. Se si tenta di acquisire un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione non riesce.
Bucket con blocco oggetti S3 attivato	Se il bucket S3 di destinazione per la replica CloudMirror ha attivato il blocco oggetti S3, l'operazione di replica non riesce e viene visualizzato un errore AccessDenied.

#### Informazioni correlate

["Utilizzare S3"](#)

#### Configurazione degli endpoint dei servizi di 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 Manage Endpoints (Gestisci endpoint) o Root Access (accesso root), in una griglia la cui rete è stata configurata per consentire ai nodi di storage di accedere alle risorse esterne degli endpoint. Per ulteriori informazioni, contattare l'amministratore di StorageGRID.

## **Che cos'è un endpoint di servizi di piattaforma**

Quando si crea un endpoint di servizi di piattaforma, si specificano 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 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 AWS.

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 in modo che utilizzi più di un endpoint come destinazione, consentendo di eseguire operazioni come l'invio di notifiche sulla creazione di oggetti a un singolo argomento SNS e le notifiche sull'eliminazione di oggetti a un secondo argomento 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 SNS (Simple Notification Service). Gli endpoint SQS (Simple Queue Service) o AWS Lambda non sono supportati.

### **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"](#)

### **Specifiche dell'URN per un endpoint di servizi di piattaforma**

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

StorageGRID convalida gli endpoint dei servizi della piattaforma 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 URN

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

- Se il servizio è ospitato su AWS, utilizzare `arn:aws`.
- Se il servizio è ospitato localmente, utilizzare `urn:mysite`

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

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

Servizio	Tipo
Replica di CloudMirror	s3
Notifiche	sns
Integrazione della ricerca	es

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

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

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

## Urns per i servizi ospitati su AWS

Per le entità AWS, 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, il `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:

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

- Integrazione della ricerca:

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



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

## Creazione di un endpoint di servizi di piattaforma

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

servizio di piattaforma.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- I servizi della piattaforma devono essere abilitati per l'account tenant da un amministratore di StorageGRID.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione Gestisci endpoint.
- La risorsa a cui fa riferimento l'endpoint dei servizi della piattaforma deve essere stata creata:
  - Replica di CloudMirror: Bucket S3
  - Notifica evento: Argomento SNS
  - Notifica di ricerca: Indice Elasticsearch, se il cluster di destinazione non è configurato per creare automaticamente gli indici.
- È necessario disporre 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)

#### ["Specifica dell'URN per un endpoint di servizi di piattaforma"](#)

- Credenziali di autenticazione (se richieste):
  - Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key
  - HTTP di base: Nome utente e password
- Certificato di protezione (se si utilizza un certificato CA personalizzato)

#### Fasi

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

Viene visualizzata la pagina Platform Services Endpoint.

# Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

0 endpoints

[Create endpoint](#)

[Delete endpoint](#)

Display name [?](#) [▲](#)

Last error [?](#) [▲](#)

Type [?](#) [▲](#)

URI [?](#) [▲](#)

URN [?](#) [▲](#)

No endpoints found

[Create endpoint](#)

2. Selezionare **Crea endpoint**.

# Create endpoint

1 Enter details    2 Select authentication type    3 Verify server

Optional    Optional

## Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name ?

URI ?

URN ?

Cancel    Continue

3. Inserire un nome visualizzato per descrivere brevemente l'endpoint e il suo scopo.

Il tipo di servizio della piattaforma supportato dall'endpoint viene visualizzato accanto al nome dell'endpoint quando viene elencato nella pagina degli endpoint, quindi non è necessario includere tali informazioni 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, la porta 443 viene utilizzata per gli URI HTTPS e la porta 80 per gli URI HTTP.

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 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 **Authentication type** (tipo di autenticazione), quindi immettere le credenziali richieste.

**Create endpoint**

1 Enter details      2 Select authentication type      3 Verify server

**Authentication type**

Select the method used to authenticate connections to the endpoint.

Anonymous

Anonymous  
Access Key  
Basic HTTP

Previous

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"><li>• ID chiave di accesso</li><li>• Chiave di accesso segreta</li></ul>
HTTP di base	Utilizza un nome utente e una password per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none"><li>• Nome utente</li><li>• Password</li></ul>

8. Selezionare **continua**.
9. Selezionare un pulsante di opzione per **verify server** (verifica server) per scegliere la modalità di verifica della connessione TLS all'endpoint.

Create endpoint X

Enter details  Select authentication type 3  Verify server

**Verify server**

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate  Use operating system CA certificate  Do not verify certificate

-----BEGIN CERTIFICATE-----  
abcdefghijklmnopqrstuvwxyz0ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890ABCDEFHIGKLM  
1234567890ABCDEFabcdefghijklmnopqrstuvwxyz1234567890ABCDEFHIGKLM  
-----END CERTIFICATE-----

[Previous](#) [Test and create endpoint](#)

Tipo di verifica del certificato	Descrizione
USA certificato CA personalizzato	Utilizzare un certificato di protezione personalizzato. Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo <b>certificato CA</b> .
Utilizzare il certificato CA del sistema operativo	Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere le connessioni.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato. Questa opzione non è sicura.

## 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

["Specifica dell'URN per un endpoint di servizi di piattaforma"](#)

["Configurazione della replica di CloudMirror"](#)

["Configurazione delle notifiche degli eventi"](#)

["Configurazione del servizio di integrazione della ricerca"](#)

### Verifica della connessione per un endpoint di servizi di 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.

### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione Gestisci endpoint.

### 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.

# Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

[Create endpoint](#)

[Delete endpoint](#)

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

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

Viene visualizzata la pagina dei dettagli dell'endpoint.

## Overview ^

Display name:	<a href="#">my-endpoint-1</a> 
Type:	<b>S3 Bucket</b>
URI:	<a href="http://10.96.104.167:10443">http://10.96.104.167:10443</a>
URN:	<a href="#">urn:sgws:s3:::bucket1</a>

---

Connection Configuration

### Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

### 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 di un endpoint di servizi di 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.

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che dispone dell'autorizzazione Gestisci endpoint.

#### 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.

# Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints[Create endpoint](#)

[Delete endpoint](#)Display name?▲Last error?▲Type?▲URI?▲URN?▲

---

<input type="checkbox"/>	my-endpoint-1	S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/
<input type="checkbox"/>	my-endpoint-4	S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Selezionare l'endpoint che si desidera modificare.

Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Configurazione**.

## Overview

Display name:	my-endpoint-3 
Type:	Notifications
URI:	http://10.96.104.202:8080/
URN:	arn:aws:sns:us-west-2::example1

Connection

Configuration

## Edit configuration

### Endpoint details

URI 

http://10.96.104.202:8080/

URN 

arn:aws:sns:us-west-2::example1

### Authentication type

Basic HTTP

Username 

testme

Password 

\*\*\*\*\*

[Edit password](#)

### Verify server

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----  
abcdefghijklmnopqrstuvwxyz123456780ABCDEFGHIJKLM  
123456/7890ABCDEFGHIJKLM  
-----END CERTIFICATE-----
```

[Test and save changes](#)

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 visualizzato 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 HTTP di base, modificare il nome utente in base alle necessità. Modificare la password in base alle necessità selezionando **Modifica password** e immettendo la nuova password. Per annullare le modifiche, selezionare **Ripristina modifica password**.
  - 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**.
- d. Se necessario, modificare il metodo di verifica del server.

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**.

#### Informazioni correlate

["Creazione di un endpoint di servizi di piattaforma"](#)

#### Eliminazione di un endpoint dei servizi della piattaforma

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

#### Di cosa hai bisogno

- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti con l'autorizzazione **Gestisci endpoint**.

#### 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.

# Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

[Create endpoint](#)

[Delete endpoint](#)

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

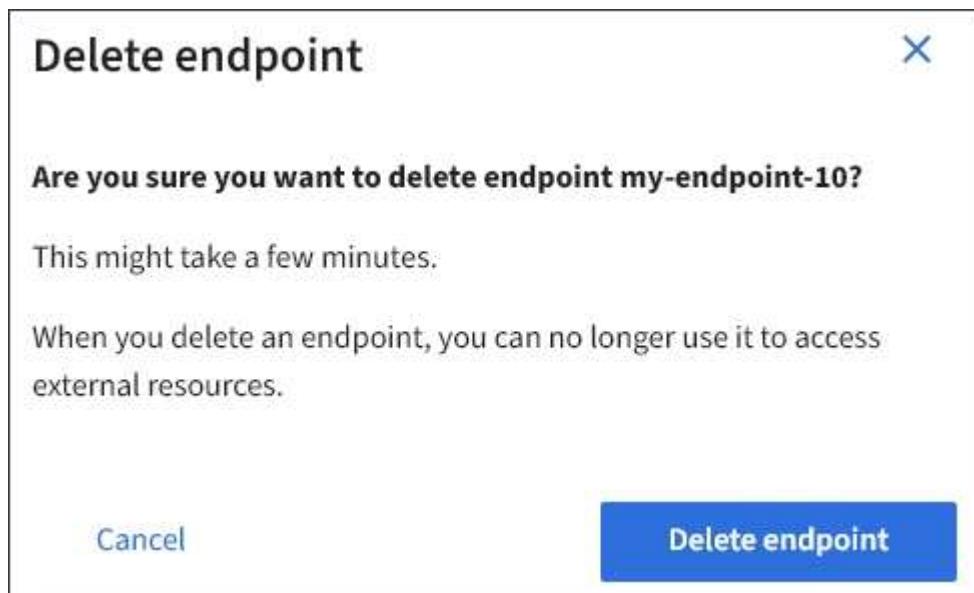
2. Selezionare la casella di controllo per ciascun endpoint che si desidera eliminare.



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 segnalera queste richieste come errori irrecuperabili.

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

Viene visualizzato un messaggio di conferma.



#### 4. Selezionare **Delete endpoint** (Elimina endpoint).

#### Risoluzione dei problemi relativi agli errori degli endpoint dei servizi della piattaforma

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi della piattaforma, viene visualizzato un messaggio nella dashboard. Nella pagina 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, il pannello di controllo 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. Errori che includono l'icona X rossa  si è verificato negli ultimi 7 giorni.

## Overview

Display name:	my-endpoint-2 
Type:	Search
URI:	http://10.96.104.30:9200
URN:	urn:sgws:es:::mydomain/sveloso/_doc

### Connection

### Configuration

## Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

 **Test connection**

### Last error details

 2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

## Verifica della presenza di un errore

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.

## Risoluzione degli 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 della piattaforma (ad esempio “403 Forbidden”), controllare le autorizzazioni associate alle credenziali dell'endpoint.

## Troubleshooting di servizi di piattaforma aggiuntivi

Per ulteriori informazioni sulla risoluzione dei problemi relativi ai servizi della piattaforma, consultare le istruzioni per l'amministrazione di StorageGRID.

### ["Amministrare StorageGRID"](#)

#### **Informazioni correlate**

["Creazione di un endpoint di servizi di piattaforma"](#)

["Verifica della connessione per un endpoint di servizi di piattaforma"](#)

["Modifica di un endpoint di servizi di piattaforma"](#)

## Configurazione della replica di CloudMirror

Il servizio di replica CloudMirror è uno dei tre servizi della piattaforma StorageGRID. È possibile utilizzare la replica CloudMirror per replicare automaticamente gli oggetti in un bucket S3 esterno.

### **Di cosa hai bisogno**

- I servizi della piattaforma devono essere abilitati per l'account tenant da un amministratore di StorageGRID.
- È necessario aver già creato un bucket per fungere da origine della replica.
- L'endpoint che si intende utilizzare come destinazione per la replica di CloudMirror deve già esistere ed è necessario disporre dell'URN.
- È necessario appartenere a un gruppo di utenti con l'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root), che consente di gestire le impostazioni di tutti i bucket S3

nell'account tenant. 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 attivare la replica CloudMirror per un bucket, è necessario creare e applicare un XML di configurazione valido per la replica del bucket. L'XML di configurazione della replica deve utilizzare l'URN di un endpoint del bucket S3 per ciascuna destinazione.



La replica non è supportata per i bucket di origine o di destinazione con blocco oggetti S3 attivato.

Per informazioni generali sulla replica bucket e su come configurarla, consultare la documentazione Amazon sulla replica cross-region (CRR). Per informazioni su come StorageGRID implementa l'API di configurazione della replica del bucket S3, vedere le istruzioni per l'implementazione delle applicazioni client S3.

Se si attiva la replica di CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket vengono replicati, ma gli oggetti esistenti nel bucket non lo sono. 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 di `Filter`. 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 si desidera, aggiungere `<StorageClass>` e specificare una delle seguenti opzioni:
  - **STANDARD**: La classe di storage predefinita. Se non si specifica una classe di storage quando si carica un oggetto, il **STANDARD** viene utilizzata la classe di storage.
  - **STANDARD\_IA**: (Standard - accesso non frequente). Utilizzare 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 storage per i dati non critici e riproducibili che possono essere memorizzati con una ridondanza inferiore rispetto a. **STANDARD** classe di storage.
- Se si specifica un `Role` nel file XML di configurazione, 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. 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 > 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).

Bucket options
Bucket access
Platform services

Replication
Disabled
^

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication
Clear

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

Save changes



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

["Informazioni sul servizio di replica CloudMirror"](#)

["Utilizzare S3"](#)

["Creazione di un endpoint di servizi di piattaforma"](#)

## Configurazione delle notifiche degli eventi

Il servizio di notifica è uno dei tre servizi della piattaforma StorageGRID. È possibile attivare le notifiche per un bucket per inviare informazioni su eventi specifici a un servizio di destinazione che supporta AWS Simple Notification Service™ (SNS).

### Di cosa hai bisogno

- I servizi della piattaforma devono essere abilitati per l'account tenant da un amministratore di StorageGRID.
- È necessario aver già creato un bucket per fungere da origine delle notifiche.
- L'endpoint che si intende utilizzare come destinazione per le notifiche degli eventi deve già esistere ed è necessario disporre dell'URN.
- È necessario appartenere a un gruppo di utenti con l'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root), che consente di gestire le impostazioni di tutti i bucket S3 nell'account tenant. 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 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 Simple Notification Service (SNS) utilizzato come endpoint di destinazione. Per attivare le notifiche per un bucket, è necessario creare e applicare un XML di configurazione delle notifiche valido. L'XML di configurazione delle notifiche deve utilizzare l'URN di un endpoint delle notifiche degli eventi per ciascuna destinazione.

Per informazioni generali sulle notifiche degli eventi e su come configurarle, consulta la documentazione Amazon. Per informazioni su come StorageGRID implementa l'API di configurazione delle notifiche del bucket S3, vedere le istruzioni per l'implementazione delle applicazioni client S3.

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 **Enable event notifications** (attiva notifiche eventi).

6. Incollare l'XML di configurazione della notifica nella casella di testo e selezionare **Salva modifiche**.

Bucket options
Bucket access
Platform services

Replication
Disabled
▼

Event notifications
Disabled
▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS).

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications
 Clear

```
<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>
```

Save changes

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.

98

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

b. Confermare che è stata inviata una notifica all'argomento SNS di destinazione.

Ad esempio, se l'argomento di destinazione è ospitato su AWS Simple Notification Service (SNS), è possibile configurare il servizio in modo che invii un'e-mail al momento dell'invio 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

["Informazioni sulle notifiche per i bucket"](#)

["Utilizzare S3"](#)

["Creazione di un endpoint di servizi di piattaforma"](#)

#### Utilizzando il servizio di integrazione della ricerca

Il servizio di integrazione della ricerca è uno dei tre servizi della piattaforma StorageGRID. È possibile consentire a questo servizio di inviare metadati di oggetti a un indice di ricerca della destinazione ogni volta che un oggetto viene creato, cancellato o i relativi metadati o tag vengono aggiornati.

È possibile configurare l'integrazione della ricerca utilizzando Gestione tenant per applicare XML di configurazione StorageGRID personalizzato a un bucket.



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 degli eventi.

Consultare le istruzioni per l'implementazione delle applicazioni client S3 per informazioni dettagliate sulle seguenti operazioni REST API personalizzate di StorageGRID S3:

- ELIMINA la richiesta di configurazione della notifica dei metadati del bucket
- OTTIENI una richiesta di configurazione per la notifica dei metadati del bucket
- INSERIRE la richiesta di configurazione della notifica dei metadati del bucket

#### Informazioni correlate

["XML di configurazione per l'integrazione della ricerca"](#)

["Metadati degli oggetti inclusi nelle notifiche dei metadati"](#)

["JSON generato dal servizio di integrazione della ricerca"](#)

["Configurazione del servizio di integrazione della ricerca"](#)

["Utilizzare S3"](#)

#### XML di configurazione per l'integrazione della ricerca

Il servizio di integrazione della ricerca viene configurato utilizzando una serie di regole contenute in `<MetadataNotificationConfiguration>` e `</MetadataNotificationConfiguration>` tag. Ogni regola specifica gli oggetti a cui si applica la regola e la destinazione in cui StorageGRID deve inviare i metadati di tali oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, è possibile inviare

metadati per oggetti con il prefisso `/images` a una destinazione e metadati per gli oggetti con il prefisso `/videos` a un altro. Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, una configurazione che include una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2` non consentito.

Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID creato per il servizio di integrazione della ricerca. Questi endpoint si riferiscono a un indice e a un tipo definiti in un cluster Elasticsearch.

```

<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
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

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"> <li>• es deve essere il terzo elemento.</li> <li>• L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form domain-name/myindex/mytype.</li> </ul> <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> <li>• arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>L'endpoint deve essere configurato prima 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

Utilizza l'XML di configurazione delle notifiche dei metadati di esempio per scoprire come creare il tuo XML.

### Configurazione della notifica dei metadati applicabile 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>

```

### Configurazione della notifica dei metadati con due regole

In questo esempio, i metadati degli oggetti per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti per gli oggetti che corrispondono al prefisso `/videos` viene inviato a una seconda destinazione.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

### Informazioni correlate

["Utilizzare S3"](#)

["JSON generato dal servizio di integrazione della ricerca"](#)

["Configurazione del servizio di integrazione della ricerca"](#)

## Configurazione del servizio di integrazione della ricerca

Il servizio di integrazione della ricerca invia i metadati degli oggetti a un indice di ricerca di destinazione ogni volta che un oggetto viene creato, cancellato o i relativi metadati o tag vengono aggiornati.

### Di cosa hai bisogno

- I servizi della piattaforma devono essere abilitati per l'account tenant da un amministratore di StorageGRID.
- È necessario aver già 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 deve già esistere ed è necessario disporre del relativo URN.
- È necessario appartenere a un gruppo di utenti con l'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root), che consente di gestire le impostazioni di tutti i bucket S3 nell'account tenant. 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 si attiva 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. È necessario aggiornare questi oggetti esistenti per assicurarsi che i relativi metadati vengano aggiunti all'indice di ricerca della destinazione.

### Fasi

1. Utilizzare un editor di testo per creare l'XML di notifica dei metadati necessario per abilitare l'integrazione della ricerca.
  - Per l'integrazione della ricerca, consultare le informazioni relative all'XML di configurazione.
  - Quando si configura l'XML, utilizzare l'URN di un endpoint di integrazione della ricerca come destinazione.

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

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**.

Bucket options Bucket access Platform services

Replication Disabled

Event notifications Disabled

Search integration Disabled

Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the search integration service.
- You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.

Enable search integration

Clear

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Save changes



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.

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

## Al termine

Se necessario, è possibile disattivare l'integrazione della ricerca per un bucket utilizzando uno dei seguenti metodi:

- Selezionare **STORAGE (S3) > Bucket** e deselezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).
- Se si utilizza direttamente l'API S3, utilizzare una richiesta DI notifica DELETE Bucket metadata. Consultare le istruzioni per l'implementazione delle applicazioni client S3.

## Informazioni correlate

["Informazioni sul servizio di integrazione della ricerca"](#)

["XML di configurazione per l'integrazione della ricerca"](#)

["Utilizzare S3"](#)

["Creazione di un endpoint di servizi di piattaforma"](#)

## 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. Il test bucket non è configurato, quindi il versionId tag vuoto.

```
{
  "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 e descrizione dell'elemento
Informazioni su bucket e oggetti	bucket: Nome del bucket
key: Nome chiave oggetto	versionID: Versione oggetto, per gli oggetti nei bucket con 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 di oggetto
Metadati dell'utente	metadata: Tutti i metadati dell'utente per l'oggetto, come coppie chiave-valore key:value
Tag	tags: Tutti i tag di oggetto definiti per l'oggetto, come coppie chiave-valore key:value



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.

## Utilizzare S3

Scopri come le applicazioni client possono utilizzare l'API S3 per interfacciarsi con il sistema StorageGRID.

- ["Supporto per l'API REST S3"](#)
- ["Configurazione di account e connessioni tenant"](#)
- ["Come StorageGRID implementa l'API REST S3"](#)
- ["Operazioni e limitazioni supportate dall'API REST S3"](#)
- ["Operazioni REST API di StorageGRID S3"](#)
- ["Policy di accesso a bucket e gruppi"](#)
- ["Configurazione della sicurezza per l'API REST"](#)
- ["Operazioni di monitoraggio e controllo"](#)
- ["Vantaggi delle connessioni HTTP attive, inattive e simultanee"](#)

### Supporto per l'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. Ciò richiede modifiche minime all'utilizzo corrente delle chiamate API REST S3 da parte di un'applicazione client.

- ["Modifiche al supporto delle API REST S3"](#)
- ["Versioni supportate"](#)
- ["Supporto per i servizi della piattaforma StorageGRID"](#)

### Modifiche al supporto delle API REST S3

È necessario essere consapevoli delle modifiche apportate al supporto del sistema StorageGRID per l'API REST S3.

Rilasciare	Commenti
11.5	<ul style="list-style-type: none"> <li>• Aggiunto supporto per la gestione della crittografia bucket.</li> <li>• Aggiunto supporto per S3 Object Lock e richieste legacy di Compliance obsolete.</li> <li>• Aggiunto il supporto per l'utilizzo DELL'ELIMINAZIONE di più oggetti nei bucket con versione.</li> <li>• Il Content-MD5 l'intestazione della richiesta è ora supportata correttamente.</li> </ul>
11.4	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Aggiunto supporto per le notifiche bucket su s3:ObjectRestore:Post tipo di evento.</li> <li>• I limiti di dimensione AWS per le parti multipart vengono ora applicati. Ogni parte di un caricamento multipart deve essere compresa tra 5 MiB e 5 GiB. L'ultima parte può essere inferiore a 5 MiB.</li> <li>• Aggiunto il supporto per TLS 1.3 e aggiornato l'elenco delle suite di crittografia TLS supportate.</li> <li>• Il servizio CLB è obsoleto.</li> </ul>
11.3	<ul style="list-style-type: none"> <li>• Aggiunto supporto per la crittografia lato server dei dati a oggetti con chiavi fornite dal cliente (SSE-C).</li> <li>• Supporto aggiunto per LE operazioni DI eliminazione, GET e PUT del ciclo di vita del bucket (solo azione di scadenza) e per x-amz-expiration intestazione della risposta.</li> <li>• 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.</li> <li>• Elenco aggiornato delle suite di crittografia TLS supportate. Le crittografia TLS 1.1 non sono più supportate.</li> </ul>

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><b>Nota:</b> gli utilizzi di ARN/URN in altre configurazioni JSON/XML, inclusi quelli utilizzati nelle funzionalità personalizzate di StorageGRID, non sono cambiati.</p>
11.1	<p>Aggiunto supporto per Cross-Origin Resource Sharing (CORS), HTTP per connessioni client S3 ai nodi di rete e impostazioni di conformità sui bucket.</p>
11.0	<p>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 per il tag degli oggetti per i bucket e l'impostazione di controllo della coerenza disponibile.</p>
10.4	<p>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.</p>
10.3	<p>Aggiunto supporto per il controllo delle versioni.</p>
10.2	<p>Aggiunto supporto per policy di accesso di gruppo e bucket e per copia multiparte (carica parte - Copia).</p>
10.1	<p>Aggiunto supporto per upload multiparte, richieste virtuali in stile host e autenticazione v4.</p>
10.0	<p>Supporto iniziale dell'API REST S3 da parte del sistema StorageGRID. La versione attualmente supportata del <i>riferimento API del servizio di storage semplice</i> è 2006-03-01.</p>

## Versioni supportate

StorageGRID supporta le seguenti versioni specifiche di S3 e HTTP.

Elemento	Versione
Specifiche S3	Riferimento API Simple Storage Service 2006-03-01
HTTP	<p>1.1</p> <p>Per ulteriori informazioni su HTTP, vedere HTTP/1.1 (RFC 7230-35).</p> <p><b>Nota:</b> StorageGRID non supporta la pipelining HTTP/1.1.</p>

#### Informazioni correlate

["IETF RFC 2616: Protocollo di trasferimento ipertestuale \(HTTP/1.1\)"](#)

["Documentazione Amazon Web Services \(AWS\): Riferimento API Amazon Simple Storage Service"](#)

#### Supporto per i servizi della piattaforma StorageGRID

I servizi della piattaforma StorageGRID consentono agli account tenant StorageGRID di sfruttare servizi esterni come un bucket S3 remoto, un endpoint SNS (Simple Notification Service) o un cluster Elasticsearch per estendere i servizi forniti da un grid.

Nella tabella seguente sono riepilogati i servizi della piattaforma disponibili e le API S3 utilizzate per configurarli.

Servizio di piattaforma	Scopo	S3 API utilizzata per configurare il servizio
Replica di CloudMirror	Replica gli oggetti da un bucket StorageGRID di origine al bucket S3 remoto configurato.	METTI la replica del bucket
Notifiche	Invia notifiche sugli eventi in un bucket StorageGRID di origine a un endpoint configurato per il servizio di notifica semplice (SNS).	NOTIFICA DEL bucket
Integrazione della ricerca	Invia i metadati degli oggetti memorizzati in un bucket StorageGRID a un indice Elasticsearch configurato.	<p>METTI la notifica dei metadati del bucket</p> <p><b>Nota:</b> questa è un'API S3 personalizzata di StorageGRID.</p>

Un amministratore di grid deve abilitare l'utilizzo dei servizi della piattaforma per un account tenant prima di poter essere utilizzati. Quindi, un amministratore del tenant deve creare un endpoint che rappresenti il servizio remoto nell'account tenant. Questa fase è necessaria prima di poter configurare un servizio.

## Consigli per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, è necessario conoscere i seguenti consigli:

- NetApp consiglia di non consentire più di 100 tenant attivi con richieste S3 che richiedono la replica CloudMirror, le notifiche e l'integrazione della ricerca. La presenza di più di 100 tenant attivi può rallentare le performance del client S3.
- Se un bucket S3 nel sistema StorageGRID ha attivato sia la versione che la replica CloudMirror, NetApp consiglia di abilitare anche il controllo delle versioni del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica di CloudMirror di generare versioni di oggetti simili sull'endpoint.
- La replica di CloudMirror non è supportata se il bucket di origine ha attivato il blocco oggetti S3.
- La replica di CloudMirror non riesce e viene visualizzato un errore AccessDenied se nel bucket di destinazione è attivata la conformità legacy.

## Informazioni correlate

["Utilizzare un account tenant"](#)

["Amministrare StorageGRID"](#)

["Operazioni sui bucket"](#)

["INSERIRE la richiesta di configurazione della notifica dei metadati del bucket"](#)

## Configurazione di account e connessioni tenant

La configurazione di StorageGRID per accettare connessioni da applicazioni client richiede la creazione di uno o più account tenant e la configurazione delle connessioni.

### Creazione e configurazione di account tenant S3

È necessario un account tenant S3 prima che i client API S3 possano memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant dispone di un proprio ID account, di gruppi e utenti, nonché di container e oggetti.

Gli account del tenant S3 vengono creati da un amministratore del grid StorageGRID utilizzando l'API Gestione griglia o Gestione griglia. Quando si crea un account tenant S3, l'amministratore della griglia specifica le seguenti informazioni:

- Nome visualizzato per il tenant (l'ID account del tenant viene assegnato automaticamente e non può essere modificato).
- Se l'account tenant è autorizzato a utilizzare i servizi della piattaforma. Se è consentito l'utilizzo dei servizi della piattaforma, la griglia deve essere configurata per supportarne l'utilizzo.
- Facoltativamente, una quota di storage per l'account tenant, ovvero il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant. La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).
- Se la federazione delle identità è attivata per il sistema StorageGRID, il gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant.
- Se l'SSO (Single Sign-on) non è in uso per il sistema StorageGRID, se l'account tenant utilizzerà la propria origine di identità o condividerà l'origine di identità della griglia e la password iniziale per l'utente root locale del tenant.

Una volta creato un account tenant S3, gli utenti tenant possono accedere a tenant Manager per eseguire attività come le seguenti:

- Impostare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) e creare gruppi e utenti locali
- Gestire le chiavi di accesso S3
- Crea e gestisci i bucket S3, inclusi i bucket che hanno attivato il blocco oggetti S3
- Utilizzo dei servizi della piattaforma (se abilitati)
- Monitorare l'utilizzo dello storage



Gli utenti del tenant S3 possono creare e gestire i bucket S3 con Tenant Manager, ma devono disporre di chiavi di accesso S3 e utilizzare l'API REST S3 per acquisire e gestire gli oggetti.

## Informazioni correlate

["Amministrare StorageGRID"](#)

["Utilizzare un account tenant"](#)

## Come configurare le connessioni client

Un amministratore di grid effettua scelte di configurazione che influiscono sul modo in cui i client S3 si connettono a StorageGRID per memorizzare e recuperare i dati. Le informazioni specifiche necessarie per effettuare una connessione dipendono dalla configurazione scelta.

Le applicazioni client possono memorizzare o recuperare oggetti connettendosi a una delle seguenti opzioni:

- Il servizio Load Balancer sui nodi Admin o Gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità (ha) di nodi Admin o nodi Gateway
- Il servizio CLB sui nodi gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità di nodi gateway



Il servizio CLB è obsoleto. I client configurati prima della release StorageGRID 11.3 possono continuare a utilizzare il servizio CLB sui nodi gateway. Tutte le altre applicazioni client che dipendono da StorageGRID per fornire il bilanciamento del carico devono connettersi utilizzando il servizio bilanciamento del carico.

- Nodi di storage, con o senza bilanciamento del carico esterno

Durante la configurazione di StorageGRID, un amministratore della griglia può utilizzare il gestore della griglia o l'API di gestione della griglia per eseguire le seguenti operazioni, tutte facoltative:

### 1. Configurare gli endpoint per il servizio Load Balancer.

È necessario configurare gli endpoint per utilizzare il servizio Load Balancer. Il servizio Load Balancer sui nodi di amministrazione o gateway distribuisce le connessioni di rete in entrata dalle applicazioni client ai nodi di storage. Quando si crea un endpoint di bilanciamento del carico, l'amministratore di StorageGRID specifica un numero di porta, se l'endpoint accetta connessioni HTTP o HTTPS, il tipo di client (S3 o Swift) che utilizzerà l'endpoint e il certificato da utilizzare per le connessioni HTTPS (se applicabile).

### 2. Configurare reti client non attendibili.

Se un amministratore di StorageGRID configura una rete client di un nodo come non attendibile, il nodo

accetta solo connessioni in entrata sulla rete client su porte esplicitamente configurate come endpoint del bilanciamento del carico.

### 3. Configurare i gruppi ad alta disponibilità.

Se un amministratore crea un gruppo ha, le interfacce di rete di più nodi Admin o nodi Gateway vengono inserite in una configurazione di backup attivo. Le connessioni client vengono effettuate utilizzando l'indirizzo IP virtuale del gruppo ha.

Per ulteriori informazioni su ciascuna opzione, consultare le istruzioni per l'amministrazione di StorageGRID.

#### Informazioni correlate

["Amministrare StorageGRID"](#)

#### Riepilogo: Indirizzi IP e porte per le connessioni client

Le applicazioni client si connettono a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta di un servizio su tale nodo. Se sono configurati gruppi ad alta disponibilità (ha), le applicazioni client possono connettersi utilizzando l'indirizzo IP virtuale del gruppo ha.

#### Informazioni necessarie per stabilire connessioni client

La tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Per ulteriori informazioni, contattare l'amministratore di StorageGRID oppure consultare le istruzioni per l'amministrazione di StorageGRID per una descrizione di come trovare queste informazioni in Gestione griglia.

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Gruppo HA	Bilanciamento del carico	Indirizzo IP virtuale di un gruppo ha	<ul style="list-style-type: none"><li>• Porta endpoint del bilanciamento del carico</li></ul>
Gruppo HA	CLB <b>Nota:</b> il servizio CLB è obsoleto.	Indirizzo IP virtuale di un gruppo ha	Porte S3 predefinite: <ul style="list-style-type: none"><li>• HTTPS: 8082</li><li>• HTTP: 8084</li></ul>
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	<ul style="list-style-type: none"><li>• Porta endpoint del bilanciamento del carico</li></ul>
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	<ul style="list-style-type: none"><li>• Porta endpoint del bilanciamento del carico</li></ul>

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Nodo gateway	CLB  <b>Nota:</b> il servizio CLB è obsoleto.	Indirizzo IP del nodo gateway  <b>Nota:</b> per impostazione predefinita, le porte HTTP per CLB e LDR non sono attivate.	Porte S3 predefinite: <ul style="list-style-type: none"> <li>HTTPS: 8082</li> <li>HTTP: 8084</li> </ul>
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte S3 predefinite: <ul style="list-style-type: none"> <li>HTTPS: 18082</li> <li>HTTP: 18084</li> </ul>

## Esempio

Per connettere un client S3 all'endpoint Load Balancer di un gruppo ha di nodi gateway, utilizzare un URL strutturato come mostrato di seguito:

- `https://VIP-of-HA-group:_LB-endpoint-port_`

Ad esempio, se l'indirizzo IP virtuale del gruppo ha è 192.0.2.5 e il numero di porta di un endpoint di bilanciamento del carico S3 è 10443, un client S3 potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.5:10443`

È possibile configurare un nome DNS per l'indirizzo IP utilizzato dai client per la connessione a StorageGRID. Contattare l'amministratore di rete locale.

## Informazioni correlate

["Amministrare StorageGRID"](#)

### Scelta dell'utilizzo di connessioni HTTPS o HTTP

Quando le connessioni client vengono eseguite utilizzando un endpoint Load Balancer, le connessioni devono essere effettuate utilizzando il protocollo (HTTP o HTTPS) specificato per tale endpoint. Per utilizzare HTTP per le connessioni client ai nodi di storage o al servizio CLB sui nodi gateway, è necessario abilitarne l'utilizzo.

Per impostazione predefinita, quando le applicazioni client si connettono ai nodi di storage o al servizio CLB sui nodi gateway, devono utilizzare HTTPS crittografato per tutte le connessioni. In alternativa, è possibile attivare connessioni HTTP meno sicure selezionando l'opzione **Enable HTTP Connection** grid (attiva connessione HTTP) in Grid Manager. Ad esempio, un'applicazione client potrebbe utilizzare il protocollo HTTP quando si verifica la connessione a un nodo di storage in un ambiente non di produzione.



Prestare attenzione quando si attiva HTTP per una griglia di produzione, poiché le richieste verranno inviate senza crittografia.



Il servizio CLB è obsoleto.

Se l'opzione **Enable HTTP Connection** (attiva connessione HTTP) è selezionata, i client devono utilizzare porte diverse per HTTP rispetto a quelle utilizzate per HTTPS. Consultare le istruzioni per l'amministrazione di StorageGRID.

#### Informazioni correlate

["Amministrare StorageGRID"](#)

["Vantaggi delle connessioni HTTP attive, inattive e simultanee"](#)

#### Nomi di dominio degli endpoint per le richieste S3

Prima di poter utilizzare i nomi di dominio S3 per le richieste dei client, un amministratore di StorageGRID deve configurare il sistema in modo che accetti le connessioni che utilizzano i nomi di dominio S3 nelle richieste in stile percorso S3 e in quelle in stile host virtuale S3.

#### A proposito di questa attività

Per consentire l'utilizzo delle richieste di stile in hosting virtuale S3, un amministratore di grid deve eseguire le seguenti attività:

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID.
- Assicurarsi che il certificato utilizzato dal client per le connessioni HTTPS a StorageGRID sia firmato per tutti i nomi di dominio richiesti dal client.

Ad esempio, se l'endpoint è `s3.company.com`, L'amministratore della griglia deve assicurarsi che il certificato utilizzato per le connessioni HTTPS includa `s3.company.com` Endpoint e SAN (Subject Alternative Name) con caratteri jolly dell'endpoint: `*.s3.company.com`.

- Configurare il server DNS utilizzato dal client per includere i record DNS che corrispondono ai nomi di dominio degli endpoint, inclusi i record con caratteri jolly richiesti.

Se il client si connette utilizzando il servizio Load Balancer, il certificato configurato dall'amministratore della griglia è il certificato per l'endpoint del bilanciamento del carico utilizzato dal client.



Ogni endpoint di bilanciamento del carico dispone di un proprio certificato e ciascun endpoint può essere configurato in modo da riconoscere nomi di dominio degli endpoint diversi.

Se il client connette i nodi di storage o al servizio CLB sui nodi gateway, il certificato configurato dall'amministratore della griglia è il singolo certificato server personalizzato utilizzato per la griglia.



Il servizio CLB è obsoleto.

Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

Una volta completate queste fasi, è possibile utilizzare richieste virtuali in stile host (ad esempio, `bucket.s3.company.com`).

#### Informazioni correlate

["Amministrare StorageGRID"](#)

["Configurazione della sicurezza per l'API REST"](#)

## Verifica della configurazione dell'API REST S3

È possibile utilizzare l'interfaccia della riga di comando di Amazon Web Services (AWS CLI) per verificare la connessione al sistema e la possibilità di leggere e scrivere oggetti nel sistema.

### Di cosa hai bisogno

- È necessario aver scaricato e installato la CLI AWS da ["aws.amazon.com/cli"](https://aws.amazon.com/cli).
- È necessario aver creato un account tenant S3 nel sistema StorageGRID.

### Fasi

1. Configurare le impostazioni dei servizi Web Amazon per utilizzare l'account creato nel sistema StorageGRID:
  - a. Accedere alla modalità di configurazione: `aws configure`
  - b. Inserire l'ID della chiave di accesso AWS per l'account creato.
  - c. Immettere la chiave di accesso segreta AWS 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.

```
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

Un'applicazione client può utilizzare le chiamate API REST S3 per connettersi a StorageGRID per creare, eliminare e modificare i bucket, oltre a memorizzare e recuperare oggetti.

- ["Richieste client in conflitto"](#)
- ["Controlli di coerenza"](#)
- ["Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID"](#)
- ["Versione degli oggetti"](#)
- ["Raccomandazioni per l'implementazione dell'API REST S3"](#)

### Richieste client in conflitto

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle “ultime vittorie”.

La tempistica per la valutazione “ultimi successi” si basa su quando il sistema StorageGRID completa una data richiesta e non su quando i client S3 iniziano un’operazione.

### Controlli di coerenza

I controlli di coerenza offrono un compromesso tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage, come richiesto dall'applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET che segue UN PUT completato con successo sarà in grado di leggere i dati appena scritti. Le sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni sono coerenti. Le sovrascritture in genere richiedono secondi o minuti per la propagazione, ma possono richiedere fino a 15 giorni.

Se si desidera eseguire operazioni a oggetti a un livello di coerenza diverso, è possibile specificare un controllo di coerenza per ciascun bucket o per ciascuna operazione API.

### Controlli di coerenza

Il controllo della coerenza influisce sul modo in cui i metadati utilizzati da StorageGRID per tenere traccia degli oggetti vengono distribuiti tra i nodi e, di conseguenza, sulla disponibilità degli oggetti per le richieste dei client.

È possibile impostare il controllo di coerenza per un bucket o un'operazione API su uno dei seguenti valori:

Controllo della 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	<p>(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. Corrisponde alle garanzie di coerenza di Amazon S3.</p> <p><b>Nota:</b> se l'applicazione utilizza richieste HEAD su oggetti che non esistono, potrebbe essere visualizzato un numero elevato di errori 500 interni del server se uno o più nodi di storage non sono disponibili. Per evitare questi errori, imposta il controllo di coerenza su "Available", a meno che non necessiti di garanzie di coerenza simili a Amazon S3.</p>
Disponibile (eventuale coerenza per le operazioni TESTA)	Si comporta come il livello di coerenza "read-after-new-write", ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a "read-after-new-write" se i nodi storage non sono disponibili. Differisce dalle garanzie di coerenza di Amazon S3 solo per le operazioni HEAD.

#### Utilizzando i controlli di coerenza "read-after-new-write" e "available"

Quando un'operazione HEAD o GET utilizza il controllo di coerenza "read-after-new-write" o un'operazione GET utilizza il controllo di coerenza "Available", 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 livello di coerenza successivo fino a raggiungere il livello di coerenza più elevato, "all," che richiede la disponibilità di tutte le copie dei metadati dell'oggetto.

Se un'operazione HEAD o GET utilizza il controllo di coerenza "read-after-new-write" ma l'oggetto non esiste, la ricerca dell'oggetto raggiungerà sempre il livello di coerenza "all". Poiché questo livello di coerenza richiede la disponibilità di tutte le copie dei metadati dell'oggetto, è possibile ricevere un numero elevato di errori 500 interni del server se uno o più nodi di storage non sono disponibili.

A meno che non necessiti di garanzie di coerenza simili a Amazon S3, puoi evitare questi errori per le operazioni HEAD impostando il controllo di coerenza su "Available". Quando un'operazione HEAD utilizza il controllo di coerenza "Available", StorageGRID fornisce solo la coerenza finale. Non ritenta un'operazione non

riuscita fino a quando non raggiunge il livello di coerenza “all”, quindi non richiede la disponibilità di tutte le copie dei metadati dell’oggetto.

#### Specifiche del controllo di coerenza per un’operazione API

Per impostare il controllo di coerenza per una singola operazione API, i controlli di coerenza devono essere supportati per l’operazione e occorre specificare il controllo di coerenza nell’intestazione della richiesta. Questo esempio imposta il controllo di coerenza su “strong-site” per un’operazione GET Object.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```



È necessario utilizzare lo stesso controllo di coerenza per le operazioni PUT object e GET object.

#### Specifiche del controllo di coerenza per un bucket

Per impostare il controllo di coerenza per il bucket, è possibile utilizzare la richiesta di coerenza PUT bucket StorageGRID e LA richiesta di coerenza GET bucket. In alternativa, puoi utilizzare l’API di gestione tenant o tenant Manager.

Quando si impostano i controlli di coerenza per un bucket, tenere presente quanto segue:

- L’impostazione del controllo di coerenza per un bucket determina quale controllo di coerenza viene utilizzato per le operazioni S3 eseguite sugli oggetti nel bucket o sulla configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- Il controllo di coerenza per una singola operazione API sovrascrive il controllo di coerenza per il bucket.
- In generale, i bucket devono utilizzare il controllo di coerenza predefinito, “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 il controllo di coerenza per ogni richiesta API. Impostare il controllo di coerenza a livello di bucket solo come ultima risorsa.

#### Come interagiscono i controlli di coerenza e le regole ILM per influire sulla protezione dei dati

La scelta del controllo di coerenza e la regola ILM influiscono sulla modalità di protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, il controllo di coerenza utilizzato quando un oggetto viene memorizzato influisce sul posizionamento iniziale dei metadati dell’oggetto, mentre il comportamento di acquisizione selezionato per la regola ILM influisce sul posizionamento iniziale delle copie dell’oggetto. Poiché StorageGRID richiede l’accesso sia ai metadati di un oggetto che ai suoi dati per soddisfare le richieste dei client, la selezione dei livelli di protezione corrispondenti per il livello di coerenza e il comportamento di acquisizione può fornire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Strict:** Tutte le copie specificate nella regola ILM devono essere eseguite prima che il client sia riuscito.

- **Balanced:** StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono eseguite copie temporanee e viene restituito il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.
- **Doppio commit:** StorageGRID esegue immediatamente copie temporanee dell'oggetto e restituisce il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.



Prima di selezionare il comportamento di acquisizione per una regola ILM, leggere la descrizione completa di queste impostazioni nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

#### Esempio di come il controllo di coerenza e la regola ILM possono interagire

Si supponga di disporre di una griglia a due siti con la seguente regola ILM e la seguente impostazione del livello di coerenza:

- **ILM rule:** Creare due copie di oggetti, una nel sito locale e una in un sito remoto. Viene selezionato il comportamento rigoroso dell'acquisizione.
- **Livello di coerenza:** "strong-Global" (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie degli oggetti e distribuisce i metadati a entrambi i siti prima di restituire il risultato al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione del messaggio di successo. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, le copie dei dati dell'oggetto e dei metadati dell'oggetto rimangono nel sito remoto. L'oggetto è completamente recuperabile.

Se invece sono state utilizzate la stessa regola ILM e il livello di coerenza "strong-site", il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati nella sitqe remota, ma prima che i metadati dell'oggetto siano distribuiti in essa. 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 poco dopo l'acquisizione, i metadati dell'oggetto andranno persi. Impossibile recuperare l'oggetto.

L'interconnessione tra i livelli di coerenza e le regole ILM può essere complessa. Contattare NetApp per assistenza.

#### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["OTTIENI una richiesta di coerenza bucket"](#)

["INSERIRE la richiesta di coerenza del bucket"](#)

#### Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID

L'amministratore del grid crea regole ILM (Information Lifecycle Management) per gestire i dati degli oggetti acquisiti nel sistema StorageGRID dalle applicazioni client API REST S3. Queste regole vengono quindi aggiunte al criterio ILM per determinare come e dove i dati degli oggetti vengono memorizzati nel tempo.

Le impostazioni ILM determinano i seguenti aspetti di un oggetto:

- **Geografia**

La posizione dei dati di un oggetto, all'interno del sistema StorageGRID (pool di storage) o in un pool di storage cloud.

- **Grado di storage**

Il tipo di storage utilizzato per memorizzare i dati dell'oggetto, ad esempio flash o disco rotante.

- **Protezione contro le perdite**

Quante copie vengono eseguite e i tipi di copie create: Replica, erasure coding o entrambe.

- **Conservazione**

Il cambia nel tempo in base alla modalità di gestione dei dati di un oggetto, alla posizione in cui sono memorizzati e al modo in cui sono protetti dalla perdita.

- **Protezione durante l'acquisizione**

Metodo utilizzato per proteggere i dati degli oggetti durante l'acquisizione: Posizionamento sincrono (utilizzando le opzioni bilanciate o rigide per il comportamento di Ingest) o creazione di copie intermedie (utilizzando l'opzione Dual Commit).

Le regole ILM possono filtrare e selezionare gli oggetti. Per gli oggetti acquisiti tramite S3, le regole ILM possono filtrare gli oggetti in base ai seguenti metadati:

- Account tenant
- Nome bucket
- Tempo di acquisizione
- Chiave
- Ora ultimo accesso



Per impostazione predefinita, gli aggiornamenti dell'ultimo tempo di accesso sono disattivati per tutti i bucket S3. Se il sistema StorageGRID include una regola ILM che utilizza l'opzione ultimo tempo di accesso, è necessario abilitare gli aggiornamenti per l'ultimo tempo di accesso per i bucket S3 specificati in tale regola. È possibile attivare gli ultimi aggiornamenti del tempo di accesso utilizzando la richiesta PUT Bucket Last Access Time (INSERISCI ultima ora di accesso bucket), la casella di controllo **S3 > Bucket > Configure Last Access Time** (Configura ultima ora di accesso) in Tenant Manager o l'API di gestione tenant. Quando si abilitano gli ultimi aggiornamenti del tempo di accesso, tenere presente che le prestazioni di StorageGRID potrebbero essere ridotte, soprattutto nei sistemi con oggetti di piccole dimensioni.

- Vincolo di posizione
- Dimensione oggetto
- Metadati dell'utente
- Tag oggetto

Per ulteriori informazioni su ILM, vedere le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

## Informazioni correlate

["Utilizzare un account tenant"](#)

["Gestire gli oggetti con ILM"](#)

["METTI richiesta dell'ultimo tempo di accesso al bucket"](#)

## Versione degli oggetti

È possibile utilizzare il controllo delle versioni per conservare più versioni di un oggetto, che protegge dall'eliminazione 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 1,000 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. Per attivare questa funzionalità per il bucket, è necessario abilitare esplicitamente il controllo delle versioni per ciascun bucket. A ciascun oggetto del bucket viene assegnato un ID di versione, 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 il controllo delle versioni, il supporto delle versioni consente di creare regole ILM che utilizzano l'ora non corrente come tempo di riferimento. Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. L'utilizzo di un filtro orario non corrente consente di creare policy che riducono l'impatto sullo storage delle versioni precedenti degli 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.

Vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni per un esempio di policy ILM per gli oggetti con versione S3.

## Informazioni correlate

["Gestire gli oggetti con ILM"](#)

## 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 l'applicazione verifica regolarmente l'esistenza di un oggetto in un percorso in cui non si prevede l'effettiva esistenza dell'oggetto, utilizzare il controllo di coerenza "Available". Ad esempio, è necessario utilizzare il controllo di coerenza "Available" se l'applicazione dirige una posizione prima DI INSERIRVI.

In caso contrario, se l'operazione HEAD non trova l'oggetto, potrebbe essere visualizzato un numero elevato di errori 500 nel server interno se uno o più nodi di storage non sono disponibili.

È possibile impostare il controllo di coerenza "Available" per ciascun bucket utilizzando LA richiesta di coerenza PUT bucket oppure specificare il controllo di coerenza nell'intestazione della richiesta per una singola operazione API.

### Raccomandazioni per le chiavi a oggetti

Per i bucket creati in StorageGRID 11.4 o versioni successive, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. Ad esempio, è ora possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi oggetto.

Per i bucket creati in release precedenti a StorageGRID 11.4, continuare a seguire questi consigli per i nomi delle chiavi degli oggetti:

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi oggetto. Ciò è in contrasto con la precedente raccomandazione AWS per i prefissi principali. Si consiglia invece di utilizzare 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, è necessario anteporre le chiavi oggetto a un nome di directory. Ovvero, utilizzare questo formato:

```
mybucket/mydir/f8e3-image3132.jpg
```

Invece di questo formato:

```
mybucket/f8e3-image3132.jpg
```

### Raccomandazioni per "range reads"

Se l'opzione **compress stored objects** è selezionata (**Configuration > Grid Options**), le applicazioni client S3 dovrebbero evitare di eseguire operazioni GET object che specificano la restituzione di un intervallo di byte. Queste operazioni "range Read" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. LE operazioni GET Object che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è molto 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.

## Informazioni correlate

["Controlli di coerenza"](#)

["INSERIRE la richiesta di coerenza del bucket"](#)

["Amministrare StorageGRID"](#)

## Operazioni e limitazioni supportate dall'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.

- ["Autenticare le richieste"](#)
- ["Operazioni sul servizio"](#)
- ["Operazioni sui bucket"](#)
- ["Operazioni personalizzate sui bucket"](#)
- ["Operazioni sugli oggetti"](#)
- ["Operazioni per caricamenti multipart"](#)
- ["Risposte agli errori"](#)

## 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 `x-amz-date` Intestazione nella richiesta, sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza la firma AWS versione 4, il `x-amz-date` l'intestazione deve essere presente nella richiesta firmata perché l'intestazione della data non è supportata.

## Intestazioni di richiesta comuni

Il sistema StorageGRID supporta intestazioni di richiesta comuni definite dal *riferimento API del servizio di storage semplice*, con un'eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	<p>Supporto completo per firma AWS versione 2</p> <p>Supporto per firma AWS versione 4, con le seguenti eccezioni:</p> <ul style="list-style-type: none"> <li>Il valore SHA256 non viene calcolato per il corpo della richiesta. Il valore inviato dall'utente viene accettato senza convalida, come se il valore UNSIGNED-PAYLOAD è stato fornito per <code>x-amz-content-sha256</code> intestazione.</li> </ul>
<code>x-amz-security-token</code>	Non implementato. Ritorno <code>XNotImplemented</code> .

## Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite dal *riferimento API del servizio di storage semplice*, con un'eccezione.

Intestazione della risposta	Implementazione
<code>x-amz-id-2</code>	Non utilizzato

## Informazioni correlate

["Documentazione Amazon Web Services \(AWS\): Riferimento API Amazon Simple Storage Service"](#)

## 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: `HTTP Authorization` intestazione e utilizzo dei parametri di query.

### Utilizzo dell'intestazione autorizzazione HTTP

Il protocollo `HTTP Authorization` Header viene utilizzato da tutte le operazioni API S3, ad eccezione delle richieste anonime, laddove consentito dalla policy bucket. Il `Authorization` header contiene tutte le informazioni di firma richieste per autenticare una richiesta.

### Utilizzo dei 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 terzi.

## Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
OTTIENI assistenza	Implementato con tutti i comportamenti REST API di Amazon S3.
OTTIENI l'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. Si tratta di un'operazione sul servizio con un percorso di / e un parametro di query personalizzato (?x-ntap-sg-usage) aggiunto.
OPZIONI /	Le applicazioni client possono avere problemi OPTIONS / Richiede alla porta S3 su un nodo di storage, senza fornire credenziali di autenticazione S3, di determinare se il nodo di storage 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.

### Informazioni correlate

["OTTIENI la richiesta di utilizzo dello storage"](#)

## Operazioni sui bucket

Il sistema StorageGRID supporta un massimo di 1,000 bucket per ciascun account tenant S3.

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.

["Documentazione di Amazon Web Services \(AWS\): Limitazioni e limitazioni del bucket"](#)

["Nomi di dominio degli endpoint per la richiesta S3"](#)

LE operazioni GET bucket (Elenca oggetti) e GET Bucket Versions supportano i controlli di coerenza StorageGRID.

È possibile verificare se gli aggiornamenti dell'ultimo tempo di accesso sono attivati o disattivati per i singoli 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
ELIMINA bucket	Implementato con tutti i comportamenti REST API di Amazon S3.
ELIMINA cors bucket	Questa operazione elimina la configurazione CORS per il bucket.
ELIMINA crittografia bucket	Questa operazione elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma i nuovi oggetti aggiunti al bucket non vengono crittografati.
ELIMINA ciclo di vita bucket	Questa operazione elimina la configurazione del ciclo di vita dal bucket.
ELIMINA policy bucket	Questa operazione elimina la policy associata al bucket.
ELIMINA replica bucket	Questa operazione elimina la configurazione di replica collegata al bucket.
ELIMINA tag bucket	Questa operazione utilizza <code>tagging sottorisorsa</code> per rimuovere tutti i tag da un bucket.
GET Bucket (Elenca oggetti), versione 1 e versione 2	<p>Questa operazione restituisce alcuni o tutti (fino a 1,000) gli oggetti in un bucket. La classe Storage per gli oggetti può avere due valori, anche se l'oggetto è stato acquisito con <code>REDUCED_REDUNDANCY</code> opzione classe di storage:</p> <ul style="list-style-type: none"> <li>• <b>STANDARD</b>, Che indica che l'oggetto è memorizzato in un pool di storage costituito da nodi di storage.</li> <li>• <b>GLACIER</b>, Che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool.</li> </ul> <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>
OTTIENI acl bucket	Questa operazione restituisce una risposta positiva e l'ID, il DisplayName e il permesso del proprietario del bucket, indicando che il proprietario ha pieno accesso al bucket.

Operazione	Implementazione
OTTIENI bucket cors	Questa operazione restituisce il <code>cors</code> configurazione per il bucket.
OTTIENI la crittografia bucket	Questa operazione restituisce la configurazione di crittografia predefinita per il bucket.
OTTIENI il ciclo di vita del bucket	Questa operazione restituisce la configurazione del ciclo di vita del bucket.
OTTIENI posizione bucket	Questa operazione restituisce la regione impostata utilizzando <code>LocationConstraint</code> Elemento nella richiesta <code>PUT bucket</code> . Se l'area del bucket è <code>us-east-1</code> , viene restituita una stringa vuota per la regione.
OTTIENI notifica bucket	Questa operazione restituisce la configurazione di notifica allegata al bucket.
SCARICA le versioni degli oggetti bucket	Con l'accesso IN LETTURA su un bucket, questa operazione con <code>versions</code> la sottorisorsa elenca i metadati di tutte le versioni degli oggetti nel bucket.
OTTIENI la policy bucket	Questa operazione restituisce la <code>policy</code> allegata al bucket.
OTTIENI la replica bucket	Questa operazione restituisce la configurazione di replica collegata al bucket.
OTTIENI il contrassegno bucket	Questa operazione utilizza <code>tagging</code> sottorisorsa per restituire tutti i tag per un bucket.
SCARICA la versione di bucket	Questa implementazione utilizza <code>versioning</code> sottorisorsa per restituire lo stato di versione di un bucket. Lo stato di versione restituito indica se il bucket è "Unversioned" o se la versione del bucket è "enabled" o "Suspended".
OTTIENI configurazione blocco oggetto	Questa operazione determina se S3 Object Lock è attivato per un bucket. <a href="#">"Utilizzo di S3 Object Lock"</a>
BENNA PER LA TESTA	Questa operazione determina se esiste un bucket e se si dispone dell'autorizzazione per accedervi.

Operazione	Implementazione
METTI bucket	<p>Questa operazione crea un nuovo bucket. Creando il bucket, diventerai il proprietario del bucket.</p> <ul style="list-style-type: none"> <li>I nomi dei bucket devono rispettare le seguenti regole: <ul style="list-style-type: none"> <li>Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).</li> <li>Deve essere conforme al DNS.</li> <li>Deve contenere almeno 3 e non più di 63 caratteri.</li> <li>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.</li> <li>Non deve essere simile a un indirizzo IP formattato con testo.</li> <li>Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server.</li> </ul> </li> <li>Per impostazione predefinita, i bucket vengono creati in <code>us-east-1</code> regione; tuttavia, è possibile utilizzare <code>LocationConstraint</code> elemento di richiesta nel corpo della richiesta per specificare un'area diversa. Quando si utilizza <code>LocationConstraint</code> È necessario specificare il nome esatto di una regione definita utilizzando Grid Manager o l'API Grid Management. Contattare l'amministratore di sistema se non si conosce il nome della regione da utilizzare. <b>Nota:</b> Si verifica un errore se la richiesta PUT bucket utilizza un'area non definita in StorageGRID.</li> <li>È possibile includere <code>x-amz-bucket-object-lock-enabled</code> Richiedi intestazione per creare un bucket con blocco oggetti S3 attivato.</li> </ul> <p>È necessario attivare il blocco oggetti S3 quando si crea il bucket. Non è possibile 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> <p><a href="#">"Utilizzo di S3 Object Lock"</a></p>

Operazione	Implementazione
METTI cors bucket	<p>Questa operazione imposta la configurazione del CORS per un bucket in modo che il bucket possa gestire le richieste di origine incrociata. 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. Si supponga, ad esempio, di utilizzare un bucket S3 denominato <code>images</code> per memorizzare le immagini. Impostando la configurazione CORS per <code>images</code> bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito web <code>http://www.example.com</code>.</p>
METTI la crittografia bucket	<p>Questa operazione imposta 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 <code>SSEAlgorithm</code> parametro a <code>AES256</code> e non utilizzare <code>KMSMasterKeyID</code> parametro.</p> <p>La configurazione della crittografia predefinita del bucket viene ignorata se la richiesta di caricamento degli oggetti specifica già la crittografia, ovvero se la richiesta include <code>x-amz-server-side-encryption-*</code> intestazione della richiesta).</p>

Operazione	Implementazione
METTI IL ciclo di vita del bucket	<p>Questa operazione 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"> <li>• Scadenza (giorni, data)</li> <li>• Non currentVersionExpiration (non currentDays)</li> <li>• Filtro (prefisso, tag)</li> <li>• Stato</li> <li>• ID</li> </ul> <p>StorageGRID non supporta queste azioni:</p> <ul style="list-style-type: none"> <li>• AbortIncompleteMultipartUpload</li> <li>• ExpiredObjectDeleteMarker</li> <li>• Transizione</li> </ul> <p>Per capire come l'azione di scadenza in un ciclo di vita del bucket interagisce con le istruzioni di posizionamento di ILM, consulta “funzionamento di ILM durante la vita di un oggetto” nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.</p> <p><b>Nota:</b> 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
NOTIFICA DEL bucket	<p>Questa operazione 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"> <li>• StorageGRID supporta gli argomenti del servizio di notifica semplice (SNS) come destinazioni. Gli endpoint SQS (Simple Queue Service) o Amazon Lambda non sono supportati.</li> <li>• 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.</li> </ul> <p>L'endpoint deve esistere perché la configurazione della notifica abbia esito positivo. Se l'endpoint non esiste, un 400 Bad Request viene restituito un errore con il codice InvalidArgument.</p> <ul style="list-style-type: none"> <li>• Non è possibile configurare una notifica per i seguenti tipi di eventi. Questi tipi di evento sono <b>non supportati</b>. <ul style="list-style-type: none"> <li>◦ s3:ReducedRedundancyLostObject</li> <li>◦ s3:ObjectRestore:Completed</li> </ul> </li> <li>• 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"> <li>• <b>EventSource</b> sgws:s3</li> <li>• <b>AwsRegion</b> non incluso</li> <li>• <b>x-amz-id-2</b> non incluso</li> <li>• <b>arn</b> urn:sgws:s3:::bucket_name</li> </ul> </li> </ul>
METTI la policy bucket	Questa operazione imposta la policy associata al bucket.

Operazione	Implementazione
METTI la replica del bucket	<p>Questa operazione configura la 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 style="list-style-type: none"> <li>• StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo di <code>Filter</code>. 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.</li> <li>• La replica del bucket può essere configurata su bucket con versione o senza versione.</li> <li>• 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> <li>• I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID, come specificato in Gestione tenant o nell'API di gestione tenant.</li> </ul> <p>L'endpoint deve esistere per il successo della configurazione della replica. Se l'endpoint non esiste, la richiesta fallisce come a. 400 Bad Request. Il messaggio di errore indica: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></p> <ul style="list-style-type: none"> <li>• Non è necessario specificare un <code>Role</code>. Nel file XML di configurazione, questo valore non viene utilizzato da StorageGRID e verrà ignorato se inviato.</li> <li>• Se si omette la classe di storage dall'XML di configurazione, StorageGRID utilizza <code>STANDARD</code> classe di storage per impostazione predefinita.</li> <li>• 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 style="list-style-type: none"> <li>◦ 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> <li>◦ 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.</li> </ul> </li> </ul>

Operazione	Implementazione
INSERIRE il contrassegno bucket	<p>Questa operazione utilizza <b>tagging sottorisorsa</b> per aggiungere o aggiornare un set di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni:</p> <ul style="list-style-type: none"> <li>• StorageGRID e Amazon S3 supportano fino a 50 tag per ciascun bucket.</li> <li>• Le etichette associate a un bucket devono avere chiavi tag univoche. Una chiave tag può contenere fino a 128 caratteri Unicode.</li> <li>• I valori dei tag possono contenere fino a 256 caratteri Unicode.</li> <li>• Chiavi e valori distinguono tra maiuscole e minuscole.</li> </ul>
METTERE il bucket in versione	<p>Questa implementazione utilizza <b>versioning sottorisorsa</b> 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"> <li>• Enabled (attivato): Attiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID di versione univoco.</li> <li>• Suspended (sospeso): Disattiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione null.</li> </ul>

#### Informazioni correlate

["Documentazione Amazon Web Services \(AWS\): Replica tra regioni"](#)

["Controlli di coerenza"](#)

["OTTIENI la richiesta dell'ultimo accesso al bucket"](#)

["Policy di accesso a bucket e gruppi"](#)

["Utilizzo di S3 Object Lock"](#)

["Operazioni S3 registrate nei registri di audit"](#)

["Gestire gli oggetti con ILM"](#)

["Utilizzare un account tenant"](#)

#### Creazione di una 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 i dettagli completi sulla creazione delle configurazioni del ciclo di vita S3, consulta la sezione sulla gestione del ciclo di vita degli oggetti nella *Amazon Simple Storage Service Developer Guide*. Nota: StorageGRID supporta solo le azioni di scadenza e non le azioni di transizione.

["Amazon Simple Storage Service Developer Guide: Gestione del ciclo di vita degli oggetti"](#)

### Che cos'è una 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

Se si applica una configurazione del ciclo di vita a un bucket, le impostazioni del ciclo di vita del bucket sovrascrivono sempre le impostazioni ILM di StorageGRID. StorageGRID utilizza le impostazioni di scadenza per il bucket, non ILM, per determinare se eliminare o conservare oggetti specifici.

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 "funzionamento di ILM durante la vita di un oggetto" nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.



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:

- ELIMINA ciclo di vita bucket
- OTTIENI il ciclo di vita del bucket
- METTI IL ciclo di vita del bucket

### Creazione della 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 alla

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 qualsiasi versione non corrente degli oggetti corrispondenti scadrà 50 giorni dopo che diventeranno non aggiornati.

```

{
  "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"
    }
  ]
}

```

## Applicazione di una configurazione del ciclo di vita a un bucket

Dopo aver creato il file di configurazione del ciclo di vita, lo si applica a un bucket inviando una richiesta DI ciclo di vita PUT bucket.

Questa richiesta applica la configurazione del ciclo di vita nel file di esempio agli oggetti in un bucket denominato testbucket:bucket

```
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, emettere una richiesta DI ciclo di vita GET Bucket. 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.

### La convalida della scadenza del ciclo di vita del bucket si applica a un 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 DI oggetto PUT, HEAD o GET. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando l'oggetto scade e quale regola di scadenza è stata associata.



Poiché il ciclo di vita del bucket ha la priorità su ILM, il sistema `expiry-date` viene visualizzata la data effettiva in cui l'oggetto verrà eliminato. Per ulteriori informazioni, vedere "come viene determinata la conservazione degli oggetti" nelle istruzioni per l'esecuzione dell'amministrazione di StorageGRID.

Ad esempio, questa richiesta DI oggetti PUT è stata emessa il 22 giugno 2020 e inserisce un oggetto in 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 di oggetto HEAD 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": {}
}
```

## Informazioni correlate

["Operazioni sui bucket"](#)

["Gestire gli oggetti con ILM"](#)

## Operazioni personalizzate sui bucket

Il sistema StorageGRID supporta operazioni bucket personalizzate aggiunte all'API REST S3 e specifiche del sistema.

La seguente tabella elenca le operazioni di bucket personalizzate supportate da StorageGRID.

Operazione	Descrizione	Per ulteriori informazioni
COERENZA del bucket	Restituisce il livello di coerenza applicato a un determinato bucket.	<a href="#">"OTTIENI una richiesta di coerenza bucket"</a>
METTI la coerenza del bucket	Imposta il livello di coerenza applicato a un bucket specifico.	<a href="#">"INSERIRE la richiesta di coerenza del bucket"</a>

Operazione	Descrizione	Per ulteriori informazioni
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.	<a href="#">"OTTIENI la richiesta dell'ultimo accesso al bucket"</a>
TEMPO ULTIMO accesso bucket	Consente di attivare o disattivare gli ultimi aggiornamenti dell'orario di accesso per un determinato bucket.	<a href="#">"METTI richiesta dell'ultimo tempo di accesso al bucket"</a>
ELIMINA la configurazione di notifica dei metadati del bucket	Elimina l'XML di configurazione della notifica dei metadati associato a un bucket specifico.	<a href="#">"ELIMINA la richiesta di configurazione della notifica dei metadati del bucket"</a>
OTTIENI la configurazione della notifica dei metadati del bucket	Restituisce l'XML di configurazione della notifica dei metadati associato a un bucket specifico.	<a href="#">"OTTIENI una richiesta di configurazione per la notifica dei metadati del bucket"</a>
INSERIRE la configurazione della notifica dei metadati del bucket	Configura il servizio di notifica dei metadati per un bucket.	<a href="#">"INSERIRE la richiesta di configurazione della notifica dei metadati del bucket"</a>
APPORTARE modifiche al bucket per la conformità	Obsoleto e non supportato: Non è più possibile creare nuovi bucket con Compliance abilitata.	<a href="#">"Deprecato: APPORTARE modifiche alla richiesta di conformità al bucket"</a>
OTTIENI la compliance del bucket	Obsoleto ma supportato: Restituisce le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.	<a href="#">"Deprecato: OTTIENI una richiesta di conformità bucket"</a>
METTI la compliance del bucket	Obsoleto ma supportato: Consente di modificare le impostazioni di conformità per un bucket compatibile esistente.	<a href="#">"Deprecato: INSERIRE la richiesta di conformità del bucket"</a>

#### Informazioni correlate

["Operazioni S3 registrate nei registri di audit"](#)

#### Operazioni sugli oggetti

Questa sezione descrive come il sistema StorageGRID implementa le operazioni API REST S3 per gli oggetti.

- ["Utilizzo di S3 Object Lock"](#)
- ["Utilizzo della crittografia lato servver"](#)

- "OTTIENI oggetto"
- "Oggetto TESTA"
- "RIPRISTINO POST-oggetto"
- "METTI oggetto"
- "METTI oggetto - Copia"

Le seguenti condizioni si applicano a tutte le operazioni a oggetti:

- I controlli di coerenza StorageGRID sono supportati da tutte le operazioni sugli oggetti, ad eccezione di quanto segue:
  - GET Object ACL (OTTIENI ACL oggetto)
  - OPTIONS /
  - METTERE in attesa legale l'oggetto
  - METTI la conservazione degli oggetti
- Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vittorie". La tempistica per la valutazione "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non su quando 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.
- Non è possibile accedere agli oggetti dati acquisiti nel sistema StorageGRID tramite Swift tramite S3.

Nella tabella seguente viene descritto il modo in cui StorageGRID implementa le operazioni degli oggetti API REST S3.

Operazione	Implementazione
<p>ELIMINA oggetto</p>	<p>Autenticazione multifattore (MFA) e intestazione della risposta <code>x-amz-mfa</code> non sono supportati.</p> <p>Durante l'elaborazione di una richiesta DI ELIMINAZIONE degli oggetti, 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 non è temporaneamente disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito.</p> <p><b>Versione</b></p> <p>Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare <code>versionId</code> sottorisorsa. L'utilizzo di questa sottorisorsa elimina in modo permanente la versione. Se il <code>versionId</code> corrisponde a un indicatore di eliminazione, l'intestazione della risposta <code>x-amz-delete-marker</code> viene restituito impostato su <code>true</code>.</p> <ul style="list-style-type: none"> <li>• Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket abilitato alla versione, si ottiene la generazione di un indicatore di eliminazione. Il <code>versionId</code> per il contrassegno di eliminazione viene restituito utilizzando <code>x-amz-version-id</code> intestazione della risposta e la <code>x-amz-delete-marker</code> l'intestazione della risposta viene restituita impostata su <code>true</code>.</li> <li>• Se un oggetto viene eliminato senza <code>versionId</code> sottorisorsa su un bucket sospeso della versione, si ottiene una cancellazione permanente di una versione 'null' già esistente o di un marker di eliminazione 'null' e la generazione di un nuovo marker di eliminazione 'null'. Il <code>x-amz-delete-marker</code> l'intestazione della risposta viene restituita impostata su <code>true</code>.</li> </ul> <p><b>Nota:</b> In alcuni casi, per un oggetto potrebbero esistere più contrassegni di eliminazione.</p>
<p>ELIMINARE più oggetti</p>	<p>Autenticazione multifattore (MFA) e intestazione della risposta <code>x-amz-mfa</code> non sono supportati.</p>
	<p>È possibile eliminare più oggetti nello stesso messaggio di richiesta.</p>

Operazione	Implementazione
ELIMINA tag oggetti	<p>Utilizza tagging sottorisorsa per rimuovere tutti i tag da un oggetto. Implementato con tutti i comportamenti REST API di Amazon S3.</p> <p><b>Versione</b></p> <p>Se il <code>versionId</code> il parametro query non è specificato nella richiesta, l'operazione elimina tutti i tag dalla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione risposta impostata su <code>true</code>.</p>
OTTIENI oggetto	<a href="#">"OTTIENI oggetto"</a>
GET Object ACL (OTTIENI ACL oggetto)	<p>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.</p>
OTTENERE un blocco legale degli oggetti	<a href="#">"Utilizzo di S3 Object Lock"</a>
OTTIENI la conservazione degli oggetti	<a href="#">"Utilizzo di S3 Object Lock"</a>
OTTIENI tag di oggetti	<p>Utilizza tagging sottorisorsa per restituire tutti i tag per un oggetto. Implementato con tutti i comportamenti REST API di Amazon S3</p> <p><b>Versione</b></p> <p>Se il <code>versionId</code> il parametro query non è specificato nella richiesta, l'operazione restituisce tutti i tag della versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione risposta impostata su <code>true</code>.</p>
Oggetto TESTA	<a href="#">"Oggetto TESTA"</a>
RIPRISTINO POST-oggetto	<a href="#">"RIPRISTINO POST-oggetto"</a>
METTI oggetto	<a href="#">"METTI oggetto"</a>

Operazione	Implementazione
METTI oggetto - Copia	<a href="#">"METTI oggetto - Copia"</a>
METTERE in attesa legale l'oggetto	<a href="#">"Utilizzo di S3 Object Lock"</a>
METTI la conservazione degli oggetti	<a href="#">"Utilizzo di S3 Object Lock"</a>

Operazione	Implementazione
INSERIRE tag degli oggetti	<p>Utilizza tagging sottorisorsa per aggiungere un set di tag a un oggetto esistente. Implementato con tutti i comportamenti REST API di Amazon S3</p> <p><b>Aggiornamenti dei tag e comportamento di acquisizione</b></p> <p>Quando si utilizza IL tag PUT Object per aggiornare i tag di un oggetto, StorageGRID non reinserisce 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><b>Risoluzione dei conflitti</b></p> <p>Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vittorie". La tempistica per la valutazione "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non su quando i client S3 iniziano un'operazione.</p> <p><b>Versione</b></p> <p>Se il <code>versionId</code> il parametro query non è specificato nella richiesta, l'operazione aggiunge tag alla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con <code>x-amz-delete-marker</code> intestazione risposta impostata su <code>true</code>.</p>

## Informazioni correlate

["Controlli di coerenza"](#)

["Operazioni S3 registrate nei registri di audit"](#)

## Utilizzo di S3 Object Lock

Se l'impostazione blocco oggetti S3 globale è attivata per il sistema StorageGRID, è possibile creare bucket con blocco oggetti S3 attivato e specificare le impostazioni di conservazione fino alla data e conservazione legale per ogni versione dell'oggetto aggiunta a tale bucket.

S3 Object Lock consente di specificare le impostazioni a livello di oggetto per impedire che gli oggetti vengano cancellati o sovrascritti per un periodo di tempo fisso o indefinito.

La funzione blocco oggetto StorageGRID S3 offre una singola modalità di conservazione equivalente alla modalità di conformità Amazon S3. Per impostazione predefinita, una versione dell'oggetto protetto non può essere sovrascritta o eliminata da alcun utente. La funzione blocco oggetti di StorageGRID S3 non supporta una modalità di governance e non consente agli utenti con autorizzazioni speciali di ignorare le impostazioni di conservazione o di eliminare gli oggetti protetti.

### Abilitazione di S3 Object Lock 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. È possibile utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando il tenant Manager.

["Utilizzare un account tenant"](#)

- Creare il bucket utilizzando una richiesta PUT bucket con `x-amz-bucket-object-lock_enabled` intestazione della richiesta.

["Operazioni sui bucket"](#)

Non è possibile aggiungere o disattivare il blocco oggetti S3 dopo la creazione del bucket. S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando si crea il bucket.

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza le impostazioni S3 Object Lock. StorageGRID non supporta la conservazione predefinita per gli oggetti nei bucket blocco oggetti S3, pertanto l'operazione DEL bucket CONFIGURAZIONE BLOCCO oggetti PUT non è supportata.

### Determinare se S3 Object Lock (blocco oggetti S3) è attivato per un bucket

Per determinare se S3 Object Lock è attivato, utilizzare la richiesta GET Object Lock Configuration.

["Operazioni sui bucket"](#)

### Creazione di un oggetto con le impostazioni S3 Object Lock

Per specificare le impostazioni di blocco oggetti S3 quando si aggiunge una versione di oggetto a un bucket con blocco oggetti S3 attivato, eseguire una richiesta PUT object, PUT object - Copy o avviare la richiesta di caricamento multiparte. Utilizzare le seguenti intestazioni di richiesta.



È necessario attivare il blocco oggetti S3 quando si crea un bucket. Non è possibile aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket.

- `x-amz-object-lock-mode`, Che deve essere CONFORME (distinzione tra maiuscole e minuscole).



Se si specifica `x-amz-object-lock-mode`, è inoltre necessario specificare `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`

- Il valore di conservazione fino alla data 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:

- Il Content-MD5 l'intestazione della richiesta è obbligatoria, se presente `x-amz-object-lock-*` L'intestazione della richiesta è presente nella richiesta DELL'oggetto PUT. Content-MD5 Non è richiesto per METTERE oggetto - copiare o avviare caricamento multipart.
- Se il bucket non ha S3 Object Lock abilitato e un `x-amz-object-lock-*` L'intestazione della richiesta è presente, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta DI oggetti PUT supporta l'utilizzo di `x-amz-storage-class: REDUCED_REDUNDANCY` Per far corrispondere il comportamento di 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 DELL'oggetto GET o HEAD includerà le intestazioni `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e. `x-amz-object-lock-legal-hold`, se configurato e se il mittente della richiesta ha il corretto s3:Get\* permessi.
- Una successiva richiesta DI versione DELL'oggetto DELETE o di versioni DELL'oggetto DELETE avrà esito negativo se è precedente alla data di conservazione o se è attiva una conservazione a fini giudiziari.

## Aggiornamento delle impostazioni di blocco oggetti S3

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:

- PUT Object legal-hold

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.

- PUT Object retention

- Il valore della modalità deve essere COMPLIANCE (distinzione tra maiuscole e minuscole).
- Il valore di conservazione fino alla data 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.

## Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Utilizzare un account tenant"](#)

["METTI oggetto"](#)

["METTI oggetto - Copia"](#)

["Avvia caricamento multiparte"](#)

["Versione degli oggetti"](#)

["Amazon Simple Storage Service User Guide \(Guida utente di Amazon Simple Storage Service\): Utilizzo di S3 Object Lock"](#)

## Utilizzo della 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 decifratura 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.

## Utilizzo di 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:

- METTI oggetto
- METTI oggetto - Copia
- Avvia caricamento multiparte

### Utilizzo di 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:

- OTTIENI oggetto
- Oggetto TESTA
- METTI oggetto
- METTI oggetto - Copia
- Avvia caricamento multiparte
- Carica parte
- Carica parte - Copia

### 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 su http quando si utilizza SSE-C. Per motivi di sicurezza, è consigliabile considerare compromessa qualsiasi chiave inviata accidentalmente utilizzando http. 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 CloudMirror è configurata per il bucket, non è possibile acquisire oggetti SSE-C. L'operazione di acquisizione non riesce.

## Informazioni correlate

["OTTIENI oggetto"](#)

["Oggetto TESTA"](#)

["METTI oggetto"](#)

["METTI oggetto - Copia"](#)

["Avvia caricamento multipart"](#)

["Carica parte"](#)

["Carica parte - Copia"](#)

["Amazon S3 Developer Guide: Protezione dei dati mediante crittografia lato server con chiavi di crittografia fornite dal cliente \(SSE-C\)"](#)

## OTTIENI oggetto

È possibile utilizzare la richiesta di oggetti GET S3 per recuperare un oggetto da un bucket S3.

## Il parametro di richiesta del numero di parte non è supportato

Il `partNumber` Il parametro di richiesta non è supportato per le richieste DI oggetti GET. Non è possibile eseguire una richiesta GET per recuperare una parte specifica di un oggetto multipart. Viene visualizzato un errore 501 non implementato con il seguente messaggio:

```
GET Object by partNumber is not implemented
```

## 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, consultare le considerazioni in "utilizzo della crittografia lato server".

## UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. LE richieste GET per un oggetto con caratteri UTF-8 escapati nei metadati definiti dall'utente non restituiscono `x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

## Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

## Versione

Se si seleziona `versionId` la sottorisorsa non viene specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "Not Found" (non trovato) con `x-amz-delete-marker` intestazione risposta impostata su `true`.

## Comportamento di GET Object per gli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in un Cloud Storage Pool (vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni), il comportamento di una richiesta DI un oggetto GET dipende dallo stato dell'oggetto. Per ulteriori informazioni, consulta "HEAD Object".



Se un oggetto viene memorizzato in un Cloud Storage Pool e una o più copie dell'oggetto sono presenti anche nella griglia, LE richieste GET Object tenteranno di recuperare i dati dalla griglia, prima di recuperarli dal Cloud Storage Pool.

Stato dell'oggetto	Comportamento dell'oggetto GET
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.

Stato dell'oggetto	Comportamento dell'oggetto GET
Oggetto sottoposto a transizione in uno stato non recuperabile	403 Forbidden, InvalidObjectState Utilizzare una richiesta DI ripristino dell'oggetto POST per ripristinare lo stato recuperabile dell'oggetto.
Oggetto in fase di ripristino da uno stato non recuperabile	403 Forbidden, InvalidObjectState Attendere il completamento della richiesta DI ripristino dell'oggetto POST.
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Viene recuperata una copia dell'oggetto.

### Oggetti multipart o segmentati in un pool di storage cloud

Se hai caricato un oggetto multipart 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, la richiesta DI un oggetto GET potrebbe non essere restituita correttamente 200 OK quando alcune parti dell'oggetto sono già state trasferite in uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

In questi casi:

- La richiesta DELL'oggetto GET potrebbe restituire alcuni dati ma arrestarsi a metà del trasferimento.
- Potrebbe essere restituita una richiesta successiva di oggetto GET 403 Forbidden.

### Informazioni correlate

["Utilizzo della crittografia lato server"](#)

["Gestire gli oggetti con ILM"](#)

["RIPRISTINO POST-oggetto"](#)

["Operazioni S3 registrate nei registri di audit"](#)

### Oggetto TESTA

È possibile utilizzare la richiesta di oggetti TESTA S3 per recuperare i metadati da un oggetto senza restituire l'oggetto stesso. Se l'oggetto è memorizzato in un Cloud Storage Pool, è possibile utilizzare l'oggetto HEAD per determinare lo stato di transizione dell'oggetto.

### 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, consultare le considerazioni in “utilizzo della crittografia lato server”.

## 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 escapati nei metadati definiti dall'utente non restituiscono `x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

## Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

## Intestazioni di risposta per gli oggetti del Cloud Storage Pool

Se l'oggetto viene memorizzato in un Cloud Storage Pool (vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni), 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 all'oggetto HEAD
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).

Stato dell'oggetto	Risposta all'oggetto HEAD
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 passa a uno stato non recuperabile, il valore per expiry-date è impostato su un periodo di 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 periodo di tempo lontano in futuro.</p> <p><b>Nota:</b> Se la copia sulla griglia non è disponibile (ad esempio, un nodo di storage è inattivo), è necessario eseguire una richiesta DI ripristino DELL'oggetto POST per ripristinare la copia dal pool di storage cloud prima di poter recuperare 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 all'oggetto HEAD
Oggetto completamente ripristinato nel Cloud Storage Pool	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"</p> <p>Il expiry-date Indica quando l'oggetto nel Cloud Storage Pool verrà riportato in uno stato non recuperabile.</p>

## Oggetti multipart o segmentati in un pool di storage cloud

Se hai caricato un oggetto multipart 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, la richiesta di un oggetto HEAD potrebbe non essere corretta x-amz-restore: ongoing-request="false" quando alcune parti dell'oggetto sono già state trasferite in uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

### Versione

Se si seleziona `versionId` la sottorisorsa non viene specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un indicatore di eliminazione, viene restituito lo stato "Not Found" (non trovato) con `x-amz-delete-marker` intestazione risposta impostata su `true`.

### Informazioni correlate

["Utilizzo della crittografia lato server"](#)

["Gestire gli oggetti con ILM"](#)

["RIPRISTINO POST-oggetto"](#)

["Operazioni S3 registrate nei registri di audit"](#)

### RIPRISTINO POST-oggetto

È possibile utilizzare la richiesta di ripristino dell'oggetto POST S3 per ripristinare un oggetto memorizzato in un Cloud Storage Pool.

### Tipo di richiesta supportato

StorageGRID supporta solo le richieste DI ripristino degli oggetti POST per ripristinare un oggetto. Non supporta SELECT tipo di ripristino. Selezionare Requests Return XNotImplemented.

### Versione

Facoltativamente, specificare `versionId` per ripristinare una versione specifica di un oggetto in un bucket con versione. Se non si specifica `versionId`, viene ripristinata la versione più recente dell'oggetto

## Comportamento del ripristino degli oggetti POST sugli oggetti del Cloud Storage Pool

Se un oggetto è stato memorizzato in un Cloud Storage Pool (vedere le istruzioni per la gestione degli oggetti con gestione del ciclo di vita delle informazioni), una richiesta DI ripristino DELL'oggetto POST ha il seguente comportamento, in base allo stato dell'oggetto. Per ulteriori informazioni, consulta "HEAD Object".



Se un oggetto viene memorizzato in un Cloud Storage Pool e una o più copie dell'oggetto sono presenti anche nella griglia, non è necessario ripristinare l'oggetto emettendo una richiesta DI ripristino POST-oggetto. Invece, la copia locale può essere recuperata direttamente, utilizzando una richiesta DI oggetto GET.

Stato dell'oggetto	Comportamento del ripristino degli oggetti POST
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. <b>Nota:</b> Prima che un oggetto sia stato spostato in uno stato non recuperabile, non è possibile modificarne lo stato expiry-date.
Oggetto sottoposto a transizione in uno stato non recuperabile	202 Accepted Ripristina una copia recuperabile dell'oggetto nel 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.  In alternativa, utilizzare Tier elemento request per determinare il tempo necessario per il completamento del processo di ripristino (Expedited, Standard, o. Bulk). Se non si specifica Tier, il Standard viene utilizzato il tier.  <b>Attenzione:</b> Se un oggetto è stato spostato in S3 Glacier Deep Archive o il Cloud Storage Pool utilizza Azure Blob Storage, non è possibile ripristinarlo utilizzando Expedited tier. Viene visualizzato 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 del ripristino degli oggetti POST
Oggetto completamente ripristinato nel Cloud Storage Pool	<p>200 OK</p> <p><b>Nota:</b> se un oggetto è stato ripristinato a uno stato recuperabile, è possibile modificarne lo stato expiry-date Inviando nuovamente la richiesta DI ripristino dell'oggetto POST con un nuovo valore per Days. La data di ripristino viene aggiornata in relazione all'ora della richiesta.</p>

### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Oggetto TESTA"](#)

["Operazioni S3 registrate nei registri di audit"](#)

### METTI oggetto

È possibile utilizzare la richiesta di oggetti PUT S3 per aggiungere un oggetto a un bucket.

### Risoluzione dei conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vittorie". La tempistica per la valutazione "ultimi successi" si basa su quando il sistema StorageGRID completa una data richiesta e non su quando i client S3 iniziano un'operazione.

### Dimensione dell'oggetto

StorageGRID supporta oggetti di dimensioni fino a 5 TB.

### 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 PUT, PUT Object-Copy, GET e HEAD hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 escapati.
- StorageGRID non restituisce `x-amz-missing-meta` header 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 `chunk-signature` rispetto ai dati del blocco.
- StorageGRID non verifica il valore fornito `x-amz-decoded-content-length` rispetto all'oggetto.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

La codifica di trasferimento chunked è supportata se `aws-chunked` viene utilizzata anche la firma del payload.

- `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-<em>name</em>: <em>value</em>
```

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 quando l'oggetto è stato creato. 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 sia le opzioni bilanciate o rigide per il comportamento di Ingest. 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`

#### ["Utilizzo di S3 Object Lock"](#)

- 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`

#### ["Operazioni e limitazioni supportate dall'API REST S3"](#)

#### **Intestazioni di richiesta non supportate**

Le seguenti intestazioni di richiesta non sono supportate:

- Il `x-amz-acl` intestazione della richiesta non supportata.
- Il `x-amz-website-redirect-location` l'intestazione della richiesta non è supportata e restituisce `XNotImplemented`.

#### **Opzioni di classe storage**

Il `x-amz-storage-class` l'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 Strict per il comportamento Ingest, l'`x-amz-storage-class` l'intestazione non ha alcun effetto.

È possibile utilizzare i seguenti valori 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). Una volta valutato l'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 degli oggetti specificate nella regola ILM (posizionamento sincrono), l'`x-amz-storage-class` l'intestazione non ha alcun 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. Il `REDUCED_REDUNDANCY` L'opzione è preferibile quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso, utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni operazione di acquisizione.

Utilizzando il `REDUCED_REDUNDANCY` l'opzione non è consigliata in altre circostanze.

`REDUCED_REDUNDANCY` aumenta il rischio di perdita dei 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.

**Attenzione:** 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.

Specificare `REDUCED_REDUNDANCY` influisce solo sul numero di copie create quando un oggetto viene acquisito per la prima volta. Non influisce sul numero di copie dell'oggetto eseguite quando l'oggetto viene valutato dal criterio ILM attivo e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

**Nota:** Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, il `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il `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`
- **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.

**Attenzione:** 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, consultare le considerazioni in "utilizzo della crittografia lato server".

**Nota:** 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 il controllo delle versioni è attivato per un bucket, viene visualizzato un valore univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene inoltre restituito nella risposta utilizzando `x-amz-version-id` intestazione della risposta.

Se il controllo delle versioni è sospeso, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` se esiste già una versione nulla, questa verrà sovrascritta.

## Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Operazioni sui bucket"](#)

["Operazioni S3 registrate nei registri di audit"](#)

["Utilizzo della crittografia lato server"](#)

["Come configurare le connessioni client"](#)

## METTI oggetto - Copia

È possibile utilizzare la richiesta S3 PUT Object - Copy per creare una copia di un oggetto già memorizzato in S3. Un'operazione PUT object - Copy equivale all'esecuzione di UN'OPERAZIONE GET e poi PUT.

## Risoluzione dei conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vittorie". La tempistica per la valutazione "ultimi successi" si basa su quando il sistema StorageGRID completa una data richiesta e non su quando i client S3 iniziano un'operazione.

## Dimensione dell'oggetto

StorageGRID supporta oggetti di dimensioni fino a 5 TB.

## 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 `x-amz-missing-meta` header 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` per sovrascrivere i metadati esistenti durante la copia dell'oggetto o per 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` per sovrascrivere i tag esistenti durante la copia dell'oggetto o per 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`

## ["Utilizzo di S3 Object Lock"](#)

- 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

#### ["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-website-redirect-location

#### **Opzioni di classe storage**

Il x-amz-storage-class L'intestazione della richiesta è supportata e influisce sul numero di copie di oggetti create da StorageGRID se la regola ILM corrispondente specifica un comportamento di Ingest di doppio commit o bilanciato.

- 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 il blocco oggetti S3 attivato, il REDUCED\_REDUNDANCY l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il 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 PUT Object - Copy**

Se il bucket e la chiave di origine, specificati in x-amz-copy-source header, 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 il x-amz-metadata-directive l'intestazione è 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 PUT Object - Copy per crittografare un oggetto esistente o per modificare la crittografia di un oggetto esistente. Se si fornisce x-amz-server-side-encryption o il x-amz-server-side-encryption-customer-algorithm Intestazione, StorageGRID rifiuta la richiesta e restituisce XNot Implemented.
- 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 la crittografia lato server, le intestazioni delle richieste fornite dipendono dalla crittografia dell'oggetto di origine e dalla crittografia dell'oggetto di destinazione.

- Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le seguenti tre intestazioni nella richiesta PUT Object - Copy, in modo che l'oggetto possa essere decrittare 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 di origine.
- 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.

**Attenzione:** 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, consultare le considerazioni in "utilizzo della crittografia lato server".

- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca gestita da SSE (StorageGRID), includere questa intestazione nella richiesta PUT Object - Copy:
  - x-amz-server-side-encryption

**Nota:** la server-side-encryption impossibile aggiornare il valore dell'oggetto. Invece, fare una copia con un nuovo server-side-encryption valore utilizzando x-amz-metadata-directive: REPLACE.

## Versione

Se il bucket di origine è configurato con la versione, è possibile utilizzare `x-amz-copy-source` intestazione per copiare l'ultima versione di un oggetto. Per copiare una versione specifica di un oggetto, è necessario specificare esplicitamente la versione da copiare utilizzando `versionId` sottorisorsa. Se il bucket di destinazione è configurato con la versione, la versione generata viene restituita in `x-amz-version-id` intestazione della risposta. Se il controllo delle versioni viene sospeso per il bucket di destinazione, allora `x-amz-version-id` restituisce un valore "null".

### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Utilizzo della crittografia lato server"](#)

["Operazioni S3 registrate nei registri di audit"](#)

["METTI oggetto"](#)

## Operazioni per caricamenti multipart

Questa sezione descrive come StorageGRID supporta le operazioni per gli upload di più parti.

- ["Elenca caricamenti multipart"](#)
- ["Avvia caricamento multipart"](#)
- ["Carica parte"](#)
- ["Carica parte - Copia"](#)
- ["Caricamento multipart completo"](#)

Le seguenti condizioni e note si applicano a tutte le operazioni di caricamento multipart:

- Non superare i 1,000 caricamenti simultanei di più parti in un singolo bucket, perché i risultati delle query di upload di List Multipart 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 multipart 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 multipart.
- ILM viene valutato per ogni parte di un oggetto multipart durante l'acquisizione e per l'oggetto nel suo complesso al termine del caricamento multipart, se la regola ILM utilizza il comportamento di acquisizione rigoroso o bilanciato. Devi essere consapevole di come questo influisca sul posizionamento di oggetti e parti:
  - Se ILM cambia mentre è in corso un caricamento S3 multipart, quando il caricamento multipart completa alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti. Tutte le parti non

posizionate correttamente vengono messe in coda per la rivalutazione ILM e spostate 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 superiori sono memorizzati in DC1 mentre tutti gli oggetti più piccoli sono memorizzati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene memorizzata in DC2. 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 i controlli di coerenza StorageGRID.
- Se necessario, è possibile utilizzare la crittografia lato server con upload multiparte. Per utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID), è necessario includere `x-amz-server-side-encryption` Intestazione della richiesta solo nella richiesta di avvio caricamento multiparte. 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 Initiate Multipart Upload (Avvia caricamento multiparte) e in ogni richiesta successiva di caricamento parte.

Operazione	Implementazione
Elenca carichi multiparte	Vedere " <a href="#">Elenca carichi multiparte</a> "
Avvia caricamento multiparte	Vedere " <a href="#">Avvia caricamento multiparte</a> "
Carica parte	Vedere " <a href="#">Carica parte</a> "
Carica parte - Copia	Vedere " <a href="#">Carica parte - Copia</a> "
Caricamento multiparte completo	Vedere " <a href="#">Caricamento multiparte completo</a> "
Interrompi caricamento multiparte	Implementato con tutti i comportamenti REST API di Amazon S3
Elencare le parti	Implementato con tutti i comportamenti REST API di Amazon S3

## Informazioni correlate

["Controlli di coerenza"](#)

["Utilizzo della crittografia lato server"](#)

## Elenca carichi multiparte

L'operazione List Multipart Uploads elenca i carichi multiparte in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

- `encoding-type`
- `max-uploads`

- key-marker
- prefix
- upload-id-marker

Il `delimiter` il parametro della richiesta non è supportato.

## 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 viene eseguita l'operazione completa di caricamento multiparte, il punto in cui vengono creati gli oggetti (e la versione, se applicabile).

### Avvia caricamento multiparte

L'operazione `Initiate Multipart Upload` (Avvia caricamento multiparte) avvia un caricamento multiparte per un oggetto e restituisce un ID di caricamento.

Il `x-amz-storage-class` l'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 Strict per il comportamento Ingest, l'`x-amz-storage-class` l'intestazione non ha alcun effetto.

È possibile utilizzare i seguenti valori 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). Una volta valutato l'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 degli oggetti specificate nella regola ILM (posizionamento sincrono), l'`x-amz-storage-class` l'intestazione non ha alcun 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. Il `REDUCED_REDUNDANCY` L'opzione è preferibile quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso, utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni

operazione di acquisizione.

Utilizzando il REDUCED\_REDUNDANCY l'opzione non è consigliata in altre circostanze.

REDUCED\_REDUNDANCY aumenta il rischio di perdita dei 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.

**Attenzione:** 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.

Specificare REDUCED\_REDUNDANCY influisce solo sul numero di copie create quando un oggetto viene acquisito per la prima volta. Non influisce sul numero di copie dell'oggetto eseguite quando l'oggetto viene valutato dal criterio ILM attivo e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

**Nota:** Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, il REDUCED\_REDUNDANCY l'opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il REDUCED\_REDUNDANCY l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Sono supportate le seguenti intestazioni di richiesta:

- Content-Type
- 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 quando l'oggetto è stato creato. Ad esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per creation-time viene valutato in secondi dal 1° gennaio 1970.



Aggiunta creation-time Poiché i metadati definiti dall'utente non sono consentiti se si aggiunge un oggetto a un bucket che ha abilitato 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

## "Utilizzo di S3 Object Lock"

- 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

## "Operazioni e limitazioni supportate dall'API REST S3"



Per informazioni su come StorageGRID gestisce i caratteri UTF-8, consultare la documentazione relativa A PUT Object.

### Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto multipart con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE**: Utilizzare la seguente intestazione nella richiesta di avvio caricamento multipart se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste di carica parte.
  - x-amz-server-side-encryption
- **SSE-C**: Utilizzare tutte e tre queste intestazioni nella richiesta Initiate Multipart Upload (e in ogni richiesta successiva di carica parte) 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.

**Attenzione:** 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, consultare le considerazioni in "utilizzo della crittografia lato server".

### Intestazioni di richiesta non supportate

La seguente intestazione di richiesta non è supportata e restituisce XNotImplemented

- x-amz-website-redirect-location

### 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. Gli oggetti vengono creati (e, se applicabile, con la versione) quando viene eseguita l'operazione completa di caricamento multipart.

### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Utilizzo della crittografia lato server"](#)

["METTI oggetto"](#)

#### **Carica parte**

L'operazione carica parte carica una parte in un caricamento multipart per un oggetto.

#### **Intestazioni di richiesta supportate**

Sono supportate le seguenti intestazioni di richiesta:

- Content-Length
- Content-MD5

#### **Intestazioni di richiesta per la crittografia lato server**

Se è stata specificata la crittografia SSE-C per la richiesta di avvio caricamento multipart, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta di caricamento parte:

- 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 di avvio caricamento multipart.
- x-amz-server-side-encryption-customer-key-MD5: Specificare lo stesso digest MD5 fornito nella richiesta di avvio caricamento multipart.

 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, consultare le considerazioni in "utilizzo della 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. Gli oggetti vengono creati (e, se applicabile, con la versione) quando viene eseguita l'operazione completa di caricamento multipart.

#### **Informazioni correlate**

["Utilizzo della crittografia lato server"](#)

#### **Carica parte - Copia**

L'operazione carica parte - Copia carica una parte di un oggetto copiando i dati da un oggetto esistente come origine dati.

L'operazione carica parte - Copia viene implementata con tutti i comportamenti REST API di Amazon S3.

Questa richiesta legge e scrive i dati dell'oggetto specificati in x-amz-copy-source-range **Nel** sistema

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 di avvio caricamento multipart, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta di caricamento parte - Copia:

- 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 di avvio caricamento multipart.
- x-amz-server-side-encryption-customer-key-MD5: Specificare lo stesso digest MD5 fornito nella richiesta di avvio caricamento multipart.

Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le seguenti tre intestazioni nella richiesta carica parte - Copia, in modo che l'oggetto possa essere decrittare 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 di origine.

 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, consultare le considerazioni in “utilizzo della 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. Gli oggetti vengono creati (e, se applicabile, con la versione) quando viene eseguita l'operazione completa di caricamento multipart.

#### Caricamento multipart completo

L'operazione completa di caricamento multipart completa un caricamento multipart di un oggetto assemblando le parti precedentemente caricate.

## Risoluzione dei conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle “ultime vittorie”. La tempistica per la valutazione “ultimi successi” si basa su quando il sistema StorageGRID completa una data richiesta e non su quando i client S3 iniziano un’operazione.

## Dimensione dell’oggetto

StorageGRID supporta oggetti di dimensioni fino a 5 TB.

## Intestazioni delle richieste

Il `x-amz-storage-class` L’intestazione della richiesta è supportata e influisce sul numero di copie di oggetti create da StorageGRID se la regola ILM corrispondente specifica un comportamento di Ingest di doppio commit o bilanciato.

- 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 il blocco oggetti S3 attivato, il REDUCED\_REDUNDANCY l’opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket compatibile legacy, il 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 multiparte non viene completato entro 15 giorni, l’operazione viene contrassegnata come inattiva e tutti i dati associati vengono cancellati dal sistema.



Il ETag Il valore restituito non è una somma MD5 dei dati, ma segue l’implementazione dell’API Amazon S3 di ETag valore per oggetti multiparte.

## Versione

Questa operazione completa un caricamento multiparte. Se la versione è abilitata per un bucket, la versione dell’oggetto viene creata al termine del caricamento multiparte.

Se il controllo delle versioni è attivato per un bucket, viene visualizzato un valore univoco `versionId` viene generato automaticamente per la versione dell’oggetto memorizzato. Questo `versionId` viene inoltre restituito nella risposta utilizzando `x-amz-version-id` intestazione della risposta.

Se il controllo delle versioni è sospeso, la versione dell’oggetto viene memorizzata con un valore nullo `versionId` se esiste già una versione nulla, questa 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.

In questo caso, viene generato un allarme in Grid Manager on Total Events (SMTT). Il messaggio Last Event (ultimo evento) visualizza "Failed to publish notifications for bucket-nameobject key" (Impossibile pubblicare le notifiche per la chiave bucket-nameobject) per l'ultimo oggetto la cui notifica non (Per visualizzare questo messaggio, selezionare **Nodes > Storage Node > Events**. Visualizza ultimo evento nella parte superiore della tabella.) I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

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.

### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

### 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

Nome	Stato HTTP
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
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

Nome	Stato HTTP
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
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

Nome	Descrizione	Stato HTTP
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 REST API di StorageGRID S3

Sono state aggiunte operazioni all'API REST S3 specifiche per il sistema StorageGRID.

### OTTIENI una richiesta di coerenza bucket

La richiesta DI coerenza GET Bucket consente di determinare il livello di coerenza applicato a un determinato bucket.

I controlli di coerenza predefiniti sono impostati in modo da garantire la lettura dopo la scrittura degli oggetti creati di recente.

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

#### Risposta

Nella risposta XML, <Consistency> restituisce uno dei seguenti valori:

Controllo della 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.

Controllo della coerenza	Descrizione
read-after-new-write	<p>(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. Corrisponde alle garanzie di coerenza di Amazon S3.</p> <p><b>Nota:</b> se l'applicazione utilizza richieste HEAD su oggetti che non esistono, potrebbe essere visualizzato un numero elevato di errori 500 interni del server se uno o più nodi di storage non sono disponibili. Per evitare questi errori, imposta il controllo di coerenza su "Available", a meno che non necessiti di garanzie di coerenza simili a Amazon S3.</p>
Disponibile (eventuale coerenza per le operazioni TESTA)	<p>Si comporta come il livello di coerenza "read-after-new-write", ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a "read-after-new-write" se i nodi storage non sono disponibili. Differisce dalle garanzie di coerenza di Amazon S3 solo per le operazioni HEAD.</p>

#### 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

["Controlli di coerenza"](#)

#### INSERIRE la richiesta di coerenza del bucket

La richiesta DI coerenza PUT bucket consente di specificare il livello di coerenza da applicare alle operazioni eseguite su un bucket.

I controlli di coerenza predefiniti sono impostati in modo da garantire la lettura dopo la scrittura degli oggetti creati di recente.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketConsistency o essere root dell'account.

#### Richiesta

Il `x-ntap-sg-consistency` il parametro deve contenere uno dei seguenti valori:

Controllo della 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. Corrisponde alle garanzie di coerenza di Amazon S3.  <b>Nota:</b> se l'applicazione utilizza richieste HEAD su oggetti che non esistono, potrebbe essere visualizzato un numero elevato di errori 500 interni del server se uno o più nodi di storage non sono disponibili. Per evitare questi errori, imposta il controllo di coerenza su "Available", a meno che non necessiti di garanzie di coerenza simili a Amazon S3.
Disponibile (eventuale coerenza per le operazioni TESTA)	Si comporta come il livello di coerenza "read-after-new-write", ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a "read-after-new-write" se i nodi storage non sono disponibili. Differisce dalle garanzie di coerenza di Amazon S3 solo per le operazioni HEAD.

**Nota:** in generale, utilizzare il valore del controllo di 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 il controllo di coerenza per ogni richiesta API. Impostare il controllo di coerenza a livello di bucket solo come ultima risorsa.

#### Esempio di richiesta

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

## Informazioni correlate

["Controlli di coerenza"](#)

## OTTIENI la richiesta dell'ultimo accesso al 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

## 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>
```

## METTI richiesta dell'ultimo tempo di accesso al 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'ultimo accesso utilizzando LA richiesta PUT bucket last access time (INSERISCI ultima ora di accesso bucket), la casella di controllo **S3 > Bucket > Change Last Access Setting** (Modifica ultima impostazione di accesso) in Tenant Manager o l'API di gestione tenant.

Se gli ultimi aggiornamenti dell'ora di accesso sono disattivati per un bucket, alle operazioni sul bucket viene applicato il seguente comportamento:

- LE richieste GET Object, GET Object ACL, GET Object Tagging e HEAD Object non aggiornano l'ultimo tempo di accesso. L'oggetto non viene aggiunto alle code per la valutazione ILM (Information Lifecycle Management).
- PUT Object (INSERISCI oggetto) - le richieste di tag degli oggetti di copia e INSERIMENTO che aggiornano solo i metadati aggiornano anche l'ultimo tempo di accesso. L'oggetto viene aggiunto alle code per la valutazione ILM.
- Se gli aggiornamenti dell'ultimo tempo di accesso sono disattivati per il bucket di origine, LE richieste PUT Object - Copy non aggiornano l'ultimo tempo di 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, PUT Object - le richieste di copia aggiornano sempre l'ultimo tempo di accesso. La copia dell'oggetto viene aggiunta alle code per la valutazione ILM.
- Le richieste complete di caricamento Multipart aggiornano l'ultimo tempo di 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Questo esempio disattiva l'ultimo tempo di accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

#### Informazioni correlate

["Utilizzare un account tenant"](#)

## ELIMINA la richiesta di configurazione della 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

## OTTIENI una richiesta di configurazione per la 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

## 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

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

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"> <li>• es deve essere il terzo elemento.</li> <li>• L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form domain-name/myindex/mytype.</li> </ul> <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> <li>• arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>L'endpoint deve essere configurato prima 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

`<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 `current` e digitare `named 2017` Che è ospitato in un dominio AWS denominato `records`.

```

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-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

## Informazioni correlate

["Utilizzare un account tenant"](#)

## INSERIRE la richiesta di 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 oggetti con il prefisso /images a una destinazione e agli oggetti con il prefisso /videos a un altro.

Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, una configurazione che includeva una regola per gli oggetti con il prefisso test e una seconda regola per gli oggetti con il prefisso test2 non sarebbe consentito.

Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID. L'endpoint deve esistere quando viene inviata la configurazione della notifica dei metadati, oppure la richiesta non riesce come a. 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
MetadataNotificationConfiguration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati.  Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato.  Le regole con prefissi sovrapposti vengono rifiutate.  Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola.  Incluso nell'elemento Rule.	No

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

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"> <li>• es deve essere il terzo elemento.</li> <li>• L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form domain-name/myindex/mytype.</li> </ul> <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> <li>• arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>L'endpoint deve essere configurato prima 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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 per gli oggetti che corrispondono al prefisso `/images` viene inviato a una destinazione, mentre i metadati degli oggetti per gli oggetti che corrispondono al prefisso `/videos` viene inviato a una seconda destinazione.

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

## Informazioni correlate

["Utilizzare un account tenant"](#)

## 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. Il test bucket non è configurato, quindi il versionId tag vuoto.

```
{
  "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.

<b>Tipo</b>	<b>Nome dell'elemento</b>	<b>Descrizione</b>
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	Area bucket, ad esempio us-east-1
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

**Nota:** 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.

## 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 storage utilizzata da un account e dai relativi bucket può essere ottenuta tramite una richiesta GET Service modificata con `x-ntap-sg-usage` parametro di 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 coerenza globale, StorageGRID tenta di recuperare le informazioni sull'utilizzo in modo coerente con il 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

### 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 a `ObjectCount` e `DataBytes` valori nella risposta. I contrassegni di eliminazione non vengono aggiunti a `ObjectCount` totale.

## Informazioni correlate

["Controlli di coerenza"](#)

## 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 automaticamente quando si esegue l'aggiornamento a StorageGRID 11.5. 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.

["Utilizzo di S3 Object Lock"](#)

["Gestire gli oggetti con ILM"](#)

["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

**Deprecato: 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.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3.

["Utilizzo di S3 Object Lock"](#)

["Gestire gli oggetti con ILM"](#)

["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. Il seguente messaggio di errore viene visualizzato se si tenta di utilizzare LE modifiche DELLA richiesta PUT bucket per la conformità per creare un nuovo bucket Compliance:

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

**Informazioni correlate**

["Gestire gli oggetti con ILM"](#)

["Utilizzare un account tenant"](#)

**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.

["Utilizzo di S3 Object Lock"](#)

["Gestire gli oggetti con ILM"](#)

["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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

## Esempio di risposta

Nella risposta XML, <SGCompliance> elenca le impostazioni di compliance 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: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
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.

Nome	Descrizione
LegalHold	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.</li> </ul>
Eliminazione automatica	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.</li> </ul>

## 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.

### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Utilizzare un account tenant"](#)

### Deprecato: INSERIRE la richiesta di conformità del bucket

La richiesta DI compliance DEL bucket PUT 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.

["Utilizzo di S3 Object Lock"](#)

["Gestire gli oggetti con ILM"](#)

["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 compliance per il bucket denominato `mybucket`. In questo esempio, gli oggetti in `mybucket` verrà ora conservato per due anni (1,051,200 minuti) invece di un anno, a partire dal momento in cui l'oggetto viene acquisito 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: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
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><b>Attenzione:</b> 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; è possibile solo aumentarlo.</p>
LegalHold	<ul style="list-style-type: none"><li>• 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.</li><li>• Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.</li></ul>

Nome	Descrizione
Eliminazione automatica	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.</li> </ul>

## Livello di 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 il livello di coerenza **strong-Global** per garantire che tutti i siti del data center e tutti i nodi di storage che contengono metadati bucket abbiano coerenza di lettura dopo scrittura per le impostazioni di conformità modificate.

Se StorageGRID non riesce a raggiungere il livello di coerenza **strong-Global** perché un sito del data center o più nodi di storage 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 del grid non è in grado di rendere disponibile una quantità sufficiente di nodi di storage in ogni sito, il supporto tecnico potrebbe richiedere di riprovare la richiesta non riuscita forzando il livello di coerenza **strong-Site**.



Non forzare mai il livello di coerenza **strong-site** per LA compliance DEL bucket PUT, a meno che non sia stato richiesto dal supporto tecnico e a meno che non si comprendano le potenziali conseguenze dell'utilizzo di questo livello.

Quando il livello di coerenza viene ridotto a **strong-Site**, StorageGRID garantisce che le impostazioni di conformità aggiornate avranno una coerenza di lettura dopo scrittura solo per le richieste dei 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 sotto un blocco legale e si forza un livello di coerenza inferiore, le impostazioni di conformità precedenti del bucket (ovvero, blocco legale) potrebbero continuare a essere in vigore in alcuni siti del 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'utilizzo del livello di coerenza **strong-site**, emettere nuovamente la richiesta DI conformità PUT bucket e includere **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` 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"](#)

["Utilizzare un account tenant"](#)

["Gestire gli oggetti con ILM"](#)

## Policy di accesso a bucket e gruppi

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 due tipi di policy di accesso.

- **Le policy bucket**, configurate utilizzando le policy GET bucket, PUT bucket e DELETE Bucket Policy S3 API Operations. 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.

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": "*"
```

Nell'esempio seguente, l'istruzione utilizza gli elementi Effect, Principal, Action e Resource. Questo esempio mostra un'istruzione completa di policy bucket che utilizza l'effetto "allow" per assegnare i Principal, il gruppo di amministrazione `federated-group/admin` e il gruppo finanziario `federated-group/finance`, Autorizzazioni per eseguire l'azione `s3>ListBucket` sul bucket denominato `mybucket` E l'azione `s3GetObject` su tutti gli oggetti all'interno del bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ],
        "Action": [
          "s3>ListBucket",
          "s3GetObject"
        ],
        "Resource": [
          "arn:aws:iam:s3:::mybucket",
          "arn:aws:iam: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.

#### Informazioni correlate

["Utilizzare un account tenant"](#)

#### Impostazioni di controllo della coerenza per i criteri

Per impostazione predefinita, gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Una volta che un criterio di gruppo diventa coerente, le modifiche possono richiedere altri 15 minuti per essere effettive, a causa del caching delle policy. Per impostazione predefinita, anche gli aggiornamenti apportati alle policy del bucket

sono coerenti.

Come richiesto, è possibile modificare le garanzie di coerenza per gli aggiornamenti delle policy bucket. Ad esempio, è possibile che una modifica a una policy bucket diventi effettiva il prima possibile per motivi di sicurezza.

In questo caso, è possibile impostare `Consistency-Control` nella richiesta di policy PUT bucket, oppure puoi utilizzare la richiesta DI coerenza PUT bucket. Quando si modifica il controllo di coerenza per questa richiesta, è necessario utilizzare il valore `all`, che fornisce la massima garanzia di coerenza di lettura dopo scrittura. Se si specifica qualsiasi altro valore di controllo di coerenza in un'intestazione per la richiesta di coerenza PUT bucket, la richiesta verrà rifiutata. Se si specifica qualsiasi altro valore per una richiesta di policy PUT bucket, il valore verrà ignorato. Una volta che una policy bucket diventa coerente, le modifiche possono richiedere altri 8 secondi per essere effettive, a causa del caching delle policy.

 Se si imposta il livello di coerenza su **tutto** per forzare l'entrata in vigore di una nuova policy di bucket, assicurarsi di ripristinare il valore originale del controllo a livello di bucket al termine dell'operazione. In caso contrario, tutte le future richieste di bucket utilizzeranno l'impostazione `all`.

## Utilizzo dell'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 del criterio PUT bucket deve essere codificato con `charset=UTF-8`.

## Specifiche delle 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 l'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.

## Informazioni correlate

["Specifiche delle variabili in un criterio"](#)

## Specifiche delle 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, le entità sono indicate 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 federato ("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 lasci l'organizzazione e il nome utente Alex viene cancellato. Se un nuovo Alex entra a far parte dell'organizzazione e viene assegnato lo stesso Alex nome utente, il nuovo utente potrebbe ereditare involontariamente 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.

### Specifiche delle 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 le azioni di replica PUT e DELETE bucket. StorageGRID utilizza autorizzazioni separate per ciascuna azione, che corrispondono alla specifica originale di Amazon S3.



L'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	METTI bucket	
s3:Deletebucket	ELIMINA bucket	
s3:DeleteBucketMetadataNotification	ELIMINA la configurazione di notifica dei metadati del bucket	Sì
s3:DeleteBucketPolicy	ELIMINA policy bucket	
s3:DeleteReplicationConfiguration	ELIMINA replica bucket	Sì, separare i permessi per PUT ed DELETE*
s3:GetBucketAcl	OTTIENI ACL bucket	
s3:GetBucketCompliance	OTTIENI compliance bucket (obsoleta)	Sì
s3:GetBucketConsistency	COERENZA del bucket	Sì
s3:GetBucketCORS	OTTIENI bucket cors	
s3:GetEncryptionConfiguration	OTTIENI la crittografia bucket	
s3:GetBucketLastAccessTime	OTTIENI l'ultimo tempo di accesso a bucket	Sì
s3:GetBucketLocation	OTTIENI posizione bucket	
s3:GetBucketMetadataNotification	OTTIENI la configurazione della notifica dei metadati del bucket	Sì
s3:GetBucketNotification	OTTIENI notifica bucket	
s3:GetBucketObjectLockConfiguration	OTTIENI configurazione blocco oggetto	
s3:GetBucketPolicy	OTTIENI la policy bucket	
s3:GetBucketTagging	OTTIENI il contrassegno bucket	
s3:GetBucketVersioning	SCARICA la versione di bucket	
s3:GetLifecycleConfiguration	OTTIENI il ciclo di vita del bucket	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:GetReplicationConfiguration	OTTIENI la replica bucket	
s3>ListAllMyBucket	<ul style="list-style-type: none"> <li>OTTIENI assistenza</li> <li>OTTIENI l'utilizzo dello storage</li> </ul>	Sì, per OTTENERE l'utilizzo dello storage
s3>ListBucket	<ul style="list-style-type: none"> <li>OTTIENI bucket (Elenca oggetti)</li> <li>BENNA PER LA TESTA</li> <li>RIPRISTINO POST-oggetto</li> </ul>	
s3>ListBucketMultipartUploads	<ul style="list-style-type: none"> <li>Elenca caricamenti multipart</li> <li>RIPRISTINO POST-oggetto</li> </ul>	
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"> <li>DELETE Bucket cors† (ELIMINA cors bucket)</li> <li>METTI cors bucket</li> </ul>	
s3:PutEncryptionConfiguration	<ul style="list-style-type: none"> <li>ELIMINA crittografia bucket</li> <li>METTI la crittografia bucket</li> </ul>	
s3:PutBucketLastAccessTime	TEMPO ULTIMO accesso bucket	Sì
s3:PutBucketMetadataNotification	INSERIRE la configurazione della notifica dei metadati del bucket	Sì
s3:PutBucketNotification	NOTIFICA DEL bucket	
s3:PutBucketObjectLockConfiguration	POSIZIONARE la benna con x-amz-bucket-object-lock-enabled: true Intestazione della richiesta (richiede anche l'autorizzazione s3>CreateBucket)	
s3:PutBucketPolicy	METTI la policy bucket	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:PutBucketTagging	<ul style="list-style-type: none"> <li>• ELIMINA contrassegno bucket†</li> <li>• INSERIRE il contrassegno bucket</li> </ul>	
s3:PutBucketVersioning	METTERE il bucket in versione	
s3:PutLifecycleConfiguration	<ul style="list-style-type: none"> <li>• ELIMINA ciclo di vita bucket†</li> <li>• METTI IL ciclo di vita del bucket</li> </ul>	
s3:PutReplicationConfiguration	METTI la replica del bucket	Sì, separare i permessi per PUT ed DELETE*

#### Autorizzazioni applicabili agli oggetti

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:AbortMultipartUpload	<ul style="list-style-type: none"> <li>• Interrompi caricamento multiparte</li> <li>• RIPRISTINO POST-oggetto</li> </ul>	
s3:DeleteObject	<ul style="list-style-type: none"> <li>• ELIMINA oggetto</li> <li>• ELIMINARE più oggetti</li> <li>• RIPRISTINO POST-oggetto</li> </ul>	
s3:DeleteObjectTagging	ELIMINA tag oggetti	
s3:DeleteObjectVersionTagging	DELETE Object Tagging (ELIMINA tag oggetti) (una versione specifica dell'oggetto)	
s3:DeleteObjectVersion	DELETE Object (UNA versione specifica dell'oggetto)	
s3:GetObject	<ul style="list-style-type: none"> <li>• OTTIENI oggetto</li> <li>• Oggetto TESTA</li> <li>• RIPRISTINO POST-oggetto</li> </ul>	
s3:GetObjectAcl	GET Object ACL (OTTIENI ACL oggetto)	
s3:GetObjectLegalHold	OTTENERE un blocco legale degli oggetti	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:GetObjectRetention	OTTIENI la conservazione degli oggetti	
s3:GetObjectTagging	OTTIENI tag oggetti	
s3:GetObjectVersionTagging	GET Object Tagging (OTTIENI tag oggetti) (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GET Object (UNA versione specifica dell'oggetto)	
s3>ListMultipartUploadParts	List Parts, POST-ripristino degli oggetti	
s3:PutObject	<ul style="list-style-type: none"> <li>• METTI oggetto</li> <li>• METTI oggetto - Copia</li> <li>• RIPRISTINO POST-oggetto</li> <li>• Avvia caricamento multiparte</li> <li>• Caricamento multiparte completo</li> <li>• Carica parte</li> <li>• Carica parte - Copia</li> </ul>	
s3:PutObjectLegalHold	METTERE in attesa legale l'oggetto	
s3:PutObjectRetention	METTI la conservazione degli oggetti	
s3:PutObjectTagging	INSERIRE tag oggetti	
s3:PutObjectVersionTagging	PUT Object Tagging (UNA versione specifica dell'oggetto)	
s3:PutOverwriteObject	<ul style="list-style-type: none"> <li>• METTI oggetto</li> <li>• METTI oggetto - Copia</li> <li>• INSERIRE tag degli oggetti</li> <li>• ELIMINA tag oggetti</li> <li>• Caricamento multiparte completo</li> </ul>	Sì

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:RestoreObject (Riavvia oggetto)	RIPRISTINO POST-oggetto	

## Utilizzando 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 la versione S3 è attivata, l'impostazione Nega impedisce alle operazioni DI TAGGING OGGETTI PUT o DELETE 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 il criterio S3 corrente 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 il tagging degli oggetti. Inoltre, se la casella di controllo **Impedisci modifica client** è selezionata (**Configurazione > Opzioni griglia**), l'impostazione sovrascrive l'impostazione dell'autorizzazione PutOverwriteObject.

## Informazioni correlate

["Esempi di criteri di gruppo S3"](#)

## Specifiche delle 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: {
  <em>condition_type</em>: {
    <em>condition_key</em>: <em>condition_values</em>
```

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). Possono includere * e ? caratteri jolly.
StringNotLike	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole). Possono includere * e ? caratteri jolly.
Valori numerici Equals	Confronta una chiave con un valore numerico in base alla corrispondenza esatta.

Condizionare gli operatori	Descrizione
NumericNotEquals	Confronta una chiave con un valore numerico in base alla corrispondenza negata.
NumericGreaterThan	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore di".
NumericGreaterThanOrEqual	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore o uguale a".
NumericLessThan	Confronta una chiave con un valore numerico in base alla corrispondenza "meno di".
NumericLessThanOrEqual	Confronta una chiave con un valore numerico in base alla corrispondenza "minore o uguale a".
Bool	Confronta una chiave con un valore booleano in base alla 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.
Nullo	Controlla se è presente una chiave di condizione nel contesto della richiesta corrente.

#### Chiavi di condizione supportate

Categoria	Chiavi di condizione applicabili	Descrizione
Operatori IP	aws: Sourcelp	<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><b>Nota:</b> 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><b>Nota:</b> 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 l'intestazione verrà ignorata poiché non è possibile verificarne la validità.</p>
Risorsa/identità	aws:nome utente	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:ListBucket e. S3:autorizzazioni ListBucketVersions	s3:delimitatore	Viene confrontato con il parametro delimitatore specificato in una richiesta GET bucket o GET Bucket Object Versions.
S3:ListBucket e. S3:autorizzazioni ListBucketVersions	s3: tasti max	Viene confrontato con il parametro max-keys specificato in una richiesta GET bucket o GET Bucket Object Versions.
S3:ListBucket e. S3:autorizzazioni ListBucketVersions	s3:prefisso	Viene confrontato con il parametro di prefisso specificato in una richiesta DI versioni DI oggetti GET Bucket o GET Bucket.

### Specifiche delle 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 in Resource confronto tra elementi e stringhe in Condition elementi.

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 della condizione nel blocco condition:

```
"Condition": {  
    "StringLike": {  
        "s3:prefix": "${aws:username}/*"  
        ...  
    },  
    ...  
}
```

Variabile	Descrizione
\${aws:SourceIp}	Utilizza la chiave SourceIp come variabile fornita.
\${aws:username}	Utilizza la chiave Username come variabile fornita.
\${s3:prefix}	Utilizza la chiave di prefisso specifica del servizio come variabile fornita.
\${s3:max-keys}	Utilizza la chiave max-keys specifica del servizio come variabile fornita.
\${*}	Carattere speciale. Utilizza il carattere come carattere * letterale.
\${?}	Carattere speciale. Utilizza il carattere come letterale ? carattere.
\${\$}	Carattere speciale. Utilizza il carattere come carattere letterale.

### Creazione di 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

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Principal è un gruppo locale	Bucket	Principal non valido	Valido
La policy concede a un account non proprietario (inclusi gli account anonimi) le autorizzazioni PER INSERIRE gli 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, selezionare **Configuration > Grid Options** e selezionare la casella di controllo **Impedisci modifica 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 PUT object ALLOW al criterio S3.



L'impostazione di DeleteObject per NEGARE 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 (vedere la 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

["Gestire gli oggetti con ILM"](#)

["Creazione di policy che richiedono una gestione speciale"](#)

["Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID"](#)

["Esempi di criteri di gruppo S3"](#)

## Esempi di policy S3

Utilizza gli esempi di questa sezione per creare policy di accesso StorageGRID per bucket e gruppi.

### Esempi di policy del bucket S3

I criteri del bucket specificano le autorizzazioni di accesso per il bucket a cui è associata la policy. I criteri del bucket vengono configurati utilizzando l'API S3 PutBucketPolicy.

È possibile configurare un criterio bucket utilizzando l'interfaccia CLI AWS seguendo il seguente comando:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
<em>file://policy.json</em>
```

### Esempio: Consentire a tutti l'accesso in sola lettura a un bucket

In questo esempio, Everyone, incluso l'anonimo, è autorizzato a elencare gli oggetti nel bucket ed eseguire operazioni Get Object su tutti gli oggetti nel bucket. Tutte le altre operazioni verranno negate. Si noti che questo criterio potrebbe non essere particolarmente utile in quanto 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 shared/ prefisso chiave 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 specificato

In questo esempio, chiunque, incluso anonimo, può elencare il bucket ed eseguire operazioni GET Object su tutti gli oggetti nel bucket, mentre solo gli utenti appartengono al gruppo Marketing nell'account specificato è consentito l'accesso completo.

```
{
  "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 a examplebucket bucket e i suoi 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, il Deny Effect per PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e il tagging 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/*"
    }
  ]
}
```

## Informazioni correlate

["Operazioni sui bucket"](#)

## Esempi di criteri di gruppo S3

I criteri di gruppo specificano le autorizzazioni di accesso per il gruppo a cui è associato il criterio. Non c'è `Principal` elemento nel criterio poiché è implicito. I criteri di gruppo vengono configurati utilizzando il tenant Manager o l'API.

## Esempio: Impostazione dei criteri di gruppo utilizzando il tenant Manager

Quando si utilizza Tenant Manager per aggiungere o modificare un gruppo, è possibile selezionare la modalità di creazione dei criteri di gruppo che definiscono i permessi di accesso S3 di cui disporranno i membri di questo gruppo, come indicato di seguito:

- **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.
- **Personalizzato:** Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

In questo esempio, i membri del gruppo possono solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato.



## 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",
        "s3GetObject",
        "s3GetObjectTagging",
        "s3GetObjectVersion",
        "s3GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::/*"
    }
  ]
}
```

### Esempio: Consentire ai membri del gruppo di accedere completamente solo alla “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}/*"
    }
  ]
}

```

## Informazioni correlate

["Utilizzare un account tenant"](#)

["Utilizzando l'autorizzazione PutOverwriteObject"](#)

["Protezione WORM \(Write-Once-Read-Many\)"](#)

## Configurazione della sicurezza per l'API REST

È necessario esaminare le misure di sicurezza implementate per L'API REST e comprendere come proteggere il sistema.

### In che modo StorageGRID fornisce la sicurezza per l'API REST

È necessario comprendere in che modo il sistema StorageGRID implementa la sicurezza, l'autenticazione e l'autorizzazione per l'API REST.

StorageGRID utilizza le seguenti misure di sicurezza.

- Le comunicazioni del client con il servizio Load Balancer utilizzano HTTPS se HTTPS è configurato per l'endpoint del bilanciamento del carico.

Quando si configura un endpoint di bilanciamento del carico, è possibile attivare HTTP. Ad esempio, è possibile utilizzare HTTP per test o altri scopi non di produzione. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

- Per impostazione predefinita, StorageGRID utilizza HTTPS per le comunicazioni client con i nodi di storage e il servizio CLB sui nodi gateway.

È possibile abilitare HTTP per queste connessioni. Ad esempio, è possibile utilizzare HTTP per test o altri scopi non di produzione. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.



Il servizio CLB è obsoleto.

- Le comunicazioni tra StorageGRID e il client vengono crittografate mediante TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di storage all'interno della griglia vengono crittografate indipendentemente dal fatto che l'endpoint del bilanciamento del carico sia configurato per accettare connessioni HTTP o HTTPS.
- I client devono fornire le intestazioni di autenticazione HTTP a StorageGRID per eseguire operazioni REST API.

#### Certificati di sicurezza e applicazioni client

I client possono connettersi al servizio Load Balancer sui nodi Gateway o sui nodi Admin, direttamente ai nodi Storage o al servizio CLB sui nodi Gateway.

In tutti i casi, le applicazioni client possono stabilire connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dal sistema StorageGRID:

- Quando le applicazioni client si connettono al servizio Load Balancer, utilizzano il certificato configurato per l'endpoint specifico del bilanciamento del carico utilizzato per stabilire la connessione. Ogni endpoint dispone di un proprio certificato, ovvero un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dall'amministratore della griglia in StorageGRID durante la configurazione dell'endpoint.
- Quando le applicazioni client si connettono direttamente a un nodo di storage o al servizio CLB sui nodi gateway, utilizzano i certificati server generati dal sistema e generati per i nodi di storage al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema), oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia.

I client devono essere configurati in modo da considerare attendibile l'autorità di certificazione che ha firmato il certificato utilizzato per stabilire connessioni TLS.

Consultare le istruzioni per l'amministrazione di StorageGRID per informazioni sulla configurazione degli endpoint del bilanciamento del carico e per istruzioni sull'aggiunta di un singolo certificato server personalizzato per le connessioni TLS direttamente ai nodi di storage o al servizio CLB sui nodi gateway.

#### Riepilogo

La seguente tabella mostra come vengono implementati i problemi di sicurezza nelle API S3 e Swift REST:

Problema di sicurezza	Implementazione per API REST
Sicurezza della connessione	TLS
Autenticazione del server	Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore

Problema di sicurezza	Implementazione per API REST
Autenticazione del client	<ul style="list-style-type: none"> <li>• S3: Account S3 (ID chiave di accesso e chiave di accesso segreta)</li> <li>• Swift: Account Swift (nome utente e password)</li> </ul>
Autorizzazione del client	<ul style="list-style-type: none"> <li>• S3: Proprietà del bucket e tutte le policy di controllo degli accessi applicabili</li> <li>• Swift: Accesso al ruolo di amministratore</li> </ul>

#### Informazioni correlate

["Amministrare StorageGRID"](#)

#### Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un set limitato di suite di crittografia che le applicazioni client possono utilizzare quando si stabilisce una sessione TLS (Transport Layer Security).

#### Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3.



SSLv3 e TLS 1.1 (o versioni precedenti) non sono più supportati.

#### Suite di crittografia supportate

Versione TLS	IANA nome della suite di crittografia
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHACHA20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

#### Suite di crittografia obsolete

Le seguenti suite di crittografia sono obsolete. Il supporto per questi cifrari verrà rimosso in una release futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256

## Nome IANA

TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

### Informazioni correlate

["Come configurare le connessioni client"](#)

## Operazioni di monitoraggio e controllo

È possibile monitorare i carichi di lavoro e le efficienze per le operazioni dei client visualizzando le tendenze delle transazioni per l'intero grid o per nodi specifici. È possibile utilizzare i messaggi di audit per monitorare le operazioni e le transazioni dei client.

- ["Monitoraggio delle velocità di acquisizione e recupero degli oggetti"](#)
- ["Accesso e revisione dei registri di audit"](#)

### Monitoraggio delle velocità di acquisizione e recupero degli oggetti

È possibile monitorare i tassi di acquisizione e recupero degli oggetti, nonché le metriche per i conteggi degli oggetti, le query e la verifica. È possibile visualizzare il numero di tentativi riusciti e non riusciti da parte delle applicazioni client di lettura, scrittura e modifica degli oggetti nel sistema StorageGRID.

#### Fasi

1. Accedere a Grid Manager utilizzando un browser supportato.
2. Nella dashboard, individuare la sezione Protocol Operations (operazioni protocollo).

In questa sezione viene riepilogato il numero di operazioni client eseguite dal sistema StorageGRID. Le velocità dei protocolli vengono calcolate in media negli ultimi due minuti.

3. Selezionare **nodi**.
4. Dalla home page dei nodi (livello di implementazione), fare clic sulla scheda **Load Balancer**.

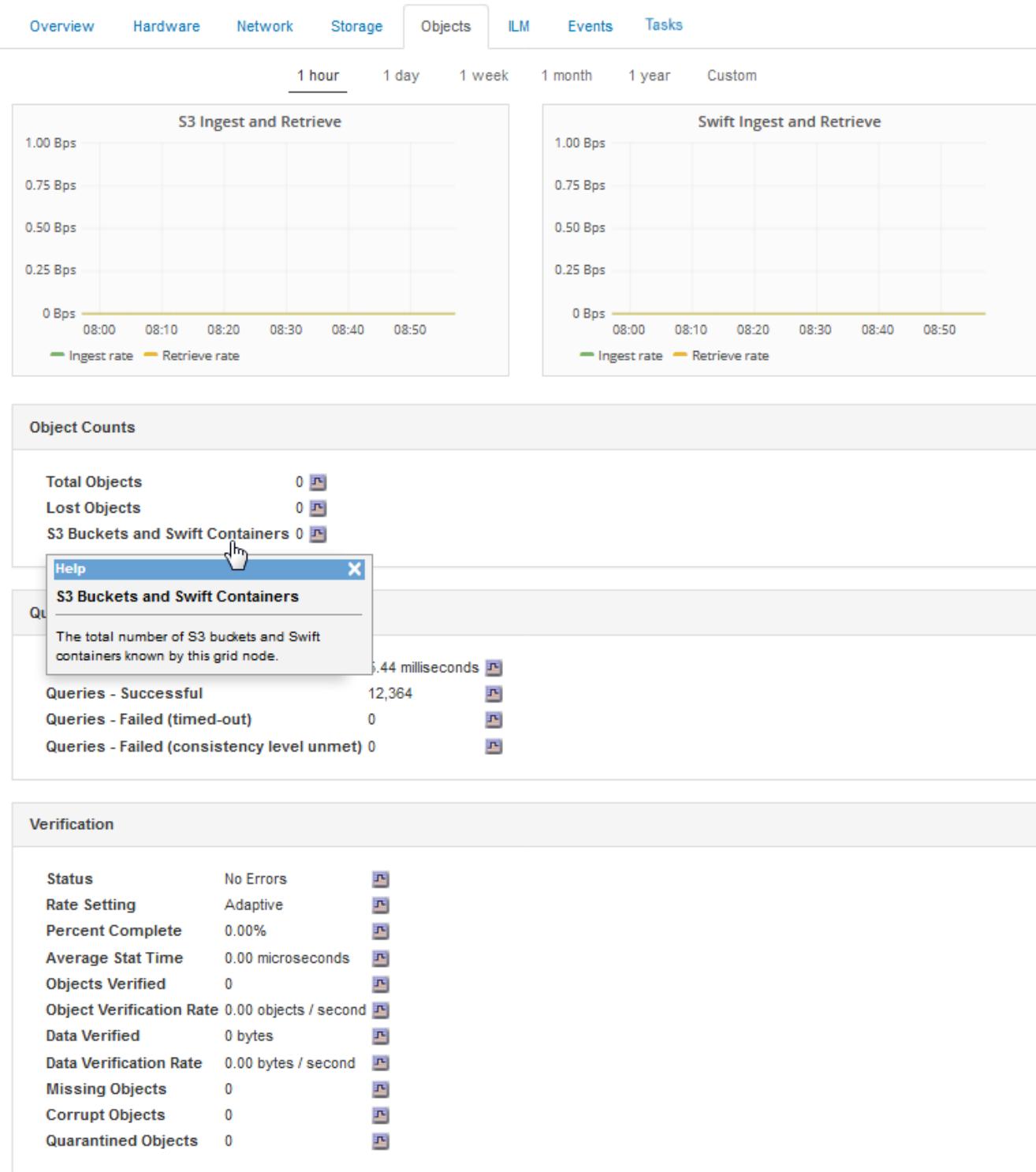
I grafici mostrano i trend di tutto il traffico client diretto agli endpoint del bilanciamento del carico all'interno della griglia. È possibile selezionare un intervallo di tempo in ore, giorni, settimane, mesi o anni, in alternativa, è possibile applicare un intervallo personalizzato.

5. Dalla home page dei nodi (livello di implementazione), fare clic sulla scheda **oggetti**.

Il grafico mostra le velocità di acquisizione e recupero dell'intero sistema StorageGRID in byte al secondo e byte totali. È possibile selezionare un intervallo di tempo in ore, giorni, settimane, mesi o anni, in alternativa, è possibile applicare un intervallo personalizzato.

6. Per visualizzare le informazioni relative a un nodo di storage specifico, selezionarlo dall'elenco a sinistra e fare clic sulla scheda **oggetti**.

Il grafico mostra le velocità di acquisizione e recupero degli oggetti per questo nodo di storage. La scheda include anche metriche per il conteggio degli oggetti, le query e la verifica. È possibile fare clic sulle etichette per visualizzare le definizioni di queste metriche.



7. Se desideri ulteriori dettagli:

- Selezionare **supporto > Strumenti > topologia griglia**.
- Selezionare **Site > Overview > Main**.

La sezione API Operations (operazioni API) visualizza informazioni riepilogative per l'intera griglia.

- Selezionare **Storage Node > LDR > client application > Overview > Main**

La sezione Operations (operazioni) visualizza informazioni riepilogative per il nodo di storage selezionato.

## Accesso e revisione dei registri di audit

I messaggi di audit vengono generati dai servizi StorageGRID e memorizzati in file di log di testo. I messaggi di audit specifici delle API nei registri di audit forniscono dati critici di sicurezza, funzionamento e monitoraggio delle performance che possono aiutare a valutare lo stato di salute del sistema.

### Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo amministratore.

### A proposito di questa attività

Il file di log di audit attivo viene denominato `audit.log` E viene memorizzato nei nodi di amministrazione.

Una volta al giorno, il file audit.log attivo viene salvato e viene visualizzato un nuovo file audit.log il file viene avviato. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato `yyyy-mm-dd.txt.gz`, che conserva la data originale.

In questo esempio viene visualizzato il valore attivo audit.log file del giorno precedente (2018-04-15.txt) e il file compresso per il giorno precedente (2018-04-14.txt.gz).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

### Fasi

1. Accedere a un nodo amministratore:
  - a. Immettere il seguente comando:  
`ssh admin@primary_Admin_Node_IP`
  - b. Immettere la password elencata in `Passwords.txt` file.

2. Accedere alla directory contenente i file di log di controllo:

```
cd /var/local/audit/export
```

3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

### Operazioni S3 registrate nei registri di audit

Nei registri di audit di StorageGRID vengono registrate diverse operazioni bucket e operazioni a oggetti.

## Operazioni bucket registrate nei registri di audit

- ELIMINA bucket
- ELIMINA tag bucket
- ELIMINARE più oggetti
- OTTIENI bucket (Elenca oggetti)
- SCARICA le versioni degli oggetti bucket
- OTTIENI il contrassegno bucket
- BENNA PER LA TESTA
- METTI bucket
- METTI la compliance del bucket
- INSERIRE il contrassegno bucket
- METTERE il bucket in versione

## Operazioni a oggetti registrate nei registri di audit

- Caricamento multiparte completo
- Parte di caricamento (quando la regola ILM utilizza comportamenti di acquisizione rigorosi o bilanciati)
- Parte di caricamento - Copia (quando la regola ILM utilizza comportamenti di acquisizione rigorosi o bilanciati)
- ELIMINA oggetto
- OTTIENI oggetto
- Oggetto TESTA
- RIPRISTINO POST-oggetto
- METTI oggetto
- METTI oggetto - Copia

### Informazioni correlate

["Operazioni sui bucket"](#)

["Operazioni sugli oggetti"](#)

## Vantaggi delle connessioni HTTP attive, inattive e simultanee

La modalità di configurazione delle connessioni HTTP può influire sulle prestazioni del sistema StorageGRID. Le configurazioni variano a seconda che la connessione HTTP sia attiva o inattiva o che si dispongano di più connessioni simultanee.

È possibile identificare i vantaggi in termini di prestazioni per i seguenti tipi di connessioni HTTP:

- Connessioni HTTP inattive
- Connessioni HTTP attive
- Connessioni HTTP simultanee

### Informazioni correlate

- ["I vantaggi di mantenere aperte le connessioni HTTP inattive"](#)
- ["Vantaggi delle connessioni HTTP attive"](#)
- ["Vantaggi delle connessioni HTTP simultanee"](#)
- ["Separazione dei pool di connessione HTTP per le operazioni di lettura e scrittura"](#)

### I vantaggi di mantenere aperte le connessioni HTTP inattive

È necessario mantenere aperte le connessioni HTTP anche quando le applicazioni client sono inattive per consentire alle applicazioni client di eseguire transazioni successive sulla connessione aperta. In base alle misurazioni del sistema e all'esperienza di integrazione, è necessario mantenere aperta una connessione HTTP inattiva per un massimo di 10 minuti. StorageGRID potrebbe chiudere automaticamente una connessione HTTP che rimane aperta e inattiva per più di 10 minuti.

Le connessioni HTTP aperte e inattive offrono i seguenti vantaggi:

- Latenza ridotta dal momento in cui il sistema StorageGRID stabilisce di eseguire una transazione HTTP al momento in cui il sistema StorageGRID può eseguire la transazione

La latenza ridotta è il vantaggio principale, in particolare per il tempo necessario per stabilire connessioni TCP/IP e TLS.

- Aumento della velocità di trasferimento dei dati mediante l'attivazione dell'algoritmo di avvio lento TCP/IP con i trasferimenti eseguiti in precedenza
- Notifica istantanea di diverse classi di condizioni di errore che interrompono la connettività tra l'applicazione client e il sistema StorageGRID

Determinare per quanto tempo mantenere aperta una connessione inattiva è un compromesso tra i benefici dell'avvio lento associati alla connessione esistente e l'allocazione ideale della connessione alle risorse di sistema interne.

### Vantaggi delle connessioni HTTP attive

Per le connessioni dirette ai nodi di storage o al servizio CLB (obsoleto) sui nodi gateway, è necessario limitare la durata di una connessione HTTP attiva a un massimo di 10 minuti, anche se la connessione HTTP esegue continuamente transazioni.

La determinazione della durata massima per cui una connessione deve essere mantenuta aperta è un compromesso tra i benefici della persistenza della connessione e l'allocazione ideale della connessione alle risorse di sistema interne.

Per le connessioni client ai nodi di storage o al servizio CLB, la limitazione delle connessioni HTTP attive offre i seguenti vantaggi:

- Consente un bilanciamento ottimale del carico nel sistema StorageGRID.

Quando si utilizza il servizio CLB, è necessario evitare connessioni TCP/IP di lunga durata per ottimizzare il bilanciamento del carico nel sistema StorageGRID. È necessario configurare le applicazioni client in modo da tenere traccia della durata di ciascuna connessione HTTP e chiudere la connessione HTTP dopo un determinato periodo di tempo, in modo da poter ristabilire e ribilanciare la connessione HTTP.

Il servizio CLB bilancia il carico nel sistema StorageGRID nel momento in cui un'applicazione client stabilisce una connessione HTTP. Con il passare del tempo, una connessione HTTP potrebbe non essere più ottimale con il variare dei requisiti di bilanciamento del carico. Il sistema esegue il miglior bilanciamento del carico quando le applicazioni client stabiliscono una connessione HTTP separata per ciascuna transazione, ma questo nega i guadagni molto più preziosi associati alle connessioni persistenti.



Il servizio CLB è obsoleto.

- Consente alle applicazioni client di indirizzare le transazioni HTTP ai servizi LDR che dispongono di spazio disponibile.
- Consente l'avvio delle procedure di manutenzione.

Alcune procedure di manutenzione vengono avviate solo dopo il completamento di tutte le connessioni HTTP in corso.

Per le connessioni client al servizio Load Balancer, la limitazione della durata delle connessioni aperte può essere utile per consentire l'avvio tempestivo di alcune procedure di manutenzione. Se la durata delle connessioni client non è limitata, potrebbero essere necessari alcuni minuti per terminare automaticamente le connessioni attive.

#### **Vantaggi delle connessioni HTTP simultanee**

Tenere aperte più connessioni TCP/IP al sistema StorageGRID per consentire il parallelismo, aumentando così le performance. Il numero ottimale di connessioni parallele dipende da diversi fattori.

Le connessioni HTTP simultanee offrono i seguenti vantaggi:

- Latenza ridotta

Le transazioni possono iniziare immediatamente invece di attendere il completamento di altre transazioni.

- Maggiore throughput

Il sistema StorageGRID può eseguire transazioni parallele e aumentare il throughput delle transazioni aggregate.

Le applicazioni client devono stabilire più connessioni HTTP. Quando un'applicazione client deve eseguire una transazione, può selezionare e utilizzare immediatamente qualsiasi connessione stabilita che non sta elaborando una transazione.

La topologia di ciascun sistema StorageGRID presenta un throughput di picco diverso per le transazioni e le connessioni simultanee prima che le performance comincino a degradarsi. Il throughput massimo dipende da fattori quali risorse di calcolo, risorse di rete, risorse di storage e collegamenti WAN. Anche il numero di server e servizi e il numero di applicazioni supportate dal sistema StorageGRID sono fattori.

I sistemi StorageGRID spesso supportano più applicazioni client. Tenere presente questo aspetto quando si determina il numero massimo di connessioni simultanee utilizzate da un'applicazione client. Se l'applicazione client è costituita da più entità software che stabiliscono connessioni al sistema StorageGRID, è necessario sommare tutte le connessioni tra le entità. Potrebbe essere necessario regolare il numero massimo di connessioni simultanee nelle seguenti situazioni:

- La topologia del sistema StorageGRID influisce sul numero massimo di transazioni e connessioni simultanee supportate dal sistema.
- Le applicazioni client che interagiscono con il sistema StorageGRID su una rete con larghezza di banda limitata potrebbero dover ridurre il grado di concorrenza per garantire che le singole transazioni vengano completate in un tempo ragionevole.
- Quando molte applicazioni client condividono il sistema StorageGRID, potrebbe essere necessario ridurre il grado di concorrenza per evitare di superare i limiti del sistema.

### Separazione dei pool di connessione HTTP per le operazioni di lettura e scrittura

È possibile utilizzare pool separati di connessioni HTTP per le operazioni di lettura e scrittura e controllare la quantità di un pool da utilizzare per ciascuno di essi. I pool separati di connessioni HTTP consentono di controllare meglio le transazioni e bilanciare i carichi.

Le applicazioni client possono creare carichi dominanti dal recupero (lettura) o dominanti dal negozio (scrittura). Con pool separati di connessioni HTTP per le transazioni di lettura e scrittura, è possibile regolare la quantità di ciascun pool da dedicare alle transazioni di lettura o scrittura.

## USA Swift

Scopri come le applicazioni client possono utilizzare l'API di OpenStack Swift per interfacciarsi con il sistema StorageGRID.

- ["Supporto API di OpenStack Swift in StorageGRID"](#)
- ["Configurazione di account e connessioni tenant"](#)
- ["Operazioni supportate da Swift REST API"](#)
- ["Operazioni API Swift REST di StorageGRID"](#)
- ["Configurazione della sicurezza per l'API REST"](#)
- ["Operazioni di monitoraggio e controllo"](#)

### Supporto API di OpenStack Swift in StorageGRID

StorageGRID supporta le seguenti versioni specifiche di Swift e HTTP.

Elemento	Versione
Specifiche Swift	OpenStack Swift Object Storage API v1 a novembre 2015
HTTP	1.1 per ulteriori informazioni su HTTP, vedere HTTP/1.1 (RFC 7230-35).  <b>Nota:</b> StorageGRID non supporta la pipelining HTTP/1.1.

### Informazioni correlate

### Cronologia del supporto delle API Swift in StorageGRID

È necessario essere a conoscenza delle modifiche apportate al supporto del sistema StorageGRID per l'API DI Swift REST.

Rilasciare	Commenti
11.5	Rimosso il controllo di coerenza debole. Verrà invece utilizzato il livello di coerenza disponibile.
11.4	Aggiunto supporto per TLS 1.3 e elenco aggiornato delle suite di crittografia TLS supportate. CLB è obsoleto. Aggiunta descrizione dell'interrelazione tra ILM e l'impostazione di coerenza.
11.3	Aggiornate le operazioni PUT object per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono all'acquisizione (le opzioni bilanciate e rigide per il comportamento di Ingest). Aggiunta descrizione delle connessioni client che utilizzano endpoint di bilanciamento del carico o gruppi ad alta disponibilità. Elenco aggiornato delle suite di crittografia TLS supportate. Le crittografia TLS 1.1 non sono più supportate.
11.2	Modifiche editoriali minori al documento.
11.1	Aggiunto supporto per l'utilizzo di HTTP per connessioni client Swift ai nodi grid. Aggiornate le definizioni dei controlli di coerenza.
11.0	Aggiunto supporto per 1,000 container per ciascun account tenant.
10.3	Aggiornamenti amministrativi e correzioni del documento. Rimosse le sezioni per la configurazione dei certificati server personalizzati.
10.2	Supporto iniziale dell'API Swift da parte del sistema StorageGRID. La versione attualmente supportata è OpenStack Swift Object Storage API v1.

### Come StorageGRID implementa l'API di Swift REST

Un'applicazione client può utilizzare le chiamate API DI SWIFT REST per connettersi ai nodi di storage e ai nodi gateway per creare container e memorizzare e recuperare oggetti. Ciò consente alle applicazioni orientate ai servizi sviluppate per OpenStack Swift

di connettersi allo storage a oggetti on-premise fornito dal sistema StorageGRID.

#### **Gestione rapida degli oggetti**

Una volta acquisiti gli oggetti Swift nel sistema StorageGRID, questi vengono gestiti dalle regole ILM (Information Lifecycle Management) nella policy ILM attiva del sistema. Le regole e i criteri ILM determinano il modo in cui StorageGRID crea e distribuisce le copie dei dati a oggetti e il modo in cui queste vengono gestite nel tempo. Ad esempio, una regola ILM potrebbe essere applicata agli oggetti in specifici contenitori Swift e potrebbe specificare che più copie di oggetti vengono salvate in diversi data center per un certo numero di anni.

Contattare l'amministratore di StorageGRID per informazioni su come le regole e le policy ILM della griglia influiranno sugli oggetti dell'account tenant Swift.

#### **Richieste client in conflitto**

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vittorie". La tempistica per la valutazione "ultimi successi" si basa su quando il sistema StorageGRID completa una data richiesta e non su quando i client Swift iniziano un'operazione.

#### **Garanzie e controlli di coerenza**

Per impostazione predefinita, StorageGRID fornisce coerenza di lettura dopo scrittura per gli oggetti appena creati ed eventuale coerenza per gli aggiornamenti degli oggetti e le operazioni HEAD. Qualsiasi GET che segue UN PUT completato con successo sarà in grado di leggere i dati appena scritti. Le sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni sono coerenti. Le sovrascritture in genere richiedono secondi o minuti per la propagazione, ma possono richiedere fino a 15 giorni.

StorageGRID consente inoltre di controllare la coerenza in base al container. È possibile modificare il controllo di coerenza per creare un compromesso tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage, come richiesto dall'applicazione.

#### **Informazioni correlate**

["Gestire gli oggetti con ILM"](#)

["OTTENERE una richiesta di coerenza dei container"](#)

["INVIO di una richiesta di coerenza del container"](#)

#### **Raccomandazioni per l'implementazione dell'API Swift REST**

Seguire questi consigli quando si implementa l'API di Swift REST per l'utilizzo con StorageGRID.

#### **Raccomandazioni per la gestione di oggetti inesistenti**

Se l'applicazione verifica regolarmente l'esistenza di un oggetto in un percorso in cui non si prevede l'effettiva esistenza dell'oggetto, utilizzare il controllo di coerenza "Available". Ad esempio, è necessario utilizzare il controllo di coerenza "Available" se l'applicazione esegue un'operazione HEAD in una posizione prima di eseguire un'operazione PUT in tale posizione.

In caso contrario, se l'operazione HEAD non trova l'oggetto, potrebbe essere visualizzato un numero elevato di errori 500 nel server interno se uno o più nodi di storage non sono disponibili.

È possibile impostare il controllo di coerenza "Available" per ciascun container utilizzando la richiesta DI

coerenza PUT container.

#### Raccomandazioni per i nomi degli oggetti

Non utilizzare valori casuali come primi quattro caratteri dei nomi degli oggetti. Si consiglia invece di utilizzare prefissi non casuali e non univoci, ad esempio image.

Se è necessario utilizzare caratteri casuali e univoci nei prefissi dei nomi degli oggetti, è necessario anteporre i nomi degli oggetti a un nome di directory. Ovvero, utilizzare questo formato:

```
mycontainer/mydir/f8e3-image3132.jpg
```

Invece di questo formato:

```
mycontainer/f8e3-image3132.jpg
```

#### Raccomandazioni per “range reads”

Se l'opzione **compress stored objects** è selezionata (**Configuration > System Settings > Grid Options**), le applicazioni client Swift dovrebbero evitare di eseguire operazioni GET object che specificano la restituzione di un intervallo di byte. Queste operazioni “range Read” sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. LE operazioni GET Object che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è molto 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.

#### Informazioni correlate

["OTTENERE una richiesta di coerenza dei container"](#)

["INVIO di una richiesta di coerenza del container"](#)

["Amministrare StorageGRID"](#)

## Configurazione di account e connessioni tenant

La configurazione di StorageGRID per accettare connessioni da applicazioni client richiede la creazione di uno o più account tenant e la configurazione delle connessioni.

#### Creazione e configurazione di account tenant Swift

È necessario un account tenant Swift prima che i client API Swift possano memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant dispone di un proprio ID account, di gruppi e utenti, nonché di container e oggetti.

Gli account del tenant Swift vengono creati da un amministratore del grid StorageGRID utilizzando il grid manager o l'API di gestione del grid.

Quando si crea un account tenant Swift, l'amministratore della griglia specifica le seguenti informazioni:

- Nome visualizzato per il tenant (l'ID account del tenant viene assegnato automaticamente e non può essere modificato)
- Facoltativamente, una quota di storage per l'account tenant, ovvero il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant. La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).
- Se l'SSO (Single Sign-on) non è in uso per il sistema StorageGRID, se l'account tenant utilizzerà la propria origine di identità o condividerà l'origine di identità della griglia e la password iniziale per l'utente root locale del tenant.
- Se SSO è attivato, quale gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant.

Una volta creato un account tenant Swift, gli utenti con l'autorizzazione Root Access possono accedere a Tenant Manager per eseguire attività come le seguenti:

- Impostazione della federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) e creazione di gruppi e utenti locali
- Monitoraggio dell'utilizzo dello storage

 Gli utenti Swift devono disporre dell'autorizzazione Root Access per accedere a Tenant Manager. Tuttavia, l'autorizzazione Root Access non consente agli utenti di autenticarsi nell'API SWIFT REST per creare container e acquisire oggetti. Gli utenti devono disporre dell'autorizzazione di amministratore Swift per autenticarsi nell'API DI Swift REST.

#### Informazioni correlate

["Amministrare StorageGRID"](#)

["Utilizzare un account tenant"](#)

["Endpoint API Swift supportati"](#)

#### Come configurare le connessioni client

Un amministratore di grid effettua scelte di configurazione che influiscono sul modo in cui i client Swift si connettono a StorageGRID per memorizzare e recuperare i dati. Le informazioni specifiche necessarie per effettuare una connessione dipendono dalla configurazione scelta.

Le applicazioni client possono memorizzare o recuperare oggetti connettendosi a una delle seguenti opzioni:

- Il servizio Load Balancer sui nodi Admin o Gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità (ha) di nodi Admin o nodi Gateway
- Il servizio CLB sui nodi gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità di nodi gateway



Il servizio CLB è obsoleto. I client configurati prima della release StorageGRID 11.3 possono continuare a utilizzare il servizio CLB sui nodi gateway. Tutte le altre applicazioni client che dipendono da StorageGRID per fornire il bilanciamento del carico devono connettersi utilizzando il servizio bilanciamento del carico.

- Nodi di storage, con o senza bilanciamento del carico esterno

Durante la configurazione di StorageGRID, un amministratore della griglia può utilizzare il gestore della griglia o l'API di gestione della griglia per eseguire le seguenti operazioni, tutte facoltative:

1. Configurare gli endpoint per il servizio Load Balancer.

È necessario configurare gli endpoint per utilizzare il servizio Load Balancer. Il servizio Load Balancer sui nodi di amministrazione o gateway distribuisce le connessioni di rete in entrata dalle applicazioni client ai nodi di storage. Quando si crea un endpoint di bilanciamento del carico, l'amministratore di StorageGRID specifica un numero di porta, se l'endpoint accetta connessioni HTTP o HTTPS, il tipo di client (S3 o Swift) che utilizzerà l'endpoint e il certificato da utilizzare per le connessioni HTTPS (se applicabile).

2. Configurare reti client non attendibili.

Se un amministratore di StorageGRID configura una rete client di un nodo come non attendibile, il nodo accetta solo connessioni in entrata sulla rete client su porte esplicitamente configurate come endpoint del bilanciamento del carico.

3. Configurare i gruppi ad alta disponibilità.

Se un amministratore crea un gruppo ha, le interfacce di rete di più nodi Admin o nodi Gateway vengono inserite in una configurazione di backup attivo. Le connessioni client vengono effettuate utilizzando l'indirizzo IP virtuale del gruppo ha.

Per ulteriori informazioni su ciascuna opzione, consultare le istruzioni per l'amministrazione di StorageGRID.

#### **Riepilogo: Indirizzi IP e porte per le connessioni client**

Le applicazioni client si connettono a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta di un servizio su tale nodo. Se sono configurati gruppi ad alta disponibilità (ha), le applicazioni client possono connettersi utilizzando l'indirizzo IP virtuale del gruppo ha.

#### **Informazioni necessarie per stabilire connessioni client**

La tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Per ulteriori informazioni, contattare l'amministratore di StorageGRID oppure consultare le istruzioni per l'amministrazione di StorageGRID per una descrizione di come trovare queste informazioni in Gestione griglia.

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Gruppo HA	Bilanciamento del carico	Indirizzo IP virtuale di un gruppo ha	<ul style="list-style-type: none"><li>• Porta endpoint del bilanciamento del carico</li></ul>
Gruppo HA	CLB <b>Nota:</b> il servizio CLB è obsoleto.	Indirizzo IP virtuale di un gruppo ha	<p>Porte Swift predefinite:</p> <ul style="list-style-type: none"><li>• HTTPS: 8083</li><li>• HTTP: 8085</li></ul>

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	<ul style="list-style-type: none"> <li>• Porta endpoint del bilanciamento del carico</li> </ul>
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	<ul style="list-style-type: none"> <li>• Porta endpoint del bilanciamento del carico</li> </ul>
Nodo gateway	CLB  <b>Nota:</b> il servizio CLB è obsoleto.	Indirizzo IP del nodo gateway  <b>Nota:</b> per impostazione predefinita, le porte HTTP per CLB e LDR non sono attivate.	Porte Swift predefinite: <ul style="list-style-type: none"> <li>• HTTPS: 8083</li> <li>• HTTP: 8085</li> </ul>
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte Swift predefinite: <ul style="list-style-type: none"> <li>• HTTPS: 18083</li> <li>• HTTP: 18085</li> </ul>

## Esempio

Per connettere un client Swift all'endpoint Load Balancer di un gruppo ha di nodi gateway, utilizzare un URL strutturato come mostrato di seguito:

- `https://VIP-of-HA-group:LB-endpoint-port`

Ad esempio, se l'indirizzo IP virtuale del gruppo ha è 192.0.2.6 e il numero di porta di un endpoint di bilanciamento del carico di Swift è 10444, un client Swift potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.6:10444`

È possibile configurare un nome DNS per l'indirizzo IP utilizzato dai client per la connessione a StorageGRID. Contattare l'amministratore di rete locale.

## Scelta dell'utilizzo di connessioni HTTPS o HTTP

Quando le connessioni client vengono eseguite utilizzando un endpoint Load Balancer, le connessioni devono essere effettuate utilizzando il protocollo (HTTP o HTTPS) specificato per tale endpoint. Per utilizzare HTTP per le connessioni client ai nodi di storage o al servizio CLB sui nodi gateway, è necessario abilitarne l'utilizzo.

Per impostazione predefinita, quando le applicazioni client si connettono ai nodi di storage o al servizio CLB sui nodi gateway, devono utilizzare HTTPS crittografato per tutte le connessioni. In alternativa, è possibile attivare connessioni HTTP meno sicure selezionando l'opzione **Enable HTTP Connection** grid (attiva connessione HTTP) in Grid Manager. Ad esempio, un'applicazione client potrebbe utilizzare il protocollo HTTP quando si verifica la connessione a un nodo di storage in un ambiente non di produzione.



Prestare attenzione quando si attiva HTTP per una griglia di produzione, poiché le richieste verranno inviate senza crittografia.



Il servizio CLB è obsoleto.

Se l'opzione **Enable HTTP Connection** (attiva connessione HTTP) è selezionata, i client devono utilizzare porte diverse per HTTP rispetto a quelle utilizzate per HTTPS. Consultare le istruzioni per l'amministrazione di StorageGRID.

#### Informazioni correlate

["Amministrare StorageGRID"](#)

### Verifica della connessione nella configurazione dell'API Swift

È possibile utilizzare l'interfaccia utente di Swift per verificare la connessione al sistema StorageGRID e per verificare che sia possibile leggere e scrivere oggetti nel sistema.

#### Di cosa hai bisogno

- Devi aver scaricato e installato python-swiftclient, il client della riga di comando di Swift.
- È necessario disporre di un account tenant Swift nel sistema StorageGRID.

#### A proposito di questa attività

Se la protezione non è stata configurata, è necessario aggiungere --insecure contrassegnare ciascuno di questi comandi.

#### Fasi

1. Eseguire una query sull'URL delle informazioni per l'implementazione di StorageGRID Swift:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

Ciò è sufficiente per verificare che l'implementazione di Swift sia funzionale. Per verificare ulteriormente la configurazione dell'account memorizzando un oggetto, continuare con i passaggi aggiuntivi.

2. Inserire un oggetto nel contenitore:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Ottenere il container per verificare l'oggetto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Eliminare l'oggetto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Eliminare il contenitore:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `'\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'`
delete test_container
```

#### Informazioni correlate

["Creazione e configurazione di account tenant Swift"](#)

["Configurazione della sicurezza per l'API REST"](#)

## Operazioni supportate da Swift REST API

Il sistema StorageGRID supporta la maggior parte delle operazioni nell'API Swift di OpenStack. Prima di integrare i client API di Swift REST con StorageGRID, esaminare i dettagli di implementazione per le operazioni di account, container e oggetti.

## Operazioni supportate in StorageGRID

Sono supportate le seguenti operazioni API Swift:

- ["Operazioni dell'account"](#)
- ["Operazioni container"](#)
- ["Operazioni a oggetti"](#)

## Intestazioni di risposta comuni per tutte le operazioni

Il sistema StorageGRID implementa tutte le intestazioni comuni per le operazioni supportate, come definito dall'API di storage a oggetti Swift v1 di OpenStack.

### Informazioni correlate

["OpenStack: API dello storage a oggetti"](#)

### Endpoint API Swift supportati

StorageGRID supporta i seguenti endpoint API Swift: URL info, URL auth e URL storage.

#### URL info

È possibile determinare le funzionalità e i limiti dell'implementazione di Swift di StorageGRID inviando una richiesta GET all'URL di base di Swift con il percorso /info.

`https://FQDN | Node IP:Swift Port/info/`

Nella richiesta:

- *FQDN* è il nome di dominio completo.
- *Node IP* È l'indirizzo IP del nodo di storage o del nodo gateway sulla rete StorageGRID.
- *Swift Port* È il numero di porta utilizzato per le connessioni API Swift sul nodo di storage o sul nodo gateway.

Ad esempio, il seguente URL info richiede informazioni a un nodo di storage con l'indirizzo IP 10.99.106.103 e utilizzando la porta 18083.

`https://10.99.106.103:18083/info/`

La risposta include le funzionalità dell'implementazione di Swift come dizionario JSON. Uno strumento client può analizzare la risposta JSON per determinare le funzionalità dell'implementazione e utilizzarle come vincoli per le successive operazioni di storage.

L'implementazione StorageGRID di Swift consente l'accesso non autenticato all'URL delle informazioni.

#### URL di autenticazione

Un client può utilizzare l'URL auth di Swift per l'autenticazione come utente di un account tenant.

`https://FQDN | Node IP:Swift Port/auth/v1.0/`

Specificare l'ID account tenant, il nome utente e la password come parametri in X-Auth-User e X-Auth-Key intestazioni delle richieste, come segue:

`X-Auth-User: Tenant_Account_ID:Username`

`X-Auth-Key: Password`

Nelle intestazioni della richiesta:

- *Tenant\_Account\_ID* È l'ID account assegnato da StorageGRID al momento della creazione del tenant

Swift. Si tratta dello stesso ID account tenant utilizzato nella pagina di accesso di Tenant Manager.

- *Username* È il nome di un utente tenant creato in Tenant Manager. Questo utente deve appartenere a un gruppo che dispone dell'autorizzazione di amministratore Swift. L'utente root del tenant non può essere configurato per utilizzare l'API REST Swift.

Se Identity Federation è abilitato per l'account tenant, fornire il nome utente e la password dell'utente federated dal server LDAP. In alternativa, fornire il nome di dominio dell'utente LDAP. Ad esempio:

X-Auth-User: *Tenant\_Account\_ID:Username@Domain\_Name*

- *Password* è la password per l'utente tenant. Le password utente vengono create e gestite in Tenant Manager.

La risposta a una richiesta di autenticazione riuscita restituisce un URL di storage e un token di autenticazione, come segue:

X-Storage-Url: `https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID`

X-Auth-Token: *token*

X-Storage-Token: *token*

Per impostazione predefinita, il token è valido per 24 ore dal momento della generazione.

I token vengono generati per un account tenant specifico. Un token valido per un account non autorizza un utente ad accedere a un altro account.

#### **URL dello storage**

Un'applicazione client può eseguire chiamate API SWIFT REST per eseguire operazioni di account, container e oggetti supportate su un nodo gateway o un nodo di storage. Le richieste di storage vengono indirizzate all'URL dello storage restituito nella risposta di autenticazione. La richiesta deve includere anche l'intestazione X-Auth-Token e il valore restituito dalla richiesta auth.

`https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID`

`[/container] [/object]`

X-Auth-Token: *token*

Alcune intestazioni di risposta dello storage che contengono statistiche di utilizzo potrebbero non riflettere numeri precisi per gli oggetti modificati di recente. Potrebbero essere necessari alcuni minuti per visualizzare numeri precisi in queste intestazioni.

Le seguenti intestazioni di risposta per le operazioni di account e container sono esempi di quelle che contengono statistiche di utilizzo:

- X-Account-Bytes-Used
- X-Account-Object-Count
- X-Container-Bytes-Used
- X-Container-Object-Count

## Informazioni correlate

["Come configurare le connessioni client"](#)

["Creazione e configurazione di account tenant Swift"](#)

["Operazioni dell'account"](#)

["Operazioni container"](#)

["Operazioni a oggetti"](#)

## Operazioni dell'account

Le seguenti operazioni API Swift vengono eseguite sugli account.

### OTTIENI un account

Questa operazione recupera l'elenco di container associato alle statistiche di utilizzo dell'account e dell'account.

È necessario il seguente parametro di richiesta:

- Account

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

I seguenti parametri di query di richiesta supportati sono facoltativi:

- Delimiter
- End\_marker
- Format
- Limit
- Marker
- Prefix

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 204 No Content" se l'account viene trovato e non ha contenitori o l'elenco container è vuoto; oppure una risposta "HTTP/1.1 200 OK" se l'account viene trovato e l'elenco container non è vuoto:

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count

- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

## Conto PRINCIPALE

Questa operazione recupera le informazioni e le statistiche dell'account da un account Swift.

È necessario il seguente parametro di richiesta:

- Account

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 204 No Content":

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

## Informazioni correlate

["Operazioni rapide monitorate nei registri di audit"](#)

## Operazioni container

StorageGRID supporta un massimo di 1,000 container per account Swift. Le seguenti operazioni API Swift vengono eseguite sui container.

### ELIMINA contenitore

Questa operazione rimuove un container vuoto da un account Swift in un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 204 No Content":

- Content-Length
- Content-Type
- Date
- X-Trans-Id

#### **OTTIENI container**

Questa operazione recupera l'elenco di oggetti associato al contenitore, insieme alle statistiche e ai metadati del contenitore in un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

I seguenti parametri di query di richiesta supportati sono facoltativi:

- Delimiter
- End\_marker
- Format
- Limit
- Marker
- Path
- Prefix

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 200 Success" o "HTTP/1.1 204 No Content":

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

## CONTENITORE DI TESTA

Questa operazione recupera le statistiche e i metadati dei container da un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 204 No Content":

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

## METTI container

Questa operazione crea un container per un account in un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 201 created" o "HTTP/1.1 202 accepted" (se il container esiste già in questo account):

- Content-Length
- Date
- X-Timestamp
- X-Trans-Id

Il nome di un container deve essere univoco nello spazio dei nomi StorageGRID. Se il container esiste in un altro account, viene restituita la seguente intestazione: "HTTP/1.1 409 Conflict".

## Informazioni correlate

"Operazioni rapide monitorate nei registri di audit"

## Operazioni a oggetti

Le seguenti operazioni API Swift vengono eseguite sugli oggetti.

### ELIMINA oggetto

Questa operazione elimina il contenuto e i metadati di un oggetto dal sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container
- Object

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione corretta restituisce le seguenti intestazioni di risposta con un `HTTP/1.1 204 No Content` risposta:

- Content-Length
- Content-Type
- Date
- X-Trans-Id

Durante l'elaborazione di una richiesta DI ELIMINAZIONE degli oggetti, 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 non è temporaneamente disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito.

Per ulteriori informazioni sull'eliminazione degli oggetti, vedere le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

### OTTIENI oggetto

Questa operazione recupera il contenuto dell'oggetto e recupera i metadati dell'oggetto da un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container
- Object

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Le seguenti intestazioni di richiesta sono opzionali:

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Un'esecuzione corretta restituisce le seguenti intestazioni con un `HTTP/1.1 200 OK` risposta:

- Accept-Ranges
- Content-Disposition, restituito solo se Content-Disposition metadati impostati
- Content-Encoding, restituito solo se Content-Encoding metadati impostati
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

#### **Oggetto TESTA**

Questa operazione recupera i metadati e le proprietà di un oggetto acquisito da un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container
- Object

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione corretta restituisce le seguenti intestazioni con una risposta "HTTP/1.1 200 OK":

- Accept-Ranges
- Content-Disposition, restituito solo se Content-Disposition metadati impostati
- Content-Encoding, restituito solo se Content-Encoding metadati impostati

- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

### **METTI oggetto**

Questa operazione crea un nuovo oggetto con dati e metadati oppure sostituisce un oggetto esistente con dati e metadati in un sistema StorageGRID.

StorageGRID supporta oggetti di dimensioni fino a 5 TB.



Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle “ultime vittorie”. La tempistica per la valutazione “ultimi successi” si basa su quando il sistema StorageGRID completa una data richiesta e non su quando i client Swift iniziano un’operazione.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container
- Object

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Le seguenti intestazioni di richiesta sono opzionali:

- Content-Disposition
- Content-Encoding

Non utilizzare chunked Content-Encoding Se la regola ILM applicata a un oggetto filtra gli oggetti in base alle dimensioni e utilizza il posizionamento sincrono all’acquisizione (le opzioni bilanciate o rigide per il comportamento di Ingest).

- Transfer-Encoding

Non utilizzare file compressi o a pezzi Transfer-Encoding Se la regola ILM applicata a un oggetto filtra gli oggetti in base alle dimensioni e utilizza il posizionamento sincrono all’acquisizione (le opzioni bilanciate o rigide per il comportamento di Ingest).

- Content-Length

Se una regola ILM filtra gli oggetti in base alle dimensioni e utilizza il posizionamento sincrono

all'acquisizione, è necessario specificare Content-Length.



Se non si seguono queste linee guida per Content-Encoding, Transfer-Encoding, e. Content-Length, StorageGRID deve salvare l'oggetto prima di poter determinare la dimensione dell'oggetto e applicare la regola ILM. In altre parole, per impostazione predefinita, StorageGRID deve creare copie temporanee di un oggetto in fase di acquisizione. In altri termini, StorageGRID deve utilizzare l'opzione di doppio commit per il comportamento di Ingest.

Per ulteriori informazioni sul posizionamento sincrono e sulle regole ILM, vedere le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

- Content-Type
- ETag
- X-Object-Meta-<name\> (metadati correlati agli oggetti)

Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario memorizzare il valore in un'intestazione definita dall'utente denominata x-Object-Meta-Creation-Time. Ad esempio:

```
X-Object-Meta-Creation-Time: 1443399726
```

Questo campo viene valutato come secondi dal 1° gennaio 1970.

- X-Storage-Class: reduced\_redundancy

Questa intestazione influisce sul numero di copie di oggetti create da StorageGRID se la regola ILM che corrisponde a un oggetto acquisito specifica un comportamento Ingest di doppio commit o bilanciato.

- **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.

Il `reduced_redundancy` L'intestazione viene utilizzata al meglio quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso, utilizzando `reduced_redundancy` elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni operazione di acquisizione.

Utilizzando il `reduced_redundancy` l'intestazione non è consigliata in altre circostanze perché aumenta il rischio di perdita dei dati dell'oggetto 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.

Si noti che specificando `reduced_redundancy` influisce solo sul numero di copie create quando un oggetto viene acquisito per la prima volta. Non influisce sul numero di copie dell'oggetto eseguite quando l'oggetto viene valutato dal criterio ILM attivo e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

Un'esecuzione corretta restituisce le seguenti intestazioni con una risposta "HTTP/1.1 201 created":

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Trans-Id`

#### Informazioni correlate

["Gestire gli oggetti con ILM"](#)

["Operazioni rapide monitorate nei registri di audit"](#)

### Richiesta DI OPZIONI

La richiesta DI OPZIONI verifica la disponibilità di un singolo servizio Swift. La richiesta DI OPZIONI viene elaborata dal nodo di storage o dal nodo gateway specificato nell'URL.

#### Metodo DI OPZIONI

Ad esempio, le applicazioni client possono inviare una richiesta DI OPZIONI alla porta Swift su un nodo di storage, senza fornire credenziali di autenticazione Swift, per determinare se il nodo di storage 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.

Se utilizzato con l'URL info o l'URL di storage, il metodo OPTIONS restituisce un elenco di verbi supportati per l'URL specificato (ad esempio, HEAD, GET, OPZIONI e PUT). Il metodo DELLE OPZIONI non può essere utilizzato con l'URL auth.

È necessario il seguente parametro di richiesta:

- `Account`

I seguenti parametri di richiesta sono facoltativi:

- `Container`
- `Object`

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta “HTTP/1.1 204 No Content”. Le OPZIONI richieste all'URL di storage non richiedono l'esistenza della destinazione.

- Allow (Un elenco di verbi supportati per l'URL specificato, ad esempio, HEAD, GET, OPZIONI, E PUT)
- Content-Length
- Content-Type
- Date
- X-Trans-Id

#### Informazioni correlate

["Endpoint API Swift supportati"](#)

#### Risposte agli errori alle operazioni API di Swift

Comprendere le possibili risposte agli errori può aiutare a risolvere i problemi delle operazioni.

I seguenti codici di stato HTTP potrebbero essere restituiti quando si verificano errori durante un'operazione:

Nome errore Swift	Stato HTTP
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadataValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadataTooLarge	400 richiesta errata
Accesso negato	403 proibita
ContainerNotEmpty, ContainerAlreadyExists	409 conflitto
InternalError	500 errore interno del server
InvalidRange	416 intervallo richiesto non riscontrabile
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
Non trovato	404 non trovato
Non soddisfatto	501 non implementato
PrecondizioneFailed	412 precondizione non riuscita

Nome errore Swift	Stato HTTP
ResourceNotFound	404 non trovato
Non autorizzato	401 non autorizzato
UnprocessableEntity	422 entità non elaborabile

## Operazioni API Swift REST di StorageGRID

Sono state aggiunte operazioni all'API di Swift REST specifiche per il sistema StorageGRID.

### OTTENERE una richiesta di coerenza dei container

Il livello di coerenza crea un compromesso tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage. La richiesta DI coerenza GET Container consente di determinare il livello di coerenza applicato a un determinato container.

#### Richiesta

Richiedi intestazione HTTP	Descrizione
X-Auth-Token	Specifica il token di autenticazione Swift per l'account da utilizzare per la richiesta.
x-ntap-sg-consistency	Specifica il tipo di richiesta, dove <code>true</code> = OTTENERE la coerenza del container, e. <code>false</code> = GET container (OTTIENI container).
Host	Il nome host a cui viene indirizzata la richiesta.

#### Esempio di richiesta

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

#### Risposta

Intestazione HTTP di risposta	Descrizione
Date	La data e l'ora della risposta.
Connection	Se la connessione al server è aperta o chiusa.

Intestazione HTTP di risposta	Descrizione
X-Trans-Id	Identificativo univoco della transazione per la richiesta.
Content-Length	La lunghezza del corpo di risposta.
x-ntap-sg-consistency	<p>Il livello di controllo della coerenza applicato al container. Sono supportati i seguenti valori:</p> <ul style="list-style-type: none"> <li>• <b>All</b>: Tutti i nodi ricevono i dati immediatamente o la richiesta non riesce.</li> <li>• <b>Strong-Global</b>: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.</li> <li>• <b>Strong-Site</b>: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.</li> <li>• <b>Read-after-new-write</b>: Fornisce coerenza di lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati.</li> </ul> <p><b>Nota:</b> Se l'applicazione utilizza richieste HEAD su oggetti che non esistono, potrebbe essere visualizzato un numero elevato di errori 500 interni del server se uno o più nodi di storage non sono disponibili. Per evitare questi errori, utilizzare il livello "Available".</p> <ul style="list-style-type: none"> <li>• <b>Available</b> (eventuale coerenza per le operazioni HEAD): Si comporta come il livello di coerenza "read-after-new-write", ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a "read-after-new-write" se i nodi storage non sono disponibili.</li> </ul>

### Esempio di risposta

```

HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site

```

### Informazioni correlate

## INVIO di una richiesta di coerenza del container

La richiesta DI coerenza PUT container consente di specificare il livello di coerenza da applicare alle operazioni eseguite su un container. Per impostazione predefinita, i nuovi contenitori vengono creati utilizzando il livello di coerenza “read-after-new-write”.

### Richiesta

Richiedi intestazione HTTP	Descrizione
X-Auth-Token	Il token di autenticazione Swift per l'account da utilizzare per la richiesta.
x-ntap-sg-consistency	<p>Il livello di controllo della coerenza da applicare alle operazioni sul container. Sono supportati i seguenti valori:</p> <ul style="list-style-type: none"> <li>• <b>All:</b> Tutti i nodi ricevono i dati immediatamente o la richiesta non riesce.</li> <li>• <b>Strong-Global:</b> Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.</li> <li>• <b>Strong-Site:</b> Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.</li> <li>• <b>Read-after-new-write:</b> Fornisce coerenza di lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati.</li> </ul> <p><b>Nota:</b> Se l'applicazione utilizza richieste HEAD su oggetti che non esistono, potrebbe essere visualizzato un numero elevato di errori 500 interni del server se uno o più nodi di storage non sono disponibili. Per evitare questi errori, utilizzare il livello “Available”.</p> <ul style="list-style-type: none"> <li>• <b>Available</b> (eventuale coerenza per le operazioni HEAD): Si comporta come il livello di coerenza “read-after-new-write”, ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a “read-after-new-write” se i nodi storage non sono disponibili.</li> </ul>
Host	Il nome host a cui viene indirizzata la richiesta.

## Come interagiscono i controlli di coerenza e le regole ILM per influire sulla protezione dei dati

La scelta del controllo di coerenza e la regola ILM influiscono sulla modalità di protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, il controllo di coerenza utilizzato quando un oggetto viene memorizzato influisce sul posizionamento iniziale dei metadati dell'oggetto, mentre il comportamento di acquisizione selezionato per la regola ILM influisce sul posizionamento iniziale delle copie dell'oggetto. Poiché StorageGRID richiede l'accesso sia ai metadati di un oggetto che ai suoi dati per soddisfare le richieste dei client, la selezione dei livelli di protezione corrispondenti per il livello di coerenza e il comportamento di acquisizione può fornire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Strict:** Tutte le copie specificate nella regola ILM devono essere eseguite prima che il client sia riuscito.
- **Balanced:** StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono eseguite copie temporanee e viene restituito il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.
- **Doppio commit:** StorageGRID esegue immediatamente copie temporanee dell'oggetto e restituisce il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.



Prima di selezionare il comportamento di acquisizione per una regola ILM, leggere la descrizione completa di queste impostazioni nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

### Esempio di come il controllo di coerenza e la regola ILM possono interagire

Si supponga di disporre di una griglia a due siti con la seguente regola ILM e la seguente impostazione del livello di coerenza:

- **ILM rule:** Creare due copie di oggetti, una nel sito locale e una in un sito remoto. Viene selezionato il comportamento rigoroso dell'acquisizione.
- **Livello di coerenza:** “strong-Global” (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie degli oggetti e distribuisce i metadati a entrambi i siti prima di restituire il risultato al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione del messaggio di successo. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, le copie dei dati dell'oggetto e dei metadati dell'oggetto rimangono nel sito remoto. L'oggetto è completamente recuperabile.

Se invece sono state utilizzate la stessa regola ILM e il livello di coerenza “strong-site”, il client potrebbe ricevere un messaggio di successo dopo la replica dei dati dell'oggetto nel sito remoto, ma prima della distribuzione dei metadati dell'oggetto. 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 poco dopo l'acquisizione, i metadati dell'oggetto andranno persi. Impossibile recuperare l'oggetto.

L'interconnessione tra i livelli di coerenza e le regole ILM può essere complessa. Contattare NetApp per assistenza.

## Esempio di richiesta

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

## Risposta

Intestazione HTTP di risposta	Descrizione
Date	La data e l'ora della risposta.
Connection	Se la connessione al server è aperta o chiusa.
X-Trans-Id	Identificativo univoco della transazione per la richiesta.
Content-Length	La lunghezza del corpo di risposta.

## Esempio di risposta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

## Informazioni correlate

["Utilizzare un account tenant"](#)

## Configurazione della sicurezza per l'API REST

È necessario esaminare le misure di sicurezza implementate per L'API REST e comprendere come proteggere il sistema.

### In che modo StorageGRID fornisce la sicurezza per l'API REST

È necessario comprendere in che modo il sistema StorageGRID implementa la sicurezza, l'autenticazione e l'autorizzazione per l'API REST.

StorageGRID utilizza le seguenti misure di sicurezza.

- Le comunicazioni del client con il servizio Load Balancer utilizzano HTTPS se HTTPS è configurato per l'endpoint del bilanciamento del carico.

Quando si configura un endpoint di bilanciamento del carico, è possibile attivare HTTP. Ad esempio, è

possibile utilizzare HTTP per test o altri scopi non di produzione. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

- Per impostazione predefinita, StorageGRID utilizza HTTPS per le comunicazioni client con i nodi di storage e il servizio CLB sui nodi gateway.

È possibile abilitare HTTP per queste connessioni. Ad esempio, è possibile utilizzare HTTP per test o altri scopi non di produzione. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.



Il servizio CLB è obsoleto.

- Le comunicazioni tra StorageGRID e il client vengono crittografate mediante TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di storage all'interno della griglia vengono crittografate indipendentemente dal fatto che l'endpoint del bilanciamento del carico sia configurato per accettare connessioni HTTP o HTTPS.
- I client devono fornire le intestazioni di autenticazione HTTP a StorageGRID per eseguire operazioni REST API.

#### Certificati di sicurezza e applicazioni client

I client possono connettersi al servizio Load Balancer sui nodi Gateway o sui nodi Admin, direttamente ai nodi Storage o al servizio CLB sui nodi Gateway.

In tutti i casi, le applicazioni client possono stabilire connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dal sistema StorageGRID:

- Quando le applicazioni client si connettono al servizio Load Balancer, utilizzano il certificato configurato per l'endpoint specifico del bilanciamento del carico utilizzato per stabilire la connessione. Ogni endpoint dispone di un proprio certificato, ovvero un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dall'amministratore della griglia in StorageGRID durante la configurazione dell'endpoint.
- Quando le applicazioni client si connettono direttamente a un nodo di storage o al servizio CLB sui nodi gateway, utilizzano i certificati server generati dal sistema e generati per i nodi di storage al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema), oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia.

I client devono essere configurati in modo da considerare attendibile l'autorità di certificazione che ha firmato il certificato utilizzato per stabilire connessioni TLS.

Consultare le istruzioni per l'amministrazione di StorageGRID per informazioni sulla configurazione degli endpoint del bilanciamento del carico e per istruzioni sull'aggiunta di un singolo certificato server personalizzato per le connessioni TLS direttamente ai nodi di storage o al servizio CLB sui nodi gateway.

#### Riepilogo

La seguente tabella mostra come vengono implementati i problemi di sicurezza nelle API S3 e Swift REST:

Problema di sicurezza	Implementazione per API REST
Sicurezza della connessione	TLS

Problema di sicurezza	Implementazione per API REST
Autenticazione del server	Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore
Autenticazione del client	<ul style="list-style-type: none"> <li>S3: Account S3 (ID chiave di accesso e chiave di accesso segreta)</li> <li>Swift: Account Swift (nome utente e password)</li> </ul>
Autorizzazione del client	<ul style="list-style-type: none"> <li>S3: Proprietà del bucket e tutte le policy di controllo degli accessi applicabili</li> <li>Swift: Accesso al ruolo di amministratore</li> </ul>

#### Informazioni correlate

["Amministrare StorageGRID"](#)

#### Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un set limitato di suite di crittografia che le applicazioni client possono utilizzare quando si stabilisce una sessione TLS (Transport Layer Security).

#### Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3.



SSLv3 e TLS 1.1 (o versioni precedenti) non sono più supportati.

#### Suite di crittografia supportate

Versione TLS	IANA nome della suite di crittografia
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

#### Suite di crittografia obsolete

Le seguenti suite di crittografia sono obsolete. Il supporto per questi cifrari verrà rimosso in una release futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256

## Nome IANA

TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

### Informazioni correlate

["Come configurare le connessioni client"](#)

## Operazioni di monitoraggio e controllo

È possibile monitorare i carichi di lavoro e le efficienze per le operazioni dei client visualizzando le tendenze delle transazioni per l'intero grid o per nodi specifici. È possibile utilizzare i messaggi di audit per monitorare le operazioni e le transazioni dei client.

### Monitoraggio delle velocità di acquisizione e recupero degli oggetti

È possibile monitorare i tassi di acquisizione e recupero degli oggetti, nonché le metriche per i conteggi degli oggetti, le query e la verifica. È possibile visualizzare il numero di tentativi riusciti e non riusciti da parte delle applicazioni client di lettura, scrittura e modifica degli oggetti nel sistema StorageGRID.

#### Fasi

1. Accedere a Grid Manager utilizzando un browser supportato.
2. Nella dashboard, individuare la sezione Protocol Operations (operazioni protocollo).

In questa sezione viene riepilogato il numero di operazioni client eseguite dal sistema StorageGRID. Le velocità dei protocolli vengono calcolate in media negli ultimi due minuti.

3. Selezionare **nodi**.
4. Dalla home page dei nodi (livello di implementazione), fare clic sulla scheda **Load Balancer**.

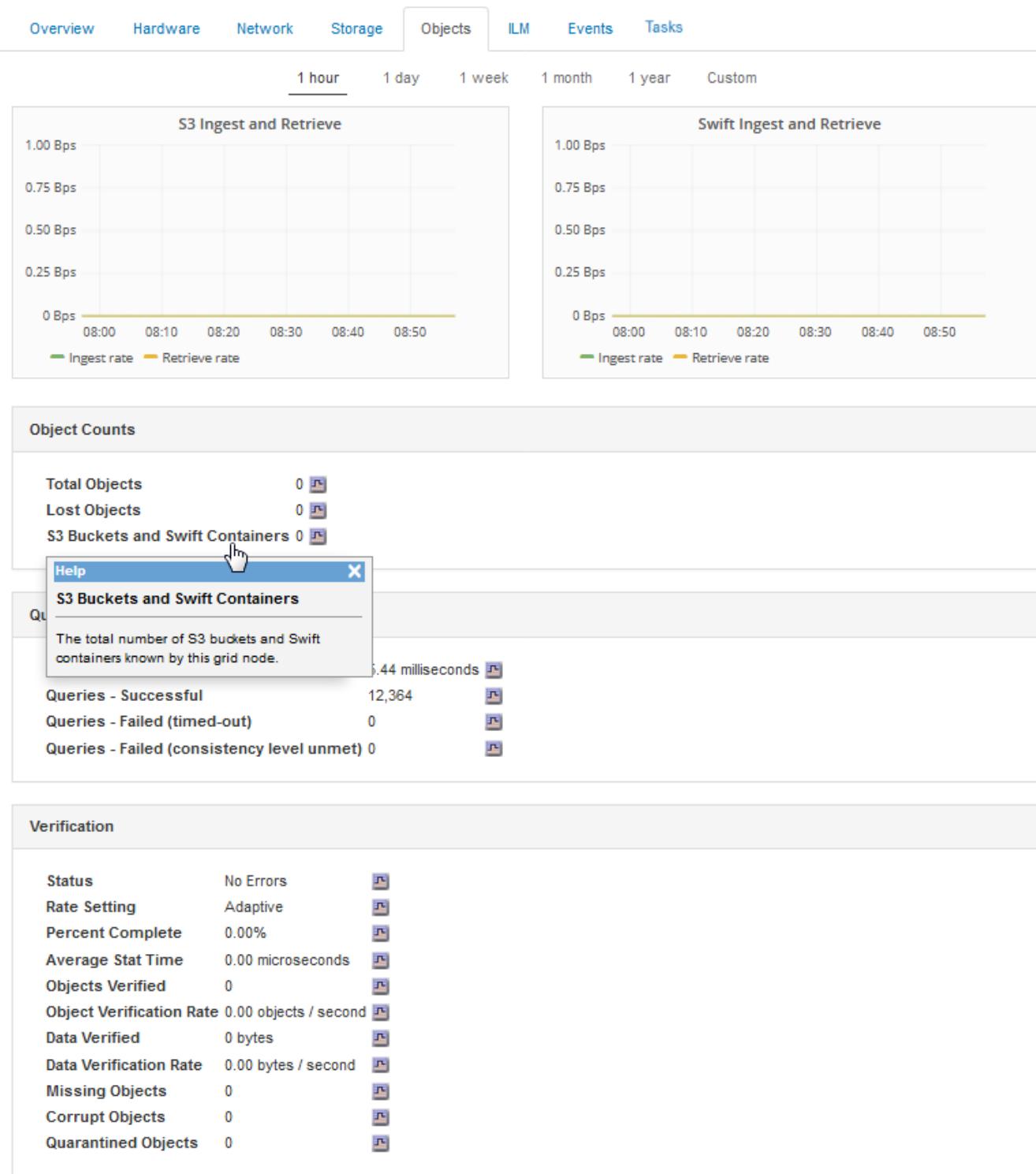
I grafici mostrano i trend di tutto il traffico client diretto agli endpoint del bilanciamento del carico all'interno della griglia. È possibile selezionare un intervallo di tempo in ore, giorni, settimane, mesi o anni, in alternativa, è possibile applicare un intervallo personalizzato.

5. Dalla home page dei nodi (livello di implementazione), fare clic sulla scheda **oggetti**.

Il grafico mostra le velocità di acquisizione e recupero dell'intero sistema StorageGRID in byte al secondo e byte totali. È possibile selezionare un intervallo di tempo in ore, giorni, settimane, mesi o anni, in alternativa, è possibile applicare un intervallo personalizzato.

6. Per visualizzare le informazioni relative a un nodo di storage specifico, selezionarlo dall'elenco a sinistra e fare clic sulla scheda **oggetti**.

Il grafico mostra le velocità di acquisizione e recupero degli oggetti per questo nodo di storage. La scheda include anche metriche per il conteggio degli oggetti, le query e la verifica. È possibile fare clic sulle etichette per visualizzare le definizioni di queste metriche.



7. Se desideri ulteriori dettagli:

- Selezionare **supporto > Strumenti > topologia griglia**.
- Selezionare **Site > Overview > Main**.

La sezione API Operations (operazioni API) visualizza informazioni riepilogative per l'intera griglia.

- Selezionare **Storage Node > LDR > client application > Overview > Main**

La sezione Operations (operazioni) visualizza informazioni riepilogative per il nodo di storage selezionato.

## Accesso e revisione dei registri di audit

I messaggi di audit vengono generati dai servizi StorageGRID e memorizzati in file di log di testo. I messaggi di audit specifici delle API nei registri di audit forniscono dati critici di sicurezza, funzionamento e monitoraggio delle performance che possono aiutare a valutare lo stato di salute del sistema.

### Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo amministratore.

### A proposito di questa attività

Il file di log di audit attivo viene denominato `audit.log` E viene memorizzato nei nodi di amministrazione.

Una volta al giorno, il file audit.log attivo viene salvato e viene avviato un nuovo file audit.log. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato `yyyy-mm-dd.txt.gz`, che conserva la data originale.

Questo esempio mostra il file audit.log attivo, il file del giorno precedente (2018-04-15.txt) e il file compresso del giorno precedente (2018-04-14.txt.gz).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

### Fasi

1. Accedere a un nodo amministratore:
  - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
  - b. Immettere la password elencata in `Passwords.txt` file.
2. Accedere alla directory contenente i file di log di controllo:`cd /var/local/audit/export`
3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

### Informazioni correlate

["Esaminare i registri di audit"](#)

### Operazioni rapide monitorate nei registri di audit

Tutte le operazioni riuscite DI ELIMINAZIONE, GET, HEAD, POST e PUT dello storage vengono monitorate nel registro di controllo di StorageGRID. Gli errori non vengono registrati, né le richieste di informazioni, auth o OPZIONI.

Per informazioni dettagliate sulle informazioni tracciate per le seguenti operazioni di Swift, consulta la sezione [informazioni sui messaggi di audit](#).

## Operazioni dell'account

- OTTIENI un account
- Conto PRINCIPALE

## Operazioni container

- ELIMINA contenitore
- OTTIENI container
- CONTENITORE DI TESTA
- METTI container

## Operazioni a oggetti

- ELIMINA oggetto
- OTTIENI oggetto
- Oggetto TESTA
- METTI oggetto

## Informazioni correlate

["Esaminare i registri di audit"](#)

["Operazioni dell'account"](#)

["Operazioni container"](#)

["Operazioni a oggetti"](#)

## Informazioni sul copyright

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

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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