Utilizzare StorageGRID

StorageGRID software

NetApp
December 03, 2025

Sommario

Utilizzare i tenant e i client StorageGRID

Utilizzare un account tenant

Utilizzare un account tenant

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

Che cos'è un conto inquilino?

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

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

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

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

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

Come creare un account tenant

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

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

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

Configurare i tenant S3

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

- Impostare la federazione delle identità (a meno che l'origine dell'identità non sia condivisa con la griglia)
- Gestisci gruppi e utenti
- Utilizzare la federazione di griglia per la clonazione degli account e la replica tra griglie
- Gestisci le chiavi di accesso S3
- Crea e gestisci bucket S3
- Utilizzare i servizi della piattaforma S3
- Utilizzare S3 Select
- Monitorare l'utilizzo dello spazio di archiviazione

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

Come accedere e uscire

Sign in a Tenant Manager

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

Prima di iniziare

- Hai le tue credenziali di accesso.
- Hai un URL per accedere a Tenant Manager, fornito dall'amministratore della tua griglia. L'URL sarà simile a uno di questi esempi:

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

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

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

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

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

Passi

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

4. Sign in a Tenant Manager.

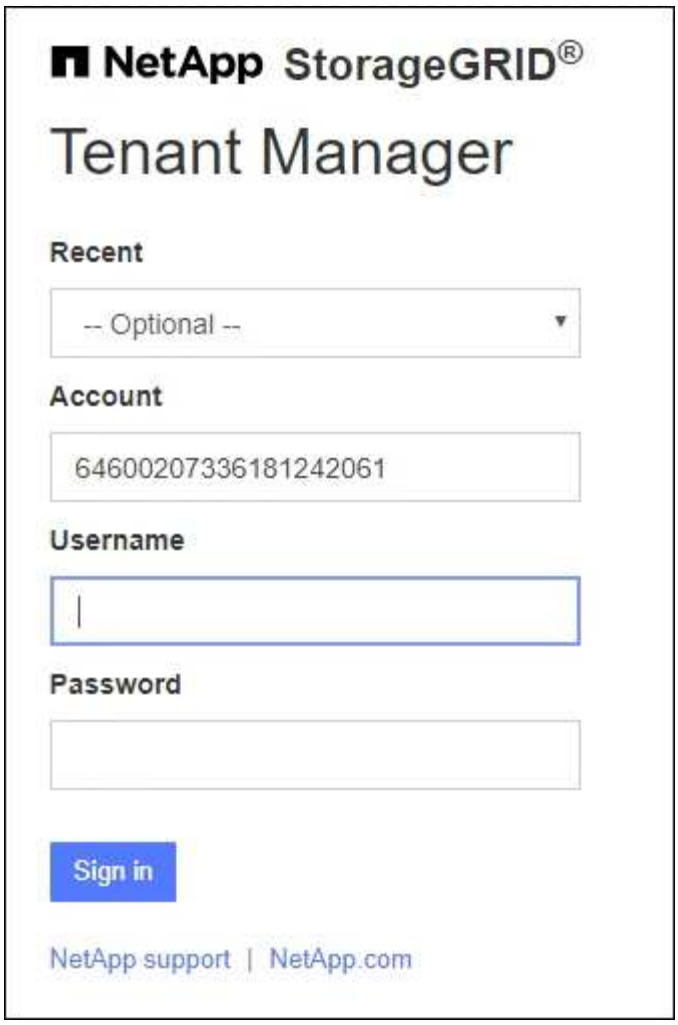
   La schermata di accesso visualizzata dipende dall'URL immesso e dal fatto che sia stato configurato l'accesso singolo (SSO) per StorageGRID.

Non si utilizza SSO

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

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

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



i. Se l'ID account di 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account del tenant se appare nell'elenco degli account recenti oppure immettere l'ID account.

ii. Inserisci il tuo nome utente e la tua password.

iii. Seleziona * Sign in*.

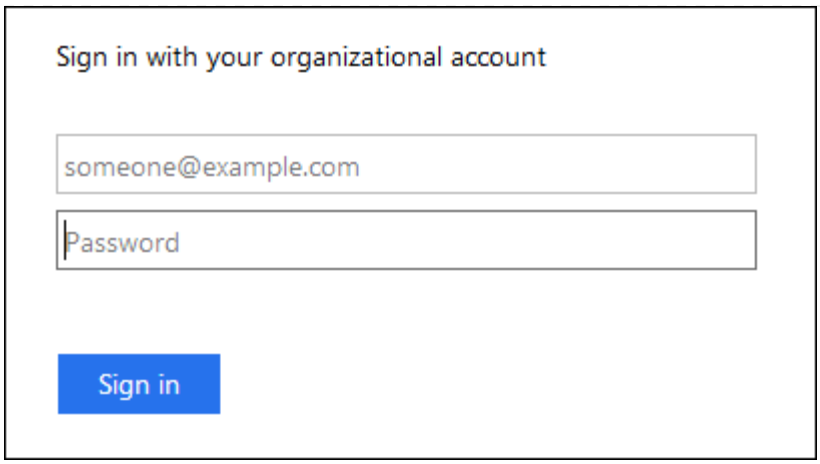
Viene visualizzata la dashboard del Tenant Manager.

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

Utilizzo di SSO

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

◦ La pagina SSO della tua organizzazione. Per esempio:



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

- Pagina di accesso SSO del Tenant Manager.

i. Se l'ID account di 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account del tenant se appare nell'elenco degli account recenti oppure immettere l'ID account.

ii. Seleziona * Sign in*.

iii. Sign in con le tue credenziali SSO standard alla pagina di accesso SSO della tua organizzazione.

Viene visualizzata la dashboard del Tenant Manager.

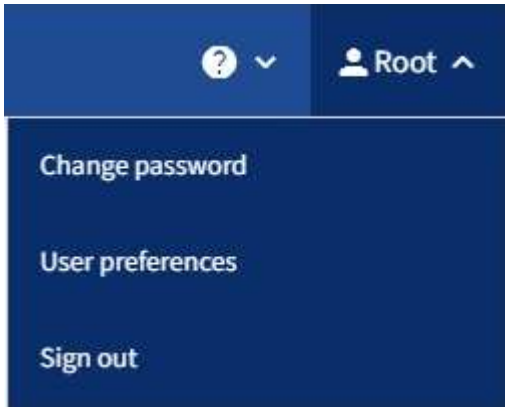
Esci da Tenant Manager

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

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

Passi

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



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

   - Se SSO non è in uso:

     Hai effettuato la disconnessione dal nodo di amministrazione. Viene visualizzata la pagina di accesso del Tenant Manager.

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

   - Se SSO è abilitato:

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

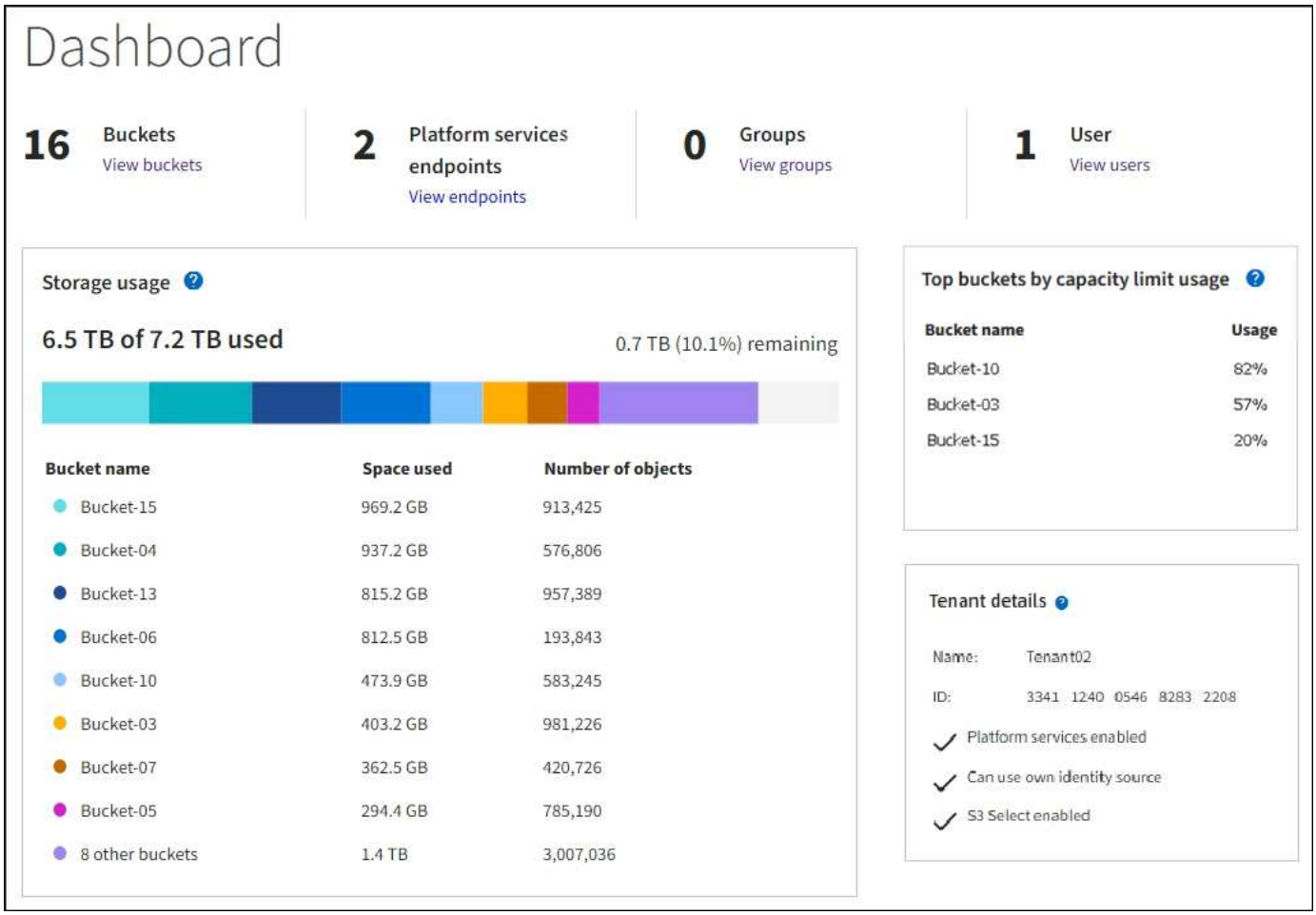
     > Se l'SSO è abilitato e hai effettuato l'accesso anche a Grid Manager, devi anche disconnetterti da Grid Manager per uscire dall'SSO.

Comprendere la dashboard di Tenant Manager

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

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

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



Informazioni sull'account dell'inquilino

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

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

Utilizzo di spazio di archiviazione e quote

Il pannello Utilizzo dello spazio di archiviazione contiene le seguenti informazioni:

- La quantità di dati oggetto per il tenant.

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

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

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

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

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

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

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

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

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

Avvisi sull'utilizzo delle quote

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

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

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

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

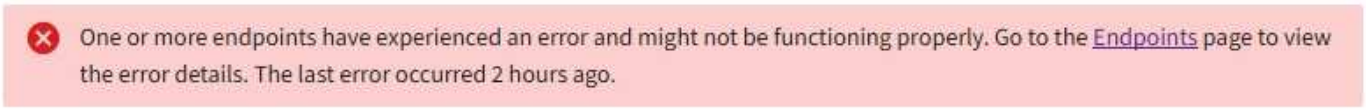
Limite di utilizzo della capacità

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

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

Errori di endpoint

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



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

API di gestione degli inquilini

Comprendere l'API di gestione degli inquilini

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

API di gestione degli inquilini:

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

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

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

operazioni API

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

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

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

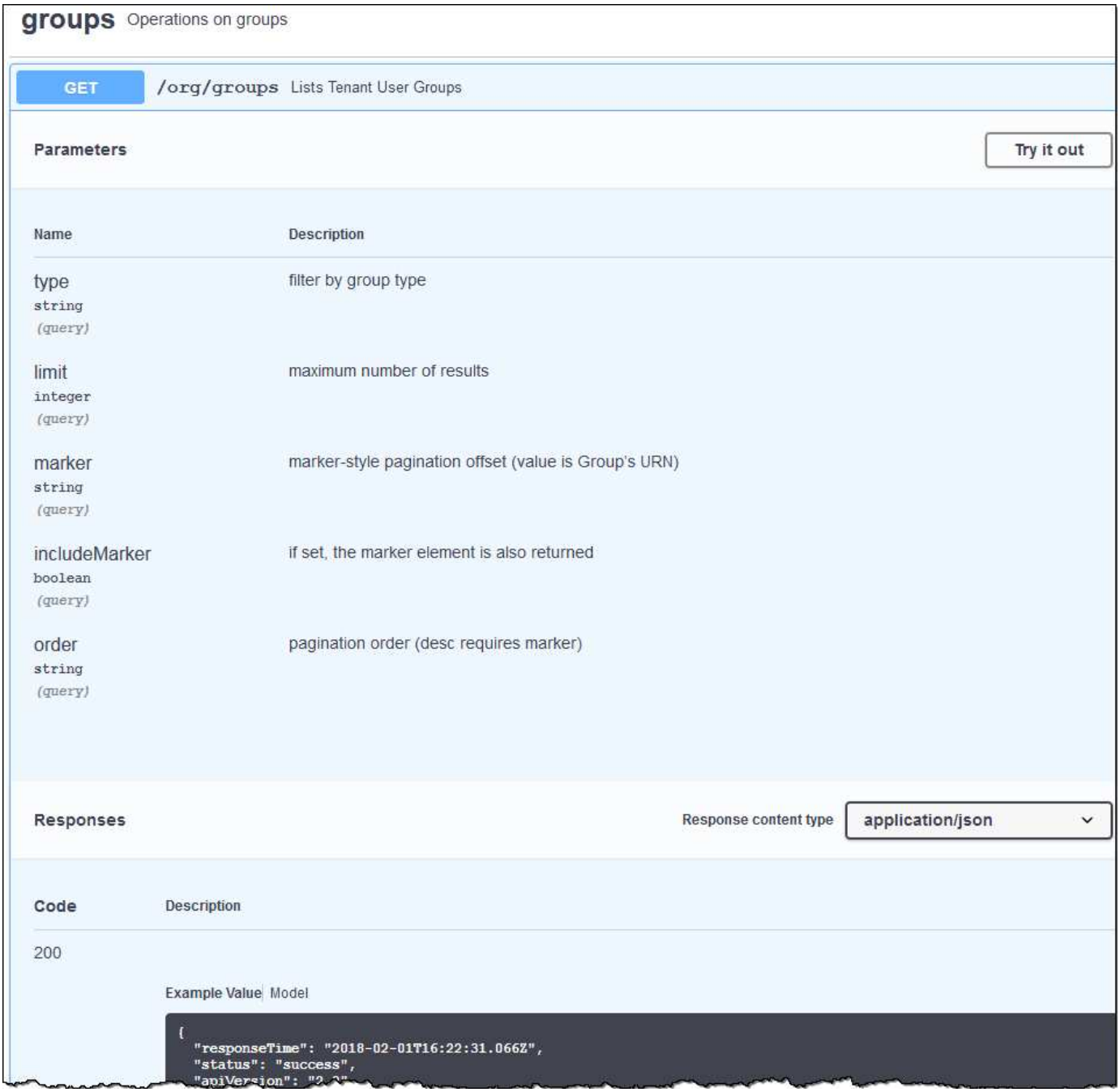
  Per informazioni su come migliorare la sicurezza dell'autenticazione, vedere"Protezione contro la falsificazione delle richieste tra siti" .

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

- **config**: Operazioni relative alla versione del prodotto e alle versioni dell'API di gestione tenant. È possibile elencare la versione del prodotto e le principali versioni dell'API supportate da tale versione.
- **contenitori**: operazioni su bucket S3 o contenitori Swift.
- **deactivated-features**: Operazioni per visualizzare le funzionalità che potrebbero essere state disattivate.
- **endpoint**: Operazioni per gestire un endpoint. Gli endpoint consentono a un bucket S3 di utilizzare un servizio esterno per la replica, le notifiche o l'integrazione della ricerca StorageGRID CloudMirror.
- **grid-federation-connections**: Operazioni sulle connessioni della federazione di griglia e sulla replicazione tra griglie.
- **gruppi**: operazioni per gestire gruppi di tenant locali e per recuperare gruppi di tenant federati da una fonte di identità esterna.
- **identity-source**: Operazioni per configurare una fonte di identità esterna e per sincronizzare manualmente le informazioni sui gruppi federati e sugli utenti.
- **ilm**: Operazioni sulle impostazioni di gestione del ciclo di vita delle informazioni (ILM).
- **regioni**: operazioni per determinare quali regioni sono state configurate per il sistema StorageGRID .
- **s3**: Operazioni per gestire le chiavi di accesso S3 per gli utenti tenant.
- **s3-object-lock**: Operazioni sulle impostazioni globali di S3 Object Lock, utilizzate per supportare la conformità normativa.
- **utenti**: operazioni per visualizzare e gestire gli utenti tenant.

Dettagli dell'operazione

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



Inviare richieste API

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

Passi

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

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

Versionamento dell'API di gestione degli inquilini

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

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

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

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

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

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

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

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

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

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

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

Determina quali versioni API sono supportate nella versione corrente

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

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

Specificare una versione API per una richiesta

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

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

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

Protezione contro la falsificazione delle richieste tra siti (CSRF)

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

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

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

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

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

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

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

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

Per configurare la protezione CSRF, utilizzare"API di gestione della griglia" O"API di gestione degli inquilini" .

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

Utilizzare connessioni di federazione di rete

Clona gruppi tenant e utenti

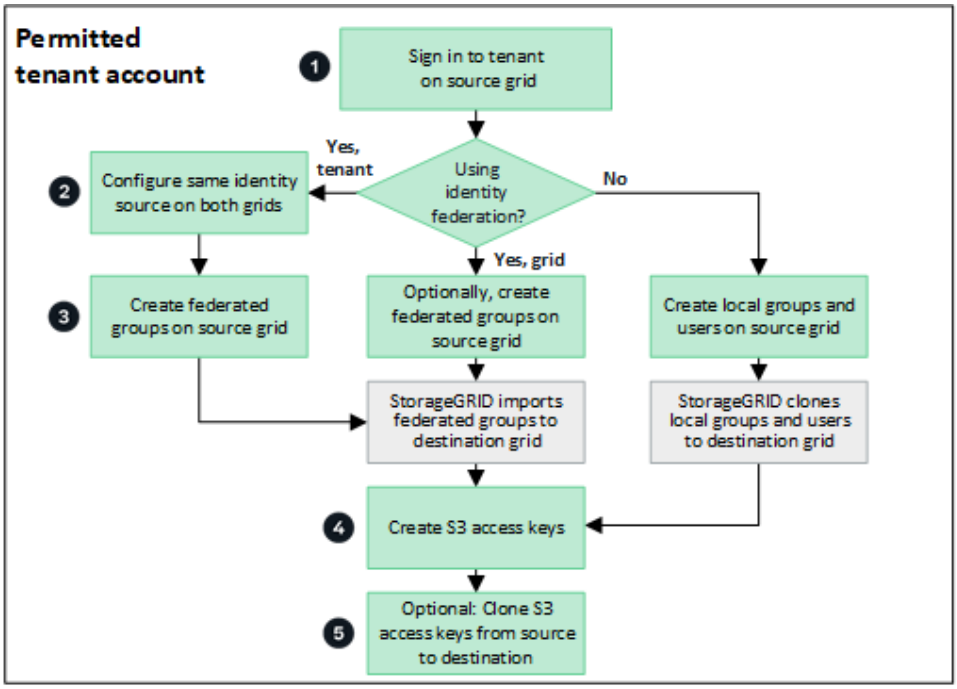
Se un tenant è stato creato o modificato per utilizzare una connessione di federazione della griglia, tale tenant viene replicato da un sistema StorageGRID (il tenant di origine) a un altro sistema StorageGRID (il tenant di replica). Dopo che il tenant è stato replicato, tutti i gruppi e gli utenti aggiunti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

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

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

Flusso di lavoro del tenant per la clonazione dell'account

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



Questi sono i passaggi principali del flusso di lavoro:

1 Sign in al tenant

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

2 Facoltativamente, configurare la federazione delle identità

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

3 Crea gruppi e utenti

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

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

4 Crea chiavi di accesso S3

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

5 Facoltativamente, clona le chiavi di accesso S3

Se devi accedere ai bucket con le stesse chiavi di accesso su entrambe le griglie, crea le chiavi di accesso sulla griglia di origine e poi usa l'API Tenant Manager per clonarle manualmente sulla griglia di destinazione. Per le istruzioni, vedere"Clona le chiavi di accesso S3 utilizzando l'API" .

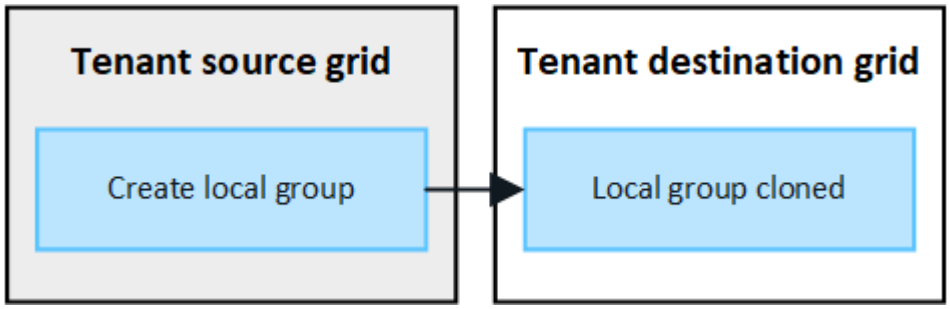
Come vengono clonati gruppi, utenti e chiavi di accesso S3?

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

I gruppi locali creati sulla griglia di origine vengono clonati

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

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

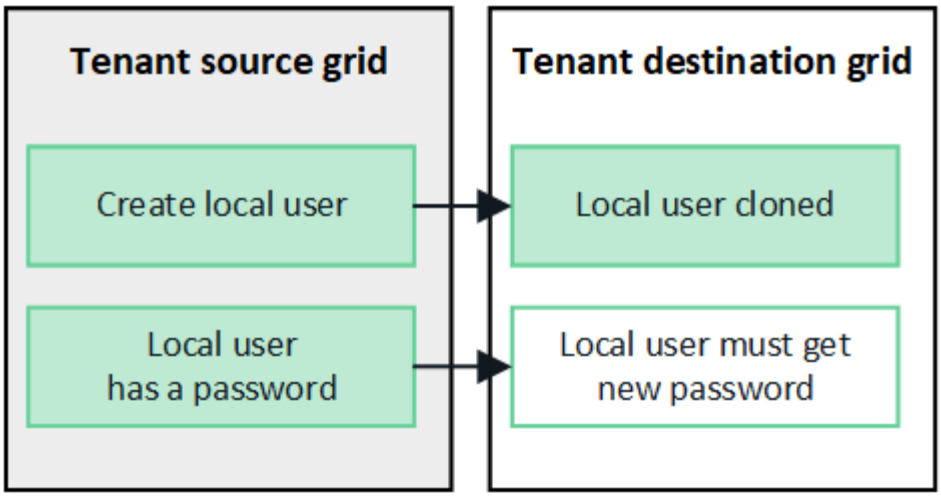


> Tutti gli utenti selezionati quando si crea un gruppo locale nella griglia di origine non vengono inclusi quando il gruppo viene clonato nella griglia di destinazione. Per questo motivo, non selezionare gli utenti quando crei il gruppo. In alternativa, seleziona il gruppo quando crei gli utenti.

Gli utenti locali creati sulla griglia di origine vengono clonati

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

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

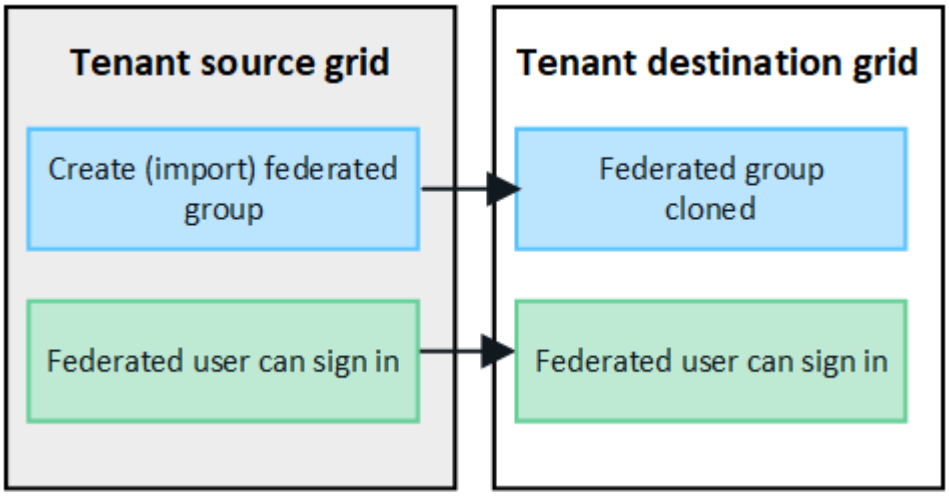


I gruppi federati creati sulla griglia di origine vengono clonati

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

Entrambi i gruppi hanno la stessa modalità di accesso, le stesse autorizzazioni di gruppo e la stessa policy di gruppo S3.

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

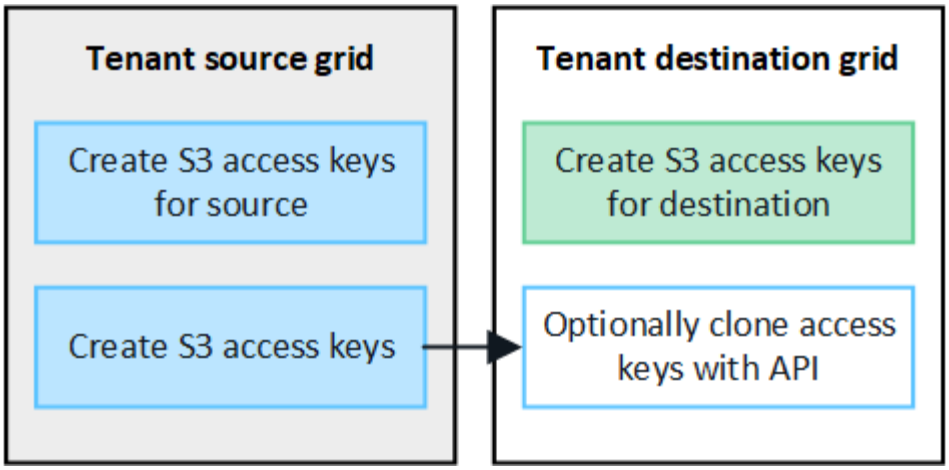


Le chiavi di accesso S3 possono essere clonate manualmente

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

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

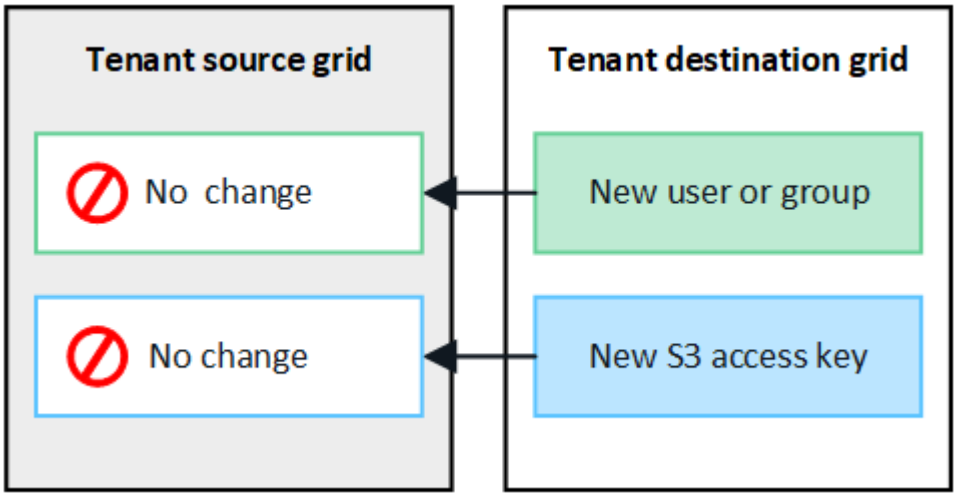
- Se non hai bisogno di usare le stesse chiavi per ogni griglia, puoi"crea le tue chiavi di accesso" O"creare le chiavi di accesso di un altro utente" su ogni griglia.
- Se devi utilizzare le stesse chiavi su entrambe le griglie, puoi creare chiavi sulla griglia di origine e quindi utilizzare l'API Tenant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



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

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

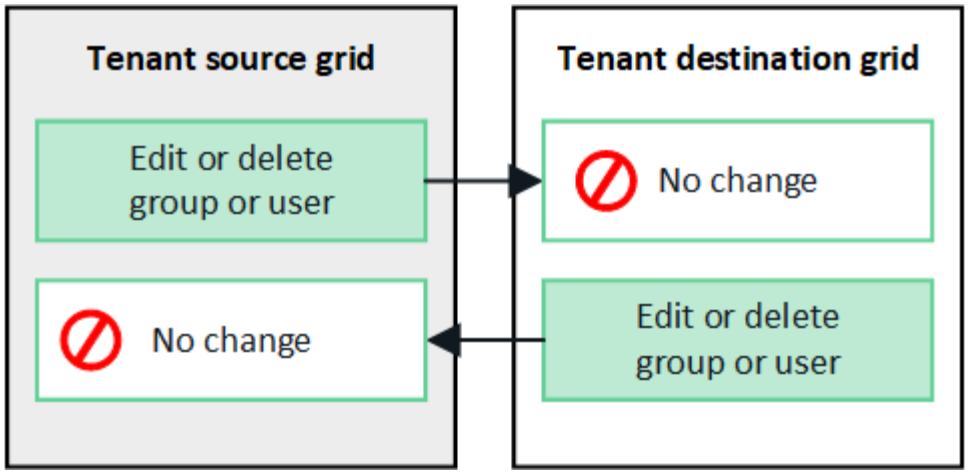
La clonazione avviene solo dalla griglia di origine del tenant alla griglia di destinazione del tenant. Se si creano o si importano gruppi e utenti nella griglia di destinazione del tenant, StorageGRID non clonerà questi elementi nella griglia di origine del tenant.



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

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

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



Clona le chiavi di accesso S3 utilizzando l'API

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

Prima di iniziare

- L'account tenant ha l'autorizzazione **Usa connessione federata alla griglia**.
- La connessione della federazione di rete ha uno **Stato di connessione** pari a **Connesso**.
- Hai effettuato l'accesso al Tenant Manager sulla griglia di origine del tenant utilizzando un"browser web supportato" .
- Appartieni a un gruppo di utenti che ha il"Gestisci le tue credenziali S3 o l'autorizzazione di accesso Root" .
- Se si clonano le chiavi di accesso per un utente locale, l'utente esiste già su entrambe le griglie.

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

Clona le tue chiavi di accesso

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

Passi

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

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

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

Assicuratevi di mantenere le virgolette doppie attorno a ciascuna stringa.

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

Clona le chiavi di accesso di un altro utente

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

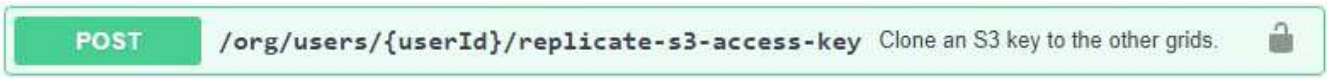
Passi

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

      ```
      GET /org/users
      ```

   b. Seleziona **Provalo**.
   c. Specificare i parametri che si desidera utilizzare durante la ricerca degli utenti.
   d. Selezionare **Esegui**.
   e. Trova l'utente di cui vuoi clonare le chiavi e copia il numero nel campo **id**.
4. Nella sezione **s3**, seleziona il seguente endpoint:

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

5. Seleziona **Provalo**.
6. Nella casella di testo **userId**, incolla l'ID utente che hai copiato.
7. Nella casella di testo **corpo**, sostituire le voci di esempio per **chiave di accesso di esempio** e **chiave di accesso segreta** con i valori del file **.csv** per quell'utente.

Assicuratevi di mantenere le virgolette doppie attorno alla stringa.

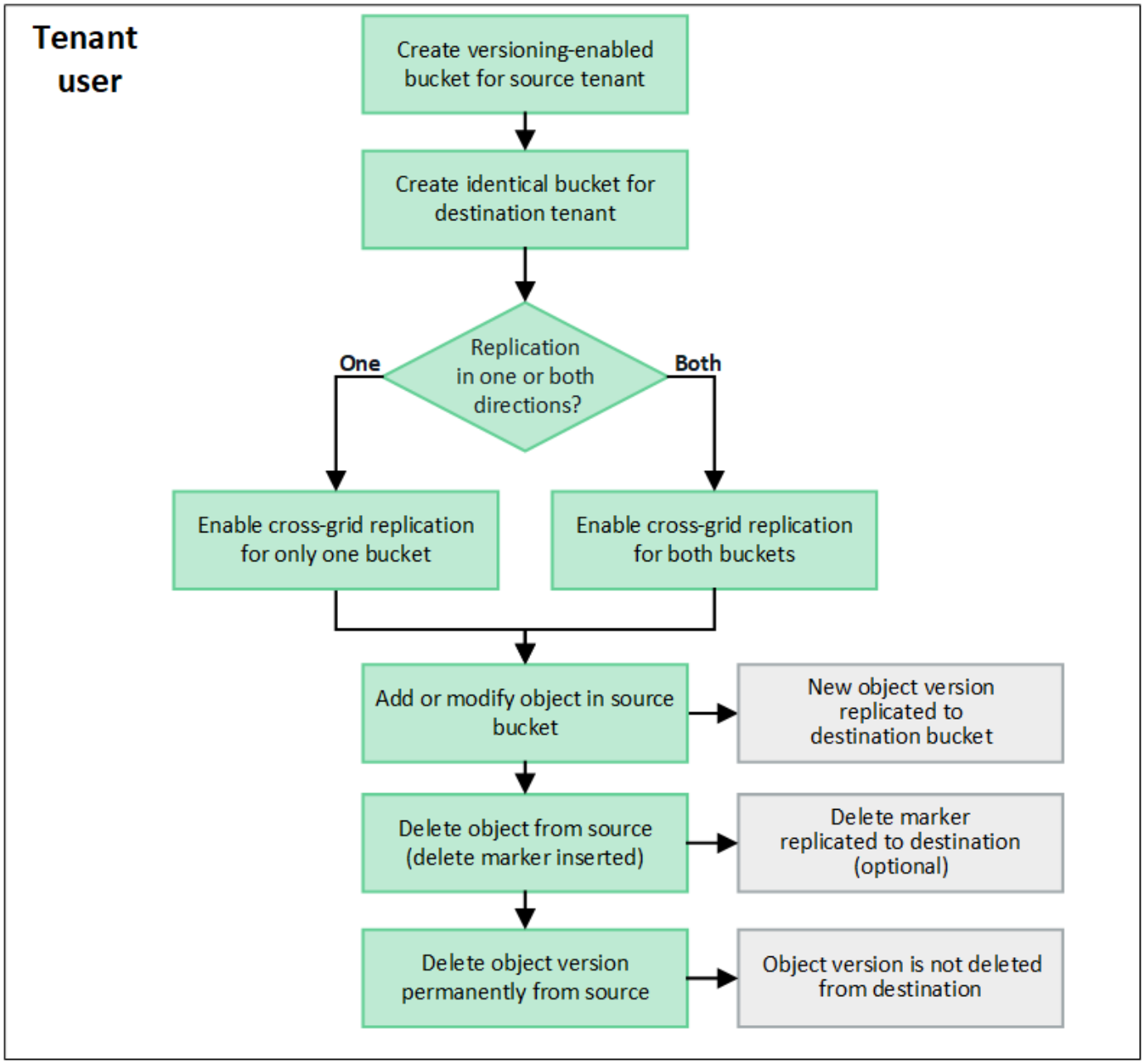
8. Se la chiave scadrà, sostituire la voce di esempio per **expires** con la data e l'ora di scadenza come stringa nel formato data-ora ISO 8601 (ad esempio, `2023-02-28T22:46:33-08:00`). Se la chiave non scade, immettere **null** come valore per la voce **expires** (oppure rimuovere la riga **Expires**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

Gestire la replicazione tra griglie

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

Flusso di lavoro per la replicazione tra griglie

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



Configurare la replicazione tra griglie

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

Prima di iniziare

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

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

Crea due bucket identici

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

Passi

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

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

   b. Seguire le istruzioni per"creare un bucket S3" .
   c. Nella scheda **Gestisci impostazioni oggetto**, seleziona **Abilita controllo delle versioni degli oggetti**.
   d. Se S3 Object Lock è abilitato per il sistema StorageGRID , non abilitare S3 Object Lock per il bucket.
   e. Seleziona **Crea bucket**.
   f. Selezionare **Fine**.
2. Ripetere questi passaggi per creare un bucket identico per lo stesso account tenant sull'altra griglia nella connessione di federazione della griglia.

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

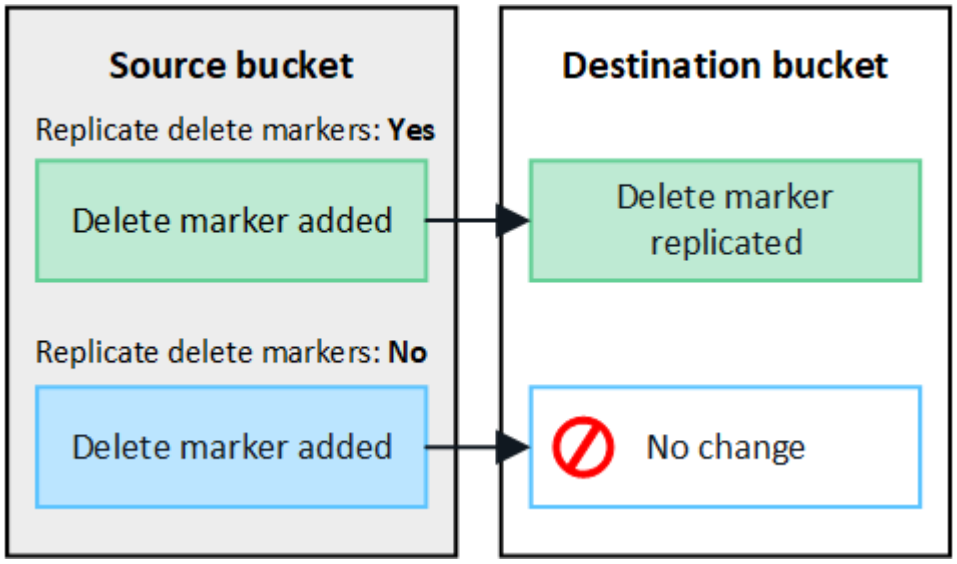
Abilita la replicazione tra griglie

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

Passi

1. Partendo da una griglia di cui vuoi replicare gli oggetti, abilita"replicazione cross-grid in una direzione" :
   a. Sign in all'account tenant per il bucket.
   b. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3)** > **Bucket**.
   c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
   d. Selezionare la scheda **Replica tra griglie**.
   e. Selezionare **Abilita** e rivedere l'elenco dei requisiti.
   f. Se tutti i requisiti sono stati soddisfatti, selezionare la connessione di federazione di rete che si desidera utilizzare.
   g. Facoltativamente, modifica l'impostazione di **Replica marcatori di eliminazione** per determinare cosa accade sulla griglia di destinazione se un client S3 invia una richiesta di eliminazione alla griglia di origine che non include un ID versione:
      - **Sì** (predefinito): un marcatore di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione.

- **No**: un marcatore di eliminazione viene aggiunto al bucket di origine ma non viene replicato nel bucket di destinazione.



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

Vedere"Che cosa è la replicazione cross-grid" per i dettagli.

a. Facoltativamente, modificare l'impostazione della categoria di controllo **Replica tra griglie** per gestire il volume dei messaggi di controllo:
   - **Errore** (predefinito): nell'output di controllo vengono incluse solo le richieste di replica tra griglie non riuscite.
   - **Normale**: vengono incluse tutte le richieste di replica tra griglie, il che aumenta significativamente il volume dell'output di audit.

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

c. Seleziona **Abilita e prova**.

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

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

Test di replicazione tra griglie

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

Prima di iniziare

- Stai utilizzando un"browser web supportato" .

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

Passi

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

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

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

Disabilita la replicazione tra griglie

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

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

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

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

Prima di iniziare

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

Passi

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

d. Selezionare la scheda **Replica tra griglie**.

e. Selezionare **Disabilita replicazione**.

f. Se sei sicuro di voler disabilitare la replica tra griglie per questo bucket, digita **Sì** nella casella di testo e seleziona **Disabilita**.

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

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

Visualizza le connessioni della federazione di griglia

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

Prima di iniziare

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

Passi

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

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

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

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

Cancella l'ultimo errore

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

- La versione dell'oggetto sorgente non è stata trovata.
- Il bucket di origine non è stato trovato.

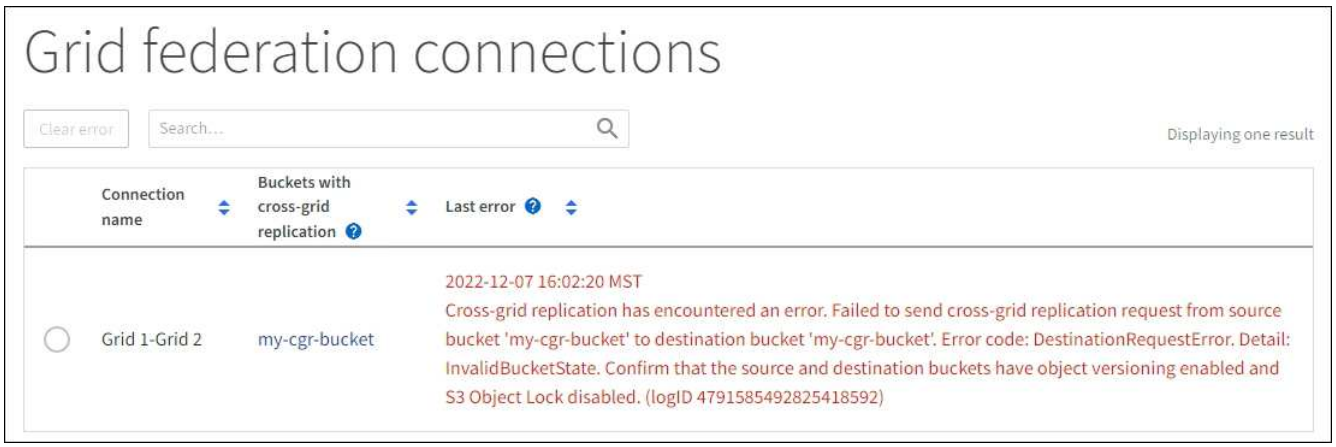
- Il bucket di destinazione è stato eliminato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il controllo delle versioni del bucket di destinazione è sospeso.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più sottoposto a controllo di versione.

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

Passi

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

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



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

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

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

Gestisci gruppi e utenti

Utilizzare la federazione delle identità

L'utilizzo della federazione delle identità velocizza la configurazione di gruppi e utenti tenant e consente agli utenti tenant di accedere all'account tenant utilizzando credenziali

familiari.

Configurare la federazione delle identità per Tenant Manager

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

Prima di iniziare

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

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

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

Informazioni su questo compito

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

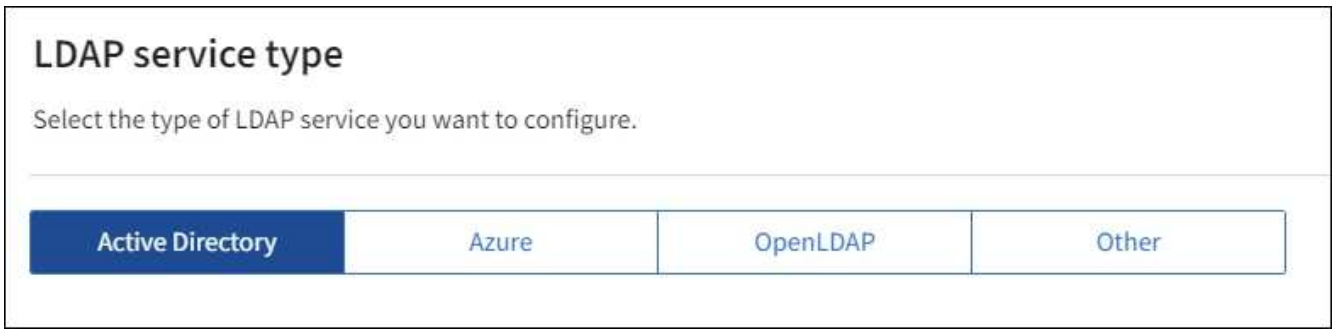
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Inserisci la configurazione

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

Passi

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



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

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. procedere al passaggio successivo.
   - **Nome univoco utente**: il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `uid` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid` .
   - **UUID utente**: il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid` . Il valore di ciascun utente per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
   - **Nome univoco del gruppo**: il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `cn` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn` .
   - **UUID gruppo**: il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid` . Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, immettere le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.
   - **Nome host**: nome di dominio completo (FQDN) o indirizzo IP del server LDAP.
   - **Porta**: la porta utilizzata per connettersi al server LDAP.

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

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

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

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

     - `sAMAccountName`O `uid`
     - `objectGUID`, `entryUUID` , O `nsuniqueid`
     - `cn`
     - `memberOf`O `isMemberOf`
     - **Directory attiva**: `objectSid` , `primaryGroupID` , `userAccountControl` , E `userPrincipalName`
     - **Azzurro**: `accountEnabled` E `userPrincipalName`
   - **Password**: la password associata al nome utente.

     Se in futuro dovessi cambiare la password, dovrai aggiornarla in questa pagina.

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

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

- **DN base utente**: percorso completo del nome distinto (DN) di un sottoalbero LDAP in cui si desidera cercare gli utenti.

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

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

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

  Inserisci uno di questi modelli:

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

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

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

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

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

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

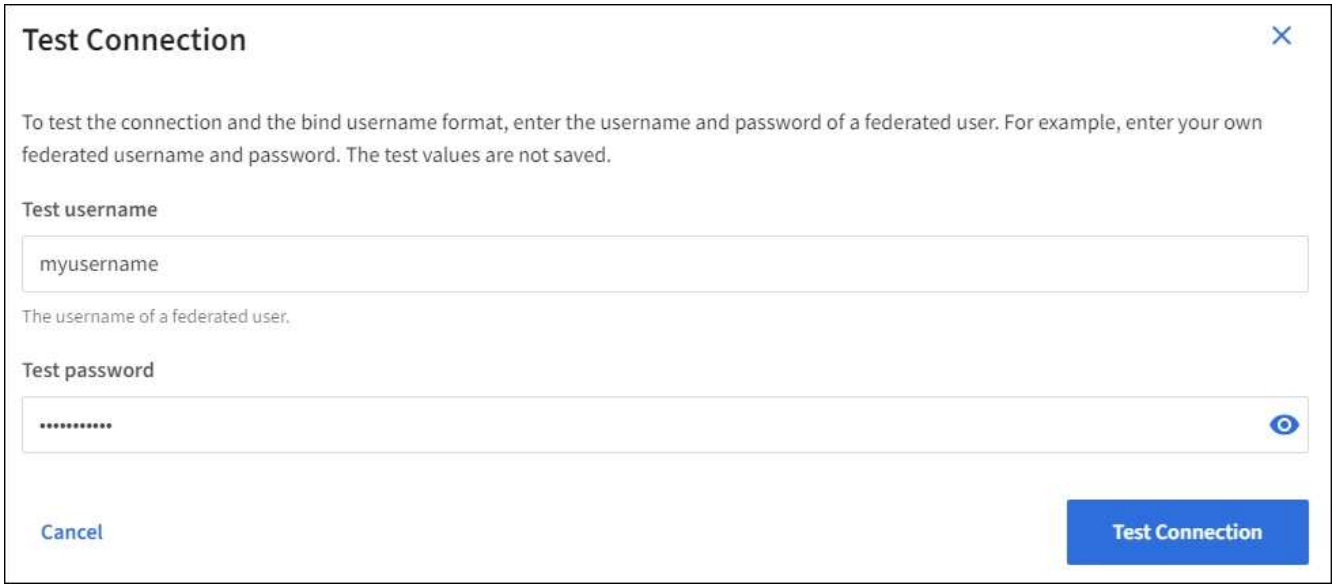
Testare la connessione e salvare la configurazione

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

Passi

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

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



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

Forza la sincronizzazione con la fonte dell'identità

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

Passi

1. Vai alla pagina Federazione delle identità.

2. Seleziona **Sincronizza server** nella parte superiore della pagina.

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

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

Disabilitare la federazione delle identità

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

Informazioni su questo compito

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

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

Passi

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

Linee guida per la configurazione del server OpenLDAP

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

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

Sovrapposizioni di membri e raffinazione

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

Indicizzazione

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

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

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

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

Gestire gruppi di tenant

Creare gruppi per un tenant S3

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

Prima di iniziare

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

Accedi alla procedura guidata Crea gruppo

Come primo passo, accedi alla procedura guidata Crea gruppo.

Passi

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

3. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

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

Passi

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

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

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

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

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

Gestisci i permessi del gruppo

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

Passi

1. Per **Modalità di accesso**, seleziona una delle seguenti opzioni:
   - **Lettura-scrittura** (predefinito): gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.

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

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

2. Seleziona una o più autorizzazioni per questo gruppo.

   Vedere "Autorizzazioni di gestione degli inquilini" .

3. Selezionare **Continua**.

Imposta i criteri di gruppo S3

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

Passi

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

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

2. Se hai selezionato **Personalizzato**, inserisci i criteri di gruppo. Ogni criterio di gruppo ha un limite di dimensione di 5.120 byte. È necessario immettere una stringa valida in formato JSON.

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

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

Aggiungi utenti (solo gruppi locali)

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

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

Passi

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

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

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

Creare gruppi per un tenant Swift

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

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

Prima di iniziare

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

Accedi alla procedura guidata Crea gruppo

Passi

Come primo passo, accedi alla procedura guidata Crea gruppo.

1. Selezionare **GESTIONE ACCESSI** > **Gruppi**.
2. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

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

Passi

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

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

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

Gestisci i permessi del gruppo

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

Passi

1. Per **Modalità di accesso**, seleziona una delle seguenti opzioni:
   - **Lettura-scrittura** (predefinito): gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
   - **Sola lettura**: gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Tenant Manager o Tenant Management API. Gli utenti locali con privilegi di sola lettura possono modificare le proprie password.

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

2. Selezionare la casella di controllo **Accesso root** se gli utenti del gruppo devono accedere a Tenant Manager o all'API Tenant Management.
3. Selezionare **Continua**.

Imposta i criteri di gruppo Swift

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

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

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

Aggiungi utenti (solo gruppi locali)

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

Passi

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

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

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

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

Autorizzazioni di gestione degli inquilini

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

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

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

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

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

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

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

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

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

Gestisci gruppi

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

Prima di iniziare

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

Visualizza o modifica il gruppo

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

Passi

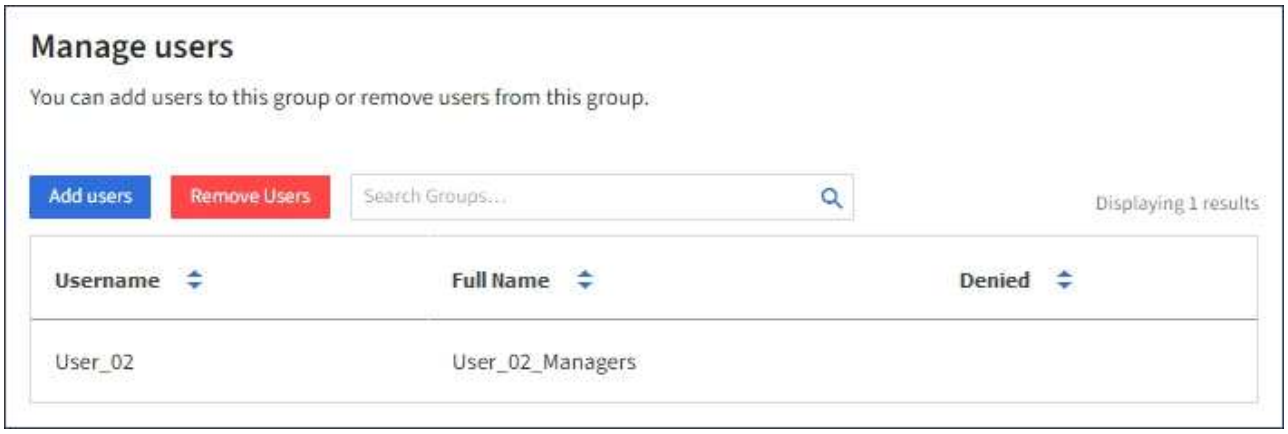
1. Selezionare **GESTIONE ACCESSI** > **Gruppi**.
2. Esaminare le informazioni fornite nella pagina Gruppi, che elenca le informazioni di base per tutti i gruppi locali e federati per questo account tenant.

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

   - Un messaggio banner indica che se modifichi o rimuovi un gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio banner indica se i gruppi non sono stati clonati nel tenant sulla griglia di destinazione. Puoiriprovare un clone di gruppo che ha fallito.
3. Se vuoi cambiare il nome del gruppo:
   a. Selezionare la casella di controllo per il gruppo.
   b. Seleziona **Azioni** > **Modifica nome gruppo**.
   c. Inserisci il nuovo nome.
   d. Seleziona **Salva modifiche.**
4. Se desideri visualizzare maggiori dettagli o apportare modifiche aggiuntive, procedi in uno dei seguenti modi:
   - Selezionare il nome del gruppo.
   - Seleziona la casella di controllo per il gruppo e seleziona **Azioni** > **Visualizza dettagli gruppo**.
5. Esaminare la sezione Panoramica, che mostra le seguenti informazioni per ciascun gruppo:
   - Nome da visualizzare
   - Nome univoco
   - Tipo

- Modalità di accesso
- Permessi
- Politica S3
- Numero di utenti in questo gruppo
- Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando il gruppo sulla griglia di origine del tenant:
  - Stato della clonazione, **Riuscito** o **Fallito**
  - Un banner blu che indica che se modifichi o elimini questo gruppo, le tue modifiche non verranno sincronizzate con l'altra griglia.

6. Modificare le impostazioni del gruppo secondo necessità. Vedere"Creare gruppi per un tenant S3" E"Creare gruppi per un tenant Swift" per i dettagli su cosa inserire.
   a. Nella sezione Panoramica, modifica il nome visualizzato selezionando il nome o l'icona di modifica .
   b. Nella scheda **Autorizzazioni gruppo**, aggiorna le autorizzazioni e seleziona **Salva modifiche**.
   c. Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.
      - Se si sta modificando un gruppo S3, è possibile selezionare facoltativamente un criterio di gruppo S3 diverso oppure immettere la stringa JSON per un criterio personalizzato, a seconda delle necessità.
      - Se stai modificando un gruppo Swift, seleziona o deseleziona facoltativamente la casella di controllo **Amministratore Swift**.
7. Per aggiungere uno o più utenti locali esistenti al gruppo:
   a. Selezionare la scheda Utenti.



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

      In alto a destra appare un messaggio di conferma.

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

      In alto a destra appare un messaggio di conferma.

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

Gruppo duplicato

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

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

Passi

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

Riprova a clonare il gruppo

Per riprovare una clonazione non riuscita:

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

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

Elimina uno o più gruppi

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

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

Passi

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

   Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Elimina gruppo** o **Elimina gruppi**.

Gestisci gli utenti locali

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

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

Prima di iniziare

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

Crea un utente locale

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

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

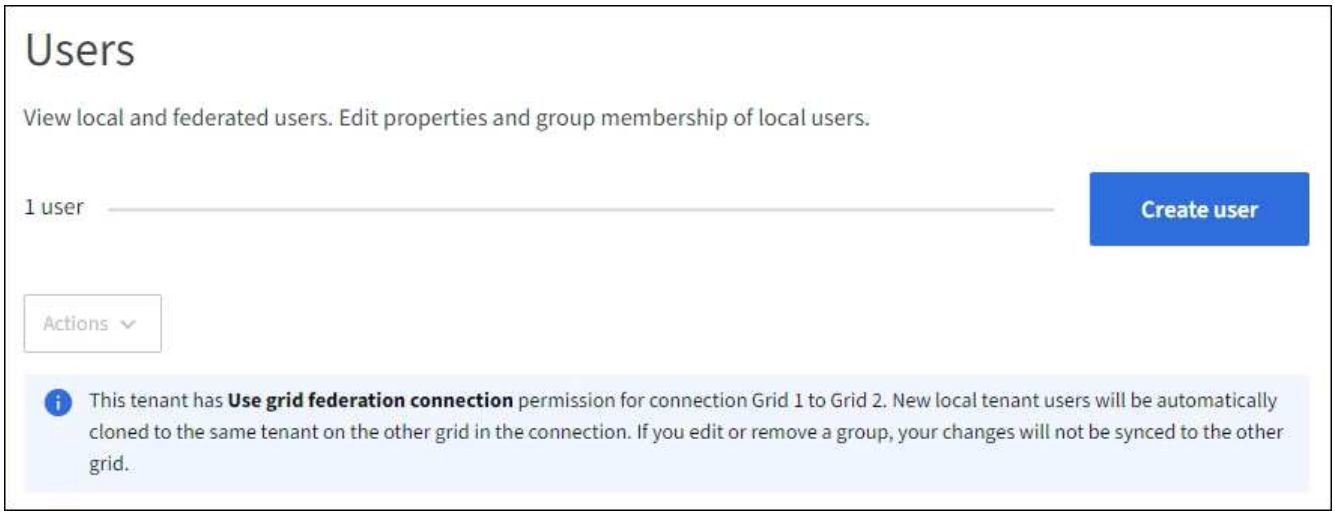
Gli utenti Swift che non appartengono ad alcun gruppo non hanno autorizzazioni di gestione né accesso al contenitore Swift.

Accedi alla procedura guidata Crea utente

Passi

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

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



2. Seleziona **Crea utente**.

Inserisci le credenziali

Passi

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

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

2. Selezionare **Continua**.

Assegna ai gruppi

Passi

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

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

modifichi i gruppi.

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

2. Seleziona **Crea utente**.

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

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

Visualizza o modifica l'utente locale

Passi

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

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

   - Un messaggio banner indica che se modifichi o rimuovi un utente, le modifiche non verranno sincronizzate con l'altra griglia.
   - Se necessario, un messaggio banner indica se gli utenti non sono stati clonati nel tenant sulla griglia di destinazione. È possibile riprova un clone utente che non è riuscito Potrebbe
3. Se vuoi cambiare il nome completo dell'utente:
   a. Selezionare la casella di controllo per l'utente.
   b. Seleziona **Azioni** > **Modifica nome completo**.
   c. Inserisci il nuovo nome.
   d. Seleziona **Salva modifiche.**
4. Se desideri visualizzare maggiori dettagli o apportare modifiche aggiuntive, procedi in uno dei seguenti modi:
   - Seleziona il nome utente.
   - Selezionare la casella di controllo per l'utente e selezionare **Azioni** > **Visualizza dettagli utente**.
5. Esaminare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:
   - Nome e cognome
   - Nome utente
   - Tipo di utente
   - Accesso negato
   - Modalità di accesso
   - Appartenenza al gruppo
   - Campi aggiuntivi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione**

griglia e si visualizza l'utente sulla griglia di origine del tenant:

- Stato della clonazione, **Riuscito** o **Fallito**
- Un banner blu che indica che se modifichi questo utente, le tue modifiche non verranno sincronizzate con l'altra griglia.

6. Modificare le impostazioni utente secondo necessità. VedereCrea utente locale per i dettagli su cosa inserire.
   a. Nella sezione Panoramica, modifica il nome completo selezionando il nome o l'icona di modifica .

      Non è possibile modificare il nome utente.

   b. Nella scheda **Password**, modifica la password dell'utente e seleziona **Salva modifiche**.
   c. Nella scheda **Accesso**, seleziona **No** per consentire all'utente di accedere oppure seleziona **Sì** per impedirgli di accedere. Quindi, seleziona **Salva modifiche**.
   d. Nella scheda **Chiavi di accesso**, seleziona **Crea chiave** e segui le istruzioni per"creazione delle chiavi di accesso S3 di un altro utente" .
   e. Nella scheda **Gruppi**, seleziona **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai gruppi. Quindi, seleziona **Salva modifiche**.
7. Conferma di aver selezionato **Salva modifiche** per ogni sezione modificata.

Utente locale duplicato

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

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

Passi

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

Riprova la clonazione dell'utente

Per riprovare una clonazione non riuscita:

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

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

Elimina uno o più utenti locali

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

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

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

Passi

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

   Viene visualizzata una finestra di dialogo di conferma.
4. Selezionare **Elimina utente** o **Elimina utenti**.

Gestisci le chiavi di accesso S3

Gestisci le chiavi di accesso S3

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

Le chiavi di accesso S3 possono essere gestite come segue:

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

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

Crea le tue chiavi di accesso S3

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

Prima di iniziare

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

Informazioni su questo compito

Puoi creare una o più chiavi di accesso S3 che ti consentono di creare e gestire i bucket per il tuo account tenant. Dopo aver creato una nuova chiave di accesso, aggiorna l'applicazione con il tuo nuovo ID chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi del necessario ed elimina quelle che non utilizzi. Se hai una sola chiave e questa sta per scadere, creane una nuova prima che scada quella vecchia, quindi eliminala.

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

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

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

Passi

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

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

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

     > La data di scadenza può essere al massimo di cinque anni dalla data corrente. L'orario di scadenza può essere di almeno un minuto rispetto all'orario corrente.

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

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

5. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   > Non chiudere questa finestra di dialogo finché non hai copiato o scaricato queste informazioni. Non è possibile copiare o scaricare le chiavi dopo aver chiuso la finestra di dialogo.

6. Selezionare **Fine**.

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

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

Visualizza le tue chiavi di accesso S3

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

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

Prima di iniziare

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

Passi

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

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

   Le chiavi scadute vengono rimosse automaticamente.

Elimina le tue chiavi di accesso S3

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

Prima di iniziare

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

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

Passi

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

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

Crea le chiavi di accesso S3 di un altro utente

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

Prima di iniziare

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

Informazioni su questo compito

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

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

- Imposta una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. Impostare un tempo di scadenza breve può aiutare a ridurre il rischio nel caso in cui l'ID della chiave di accesso e la chiave di accesso segreta vengano accidentalmente esposti. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio per la sicurezza nel tuo ambiente è basso e non hai bisogno di creare periodicamente nuove chiavi, non devi impostare una data di scadenza per le chiavi. Se in seguito decidi di creare nuove chiavi, elimina manualmente quelle vecchie.

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

Passi

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

   Viene visualizzata la pagina dei dettagli dell'utente.

3. Selezionare **Chiavi di accesso**, quindi selezionare **Crea chiave**.
4. Eseguire una delle seguenti operazioni:
   - Seleziona **Non impostare una data di scadenza** per creare una chiave che non scade. (Predefinito)
   - Seleziona **Imposta una data di scadenza** e imposta la data e l'ora di scadenza.

     La data di scadenza può essere al massimo di cinque anni dalla data corrente. L'orario di scadenza può essere di almeno un minuto rispetto all'orario corrente.

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

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

6. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

   Non chiudere questa finestra di dialogo finché non hai copiato o scaricato queste informazioni. Non è possibile copiare o scaricare le chiavi dopo aver chiuso la finestra di dialogo.

7. Selezionare **Fine**.

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

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

Visualizza le chiavi di accesso S3 di un altro utente

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

Prima di iniziare

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

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

Passi

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

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

   Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

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

Elimina le chiavi di accesso S3 di un altro utente

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

Prima di iniziare

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

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

Passi

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

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

Gestisci i bucket S3

Crea un bucket S3

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

Prima di iniziare

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

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

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

> Ogni griglia può avere un massimo di 100.000 bucket.

Accedi alla procedura guidata

Passi

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

Inserisci i dettagli

Passi

1. Inserisci i dettagli per il bucket.

Campo	Descrizione
Nome del bucket	Un nome per il bucket che rispetti queste regole: • Deve essere univoco in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). • Deve essere conforme al DNS. • Deve contenere almeno 3 e non più di 63 caratteri. • Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può contenere solo lettere minuscole, numeri e trattini. • Non devono contenere punti nelle richieste in stile ospitato virtuale. I punti causeranno problemi con la verifica dei certificati jolly del server. Per maggiori informazioni, vedere il "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione dei bucket" . **Nota**: non è possibile modificare il nome del bucket dopo averlo creato.
Regione	La regione del bucket. L'amministratore StorageGRID gestisce le regioni disponibili. La regione di un bucket può influire sulla politica di protezione dei dati applicata agli oggetti. Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione. **Nota**: non è possibile modificare la regione dopo aver creato il bucket.

2. Selezionare **Continua**.

Gestisci le impostazioni

Passi

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

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

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

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

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

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

automaticamente.

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

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

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

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

Modalità di conservazione predefinita	Descrizione
Governance	• Utenti con il `s3:BypassGovernanceRetention` il permesso può utilizzare il `x-amz-bypass-governance-retention: true` intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.
Conformità	• L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione. • La data di conservazione dell'oggetto può essere aumentata, ma non diminuita. • La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data. **Nota**: l'amministratore della rete deve consentirti di utilizzare la modalità di conformità.

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

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

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

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

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

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

5. Seleziona **Crea bucket**.

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

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

Visualizza i dettagli del bucket

Puoi visualizzare i bucket nel tuo account tenant.

Prima di iniziare

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

Passi

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

   Viene visualizzata la pagina Bucket.

2. Esaminare la tabella riepilogativa per ogni bucket.

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

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

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

   Funzionalità abilitate
   Elenco delle funzionalità abilitate per il bucket.

   Blocco oggetto S3
   Se il blocco oggetti S3 è abilitato per il bucket.

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

Regione

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

Conteggio degli oggetti

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

Quando si aggiungono o si eliminano oggetti, questo valore potrebbe non aggiornarsi immediatamente.

Spazio utilizzato

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

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

Utilizzo

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

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

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

Capacità

Se impostato, il limite di capacità per il bucket.

Data di creazione

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

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

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

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

   d. Visualizza o modifica le impostazioni per il bucket in ciascuna scheda, secondo necessità.
      - **Console S3**: visualizza gli oggetti per il bucket. Per ulteriori informazioni, fare riferimento a

"Utilizzare la console S3" .

- **Opzioni bucket**: visualizza o modifica le impostazioni delle opzioni. Alcune impostazioni, come S3 Object Lock, non possono essere modificate dopo la creazione del bucket.
  - "Gestire la coerenza del bucket"
  - "Aggiornamenti dell'ultimo orario di accesso"
  - "Limite di capacità"
  - "Versionamento degli oggetti"
  - "Blocco oggetto S3"
  - "Conservazione predefinita del bucket"
  - "Gestire la replicazione tra griglie"(se consentito all'inquilino)
- **Servizi di piattaforma**:"Gestire i servizi della piattaforma" (se consentito all'inquilino)
- **Accesso bucket**: visualizza o modifica le impostazioni delle opzioni. È necessario disporre di autorizzazioni di accesso specifiche.
  - Configurare"Condivisione delle risorse tra origini (CORS)" in modo che il bucket e gli oggetti al suo interno siano accessibili alle applicazioni web in altri domini.
  - "Controlla l'accesso degli utenti"per un bucket S3 e gli oggetti in quel bucket.

Applicare un tag di policy ILM a un bucket

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

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

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

Prima di iniziare

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

Passi

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

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

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

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

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

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

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

5. Selezionare il pulsante di opzione per il tag che si desidera assegnare al bucket.
6. Seleziona **Salva modifiche**. Un nuovo tag bucket S3 verrà impostato sul bucket con la chiave `NTAP-SG-ILM-BUCKET-TAG` e il valore del nome del tag della policy ILM.

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

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

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

Gestisci i criteri del bucket

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

Prima di iniziare

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

Passi

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

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

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

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

Gestire la coerenza del bucket

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

Prima di iniziare

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

Linee guida sulla coerenza del bucket

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

Modifica la coerenza del bucket

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

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

Passi

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

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la fisarmonica **.
4. Selezionare una coerenza per le operazioni eseguite sugli oggetti in questo bucket.
   - **Tutti**: fornisce il massimo livello di coerenza. Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
   - **Strong-global**: garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti.
   - **Strong-site**: garantisce la coerenza di lettura e scrittura per tutte le richieste client all'interno di un sito.

- **Lettura dopo nuova scrittura** (predefinito): fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
- **Disponibile**: fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool .

5. Seleziona **Salva modifiche**.

Cosa succede quando si modificano le impostazioni del bucket

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

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

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

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

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

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

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

Abilita o disabilita gli aggiornamenti dell'ultimo orario di accesso

Quando gli amministratori della griglia creano le regole di gestione del ciclo di vita delle informazioni (ILM) per un sistema StorageGRID , possono facoltativamente specificare che l'orario dell'ultimo accesso a un oggetto venga utilizzato per determinare se spostare

tale oggetto in una posizione di archiviazione diversa. Se si utilizza un tenant S3, è possibile sfruttare tali regole abilitando gli aggiornamenti dell'ora dell'ultimo accesso per gli oggetti in un bucket S3.

Queste istruzioni si applicano solo ai sistemi StorageGRID che includono almeno una regola ILM che utilizza l'opzione **Ultimo orario di accesso** come filtro avanzato o come orario di riferimento. Se il sistema StorageGRID non include tale regola, è possibile ignorare queste istruzioni. Vedere"Utilizzare l'orario dell'ultimo accesso nelle regole ILM" per i dettagli.

Prima di iniziare

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

Informazioni su questo compito

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

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

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

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

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

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

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

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

Tipo di richiesta	Comportamento se l'ultimo orario di accesso è disabilitato (predefinito)		Comportamento se l'ultimo orario di accesso è abilitato	
	Ultimo orario di accesso aggiornato?	Oggetto aggiunto alla coda di valutazione ILM?	Ultimo orario di accesso aggiornato?	Oggetto aggiunto alla coda di valutazione ILM?

Richiesta di recupero di un oggetto, del suo elenco di controllo di accesso o dei suoi metadati	NO	NO	SÌ	SÌ
Richiesta di aggiornamento dei metadati di un oggetto	SÌ	SÌ	SÌ	SÌ
Richiesta di elencare oggetti o versioni di oggetti	NO	NO	NO	NO
Richiesta di copiare un oggetto da un bucket all'altro	• No, per la copia sorgente • Sì, per la copia di destinazione	• No, per la copia sorgente • Sì, per la copia di destinazione	• Sì, per la copia sorgente • Sì, per la copia di destinazione	• Sì, per la copia sorgente • Sì, per la copia di destinazione
Richiesta di completamento di un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Passi

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

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la voce accordion **Aggiornamenti ora ultimo accesso**.
4. Abilita o disabilita gli aggiornamenti dell'orario dell'ultimo accesso.
5. Seleziona **Salva modifiche**.

Modificare il controllo delle versioni degli oggetti per un bucket

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

Prima di iniziare

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

Informazioni su questo compito

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

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

Per ulteriori informazioni, vedere quanto segue:

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

Passi

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

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la voce accordion **Versionamento oggetto**.
4. Seleziona uno stato di controllo delle versioni per gli oggetti in questo bucket.

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

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

5. Seleziona **Salva modifiche**.

Utilizzare S3 Object Lock per conservare gli oggetti

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

L’amministratore della griglia deve concederti l’autorizzazione per utilizzare funzionalità specifiche di S3 Object Lock.

Che cos’è S3 Object Lock?

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

Quando l’impostazione globale S3 Object Lock è abilitata per un sistema StorageGRID , un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se in un bucket è abilitato S3 Object Lock, è necessario il controllo delle versioni del bucket, che viene abilitato automaticamente.

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

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

Un bucket con S3 Object Lock e conservazione predefinita configurata può contenere oggetti caricati con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l’impostazione predefinita, perché l’impostazione di conservazione non è stata configurata a livello di oggetto.

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

Modalità di conservazione

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

- In modalità conformità:
  - L’oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.
  - La data di conservazione dell’oggetto può essere aumentata, ma non diminuita.
  - La data di conservazione dell’oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità di governance:
  - Gli utenti con autorizzazioni speciali possono utilizzare un’intestazione di bypass nelle richieste per modificare determinate impostazioni di conservazione.
  - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.
  - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

Impostazioni di conservazione per le versioni degli oggetti

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

- **Modalità di conservazione**: conformità o governance.
- **Retain-until-date**: se la retain-until-date di una versione di un oggetto è futura, l’oggetto può essere recuperato, ma non eliminato.

- **Sospensione legale**: l'applicazione di una sospensione legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di scadenza, ma rimane in vigore finché non viene rimossa esplicitamente. Le sospensioni legali sono indipendenti dalla data di conservazione fino alla data di scadenza.

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

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

Impostazione di conservazione predefinita per i bucket

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

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

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

Vedere"Crea un bucket S3" E"Aggiorna la conservazione predefinita del blocco degli oggetti S3" .

Attività di blocco degli oggetti S3

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

Amministratore di rete

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

Utente inquilino

- Esaminare le considerazioni relative a bucket e oggetti con S3 Object Lock.
- Se necessario, contattare l'amministratore della griglia per abilitare l'impostazione globale di blocco degli oggetti S3 e impostare le autorizzazioni.
- Crea bucket con S3 Object Lock abilitato.
- Facoltativamente, configura le impostazioni di conservazione predefinite per un bucket:
  - Modalità di conservazione predefinita: Governance o Conformità, se consentita dall'amministratore della rete.
  - Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione

massimo impostato dall'amministratore della griglia.

- Utilizzare l'applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica dell'oggetto:
  - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore della rete.
  - Conserva fino alla data: deve essere inferiore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti per i bucket con S3 Object Lock abilitato

- Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID , è possibile utilizzare Tenant Manager, Tenant Management API o S3 REST API per creare bucket con S3 Object Lock abilitato.
- Se si prevede di utilizzare S3 Object Lock, è necessario abilitarlo quando si crea il bucket. Non è possibile abilitare S3 Object Lock per un bucket esistente.
- Quando S3 Object Lock è abilitato per un bucket, StorageGRID abilita automaticamente il controllo delle versioni per quel bucket. Non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione predefinita e un periodo di conservazione per ciascun bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di impostazioni di conservazione proprie. È possibile ignorare queste impostazioni predefinite specificando una modalità di conservazione e una data di conservazione per ogni versione dell'oggetto quando viene caricata.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con S3 Object Lock abilitato.
- La replica CloudMirror non è supportata per i bucket con S3 Object Lock abilitato.

Requisiti per gli oggetti nei bucket con S3 Object Lock abilitato

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

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

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

1. **Ingestione di oggetti**

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

   - Se per l'oggetto sono specificate impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
   - Se non vengono specificate impostazioni di conservazione per l'oggetto, vengono applicate le

impostazioni predefinite del bucket, se presenti.

- Se non vengono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

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

2. **Conservazione ed eliminazione degli oggetti**

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

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

Posso continuare a gestire i bucket Compliant legacy?

La funzionalità S3 Object Lock sostituisce la funzionalità Compliance disponibile nelle versioni precedenti StorageGRID . Se hai creato bucket conformi utilizzando una versione precedente di StorageGRID, puoi continuare a gestire le impostazioni di questi bucket; tuttavia, non puoi più creare nuovi bucket conformi. Per le istruzioni, vederehttps://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"^] .

Aggiorna la conservazione predefinita del blocco degli oggetti S3

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

Prima di iniziare

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

Passi

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

   Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, seleziona la voce accordion **Blocco oggetto S3**.
4. Facoltativamente, abilita o disabilita la **Conservazione predefinita** per questo bucket.

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

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

Modalità di conservazione predefinita	Descrizione
Governance	• Utenti con il `s3:BypassGovernanceRetention` il permesso può utilizzare il `x-amz-bypass-governance-retention: true` intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.
Conformità	• L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione. • La data di conservazione dell'oggetto può essere aumentata, ma non diminuita. • La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data. **Nota**: l'amministratore della rete deve consentirti di utilizzare la modalità di conformità.

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

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

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

7. Seleziona **Salva modifiche**.

Configurare la condivisione delle risorse tra origini (CORS)

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

Prima di iniziare

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

autorizzazioni nei criteri di gruppo o di bucket.

- Per le richieste di configurazione PUT CORS, appartieni a un gruppo di utenti che ha"Gestisci tutti i permessi dei bucket" . Questa autorizzazione sostituisce le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- IL"Permesso di accesso root" fornisce l'accesso a tutte le richieste di configurazione CORS.

Informazioni su questo compito

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

Abilita CORS per un bucket

Passi

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

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

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

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

   Viene visualizzata la pagina dei dettagli del bucket.

4. Dalla scheda **Accesso bucket**, seleziona l'accordion **Condivisione risorse tra origini (CORS)**.

5. Selezionare la casella di controllo **Abilita CORS**.
6. Incollare il file XML di configurazione CORS nella casella di testo.
7. Seleziona **Salva modifiche**.

Modificare l'impostazione CORS

Passi

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

Disabilita l'impostazione CORS

Passi

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

Elimina gli oggetti nel bucket

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

Considerazioni e requisiti

Prima di eseguire questi passaggi, tenere presente quanto segue:

- Quando si eliminano gli oggetti in un bucket, StorageGRID rimuove definitivamente tutti gli oggetti e tutte le versioni degli oggetti in ciascun bucket selezionato da tutti i nodi e siti nel sistema StorageGRID . StorageGRID rimuove anche tutti i metadati degli oggetti correlati. Non sarà possibile recuperare queste informazioni.
- L'eliminazione di tutti gli oggetti in un bucket potrebbe richiedere minuti, giorni o addirittura settimane, a seconda del numero di oggetti, delle copie degli oggetti e delle operazioni simultanee.
- Se un secchio ha"Blocco oggetto S3 abilitato" , potrebbe rimanere nello stato **Eliminazione oggetti: sola lettura** per *anni*.

> Un bucket che utilizza S3 Object Lock rimarrà nello stato **Eliminazione oggetti: sola lettura** finché non verrà raggiunta la data di conservazione per tutti gli oggetti e non verranno rimossi eventuali blocchi legali.

- Durante l'eliminazione degli oggetti, lo stato del bucket è **Eliminazione oggetti: sola lettura**. In questo stato non è possibile aggiungere nuovi oggetti al bucket.
- Una volta eliminati tutti gli oggetti, il bucket rimane in stato di sola lettura. Puoi fare una delle seguenti cose:
  - Riporta il bucket in modalità scrittura e riutilizzalo per nuovi oggetti
  - Elimina il bucket
  - Mantieni il bucket in modalità di sola lettura per riservarne il nome per un uso futuro
- Se in un bucket è abilitato il controllo delle versioni degli oggetti, è possibile rimuovere i marcatori di eliminazione creati in StorageGRID 11.8 o versioni successive utilizzando le operazioni Elimina oggetti nel bucket.

- Se in un bucket è abilitato il controllo delle versioni degli oggetti, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11.7 o versioni precedenti. Visualizza le informazioni sull'eliminazione degli oggetti in un bucket in"Come vengono eliminati gli oggetti con versione S3" .
- Se usi"replicazione cross-grid" , notare quanto segue:
  - Utilizzando questa opzione non si elimina alcun oggetto dal bucket sull'altra griglia.
  - Se selezioni questa opzione per il bucket di origine, verrà attivato l'avviso **Errore di replica tra griglie** se aggiungi oggetti al bucket di destinazione sull'altra griglia. Se non puoi garantire che nessuno aggiungerà oggetti al contenitore sull'altra griglia,"disabilitare la replicazione tra griglie" per quel bucket prima di eliminare tutti gli oggetti bucket.

Prima di iniziare

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

Passi

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

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

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

   Menu Azioni

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

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

   Pagina dei dettagli

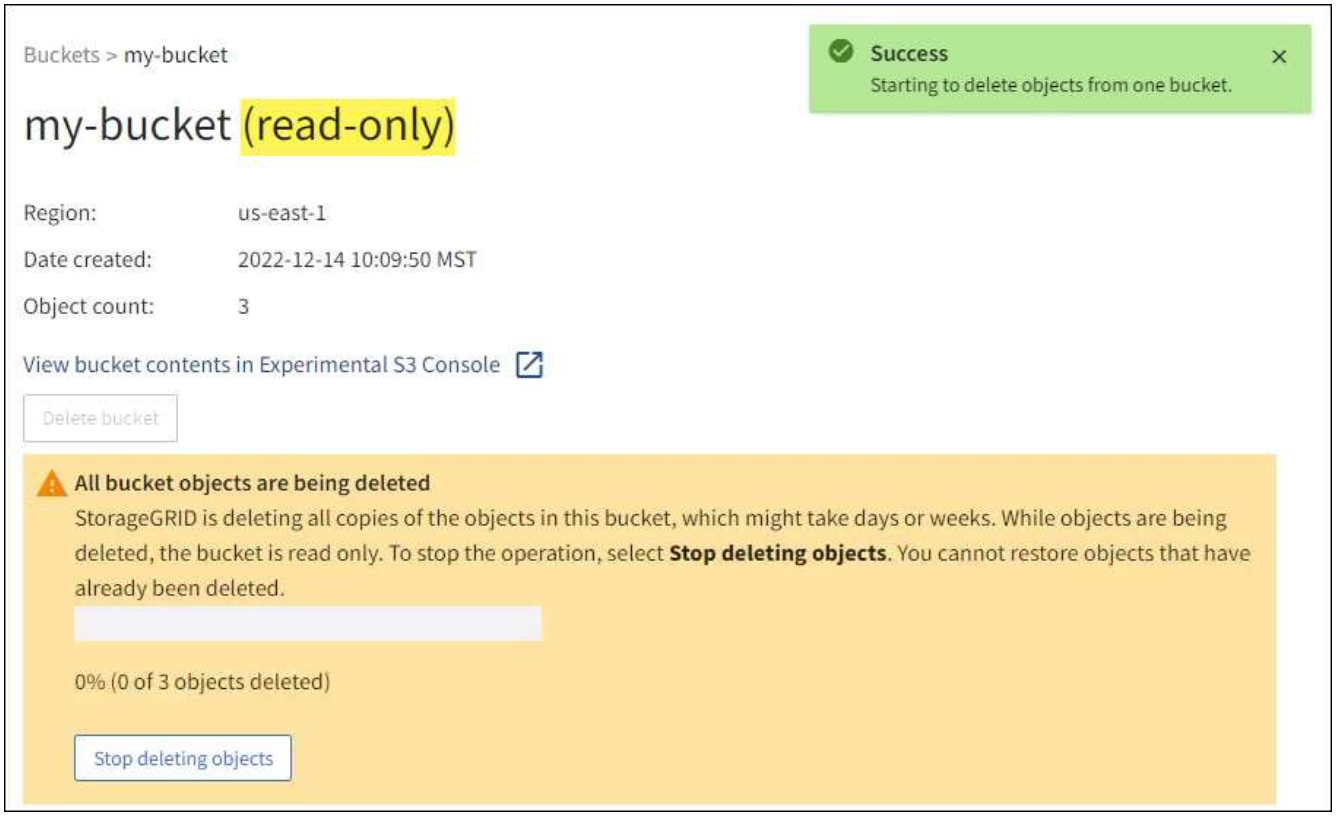
   a. Seleziona il nome di un bucket per visualizzarne i dettagli.

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

3. Quando viene visualizzata la finestra di dialogo di conferma, rivedere i dettagli, immettere **Sì** e selezionare **OK**.
4. Attendi che l'operazione di eliminazione abbia inizio.

   Dopo qualche minuto:

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

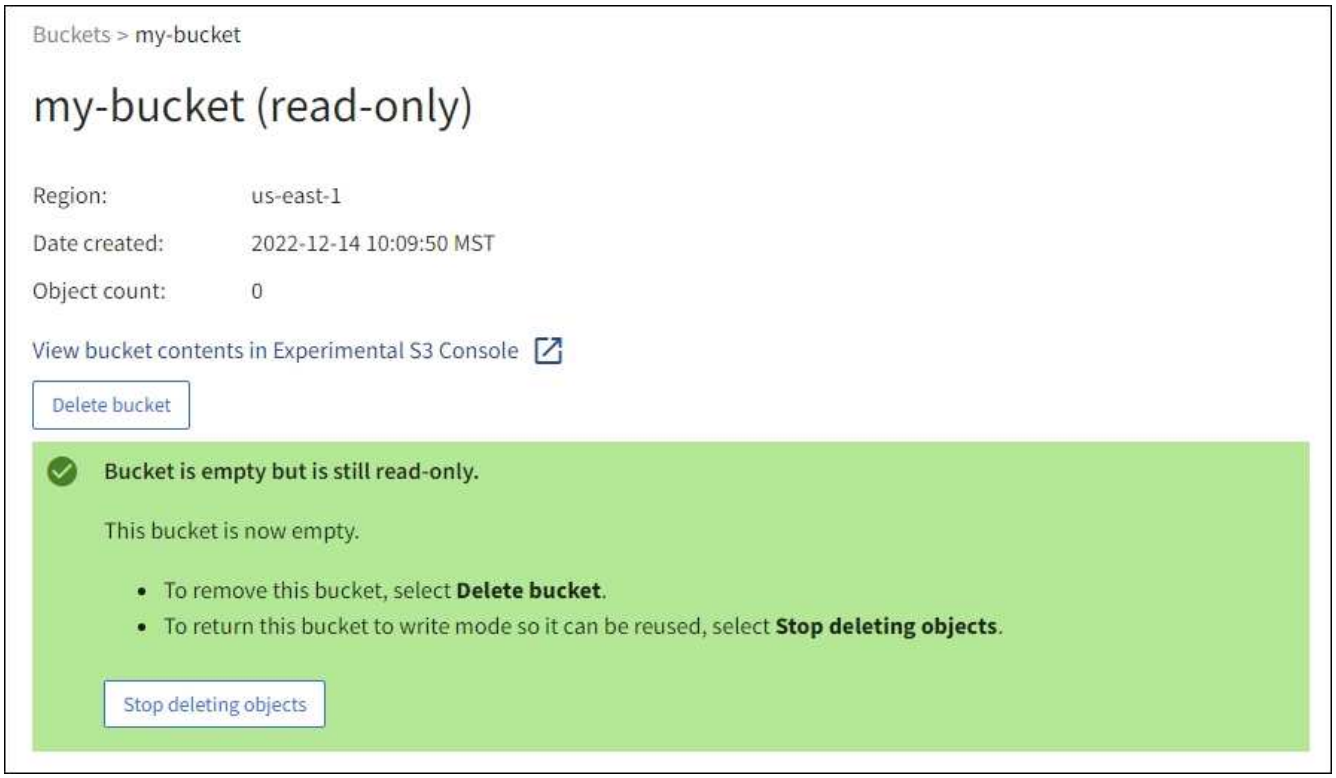


5. Se necessario, durante l'esecuzione dell'operazione, selezionare **Interrompi eliminazione oggetti** per interrompere il processo. Quindi, facoltativamente, seleziona **Elimina oggetti nel bucket** per riprendere il processo.

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

6. Attendere il completamento dell'operazione.

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



7. Eseguire una delle seguenti operazioni:
   - Esci dalla pagina per mantenere il bucket in modalità di sola lettura. Ad esempio, potresti mantenere un bucket vuoto in modalità di sola lettura per riservare il nome del bucket per un utilizzo futuro.
   - Elimina il bucket. È possibile selezionare **Elimina bucket** per eliminare un singolo bucket oppure tornare alla pagina Bucket e selezionare **Azioni** > **Elimina** bucket per rimuovere più di un bucket.

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

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

Elimina bucket S3

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

Prima di iniziare

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

Informazioni su questo compito

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

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

Passi

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

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

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

   Menu Azioni

   a. Seleziona la casella di controllo per ogni bucket che desideri eliminare.

   b. Selezionare **Azioni** > **Elimina bucket**.

   Pagina dei dettagli

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

   b. Seleziona **Elimina bucket**.

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

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

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

Utilizzare la console S3

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

S3 Console ti consente di:

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

> S3 Console offre un'esperienza utente migliorata per i casi più comuni. Non è progettato per sostituire le operazioni CLI o API in tutte le situazioni.
>
> Se l'utilizzo di S3 Console fa sì che le operazioni richiedano troppo tempo (ad esempio, minuti o ore), prendere in considerazione quanto segue:
>
> - Riduzione del numero di oggetti selezionati
> - Utilizzo di metodi non grafici (API o CLI) per accedere ai dati

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un"browser web supportato" .
- Se vuoi gestire gli oggetti, devi appartenere a un gruppo di utenti che dispone dell'autorizzazione di accesso Root. In alternativa, puoi appartenere a un gruppo di utenti che dispone dell'autorizzazione Utilizza la scheda Console S3 e dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket. Vedere "Autorizzazioni di gestione degli inquilini" .
- Per l'utente è stato configurato un criterio di gruppo o bucket S3. Vedere "Utilizzare criteri di accesso a bucket e gruppi" .
- Conosci l'ID della chiave di accesso dell'utente e la chiave di accesso segreta. Facoltativamente, hai un `.csv` file contenente queste informazioni. Vedi il"istruzioni per la creazione delle chiavi di accesso" .

Passi

1. Selezionare **ARCHIVIAZIONE** > **Bucket** > ***nome bucket***.
2. Selezionare la scheda Console S3.
3. Incolla l'ID della chiave di accesso e la chiave di accesso segreta nei campi. Altrimenti, seleziona **Carica chiavi di accesso** e seleziona il tuo `.csv` file.
4. Seleziona * Sign in*.
5. Viene visualizzata la tabella degli oggetti bucket. Puoi gestire gli oggetti in base alle tue esigenze.

Informazioni aggiuntive

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

Gestire i servizi della piattaforma S3

Servizi della piattaforma S3

Panoramica e considerazioni sui servizi della piattaforma

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

Per informazioni su S3, vedere"Utilizzare l'API REST S3" .

Panoramica dei servizi della piattaforma

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

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

Per un singolo bucket S3 è possibile configurare qualsiasi combinazione di servizi di piattaforma. Ad esempio, è possibile configurare entrambi i"Servizio CloudMirror" E"notifiche" su un bucket StorageGRID S3 in modo da poter eseguire il mirroring di oggetti specifici su Amazon Simple Storage Service (S3), inviando al contempo una notifica su ciascun oggetto a un'applicazione di monitoraggio di terze parti per aiutarti a tenere traccia delle tue spese AWS.

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

Come sono configurati i servizi della piattaforma

I servizi della piattaforma comunicano con endpoint esterni configurati tramite"Responsabile degli inquilini" o il"API di gestione degli inquilini" . Ogni endpoint rappresenta una destinazione esterna, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento Amazon SNS o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

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

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

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

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

Servizio di piattaforma	API REST S3	Fare riferimento a
Replica CloudMirror	• OttieniReplicazioneBucket • PutBucketReplication	• "Replica CloudMirror" • "Operazioni sui bucket"
Notifiche	• Configurazione di notifica di GetBucket • Configurazione della notifica PutBucket	• "Notifiche" • "Operazioni sui bucket"

Servizio di piattaforma	API REST S3	Fare riferimento a
Integrazione della ricerca	• Configurazione della notifica dei metadati del bucket GET • Configurazione della notifica dei metadati del bucket PUT	• "Integrazione della ricerca" • "Operazioni personalizzate StorageGRID"

Considerazioni sull'utilizzo dei servizi della piattaforma

Considerazione	Dettagli
Monitoraggio dell'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 e si verifica un arretrato di richieste elevato, le richieste client aggiuntive (ad esempio le richieste PUT) a StorageGRID non riusciranno. È necessario riprovare queste richieste non riuscite quando l'endpoint diventa raggiungibile.
Limitazione dell'endpoint di destinazione	Il software StorageGRID potrebbe limitare le richieste S3 in arrivo per un bucket se la velocità con cui vengono inviate le richieste supera la velocità con cui l'endpoint di destinazione può riceverle. La limitazione si verifica solo quando è presente un arretrato di richieste in attesa di essere inviate all'endpoint di destinazione. L'unico effetto visibile è che le richieste S3 in arrivo impiegheranno più tempo per essere eseguite. Se si inizia a rilevare un rallentamento significativo delle prestazioni, è opportuno ridurre la velocità di acquisizione o utilizzare un endpoint con capacità maggiore. Se l'arretrato di richieste continua ad aumentare, le operazioni S3 del client (come le richieste PUT) alla fine falliranno. Le richieste CloudMirror hanno maggiori probabilità di essere influenzate dalle prestazioni dell'endpoint di destinazione, perché in genere comportano un trasferimento di dati maggiore rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.
Garanzie di ordinazione	StorageGRID garantisce l'ordinamento delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni su un oggetto avvengono nello stesso sito, lo stato finale dell'oggetto (per la replica) sarà sempre uguale allo stato in StorageGRID. StorageGRID fa del suo meglio per ordinare le richieste quando le operazioni vengono eseguite tra i siti StorageGRID . Ad esempio, se inizialmente si scrive un oggetto sul sito A e poi si sovrascrive lo stesso oggetto sul sito B, non è garantito che l'oggetto finale replicato da CloudMirror nel bucket di destinazione sia l'oggetto più recente.

Considerazione	Dettagli
Eliminazioni di oggetti guidate da ILM	Per adeguarsi al comportamento di eliminazione di AWS CRR e Amazon Simple Notification Service, le richieste di notifica di eventi e CloudMirror non vengono inviate quando un oggetto nel bucket di origine viene eliminato a causa delle regole StorageGRID ILM. Ad esempio, non vengono inviate richieste di notifiche di eventi o CloudMirror se una regola ILM elimina un oggetto dopo 14 giorni. Al contrario, le richieste di integrazione della ricerca vengono inviate quando gli oggetti vengono eliminati a causa di ILM.
Utilizzo degli endpoint Kafka	Per gli endpoint Kafka, Mutual TLS non è supportato. Di conseguenza, se hai `ssl.client.auth` impostato su `required` nella configurazione del broker Kafka, potrebbe causare problemi di configurazione dell'endpoint Kafka. L'autenticazione degli endpoint Kafka utilizza i seguenti tipi di autenticazione. Questi tipi sono diversi da quelli utilizzati per l'autenticazione di altri endpoint, come Amazon SNS, e richiedono credenziali di nome utente e password. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Nota:** le impostazioni del proxy di archiviazione configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Considerazioni sull'utilizzo del servizio di replica CloudMirror

Considerazione	Dettagli
Stato di replicazione	StorageGRID non supporta il `x-amz-replication-status` intestazione.
Dimensione dell'oggetto	La dimensione massima degli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è 5 TiB, che è la stessa della dimensione massima *supportata* dell'oggetto. **Nota**: la dimensione massima *consigliata* per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa invece il caricamento multiparte.
Versionamento del bucket e ID versione	Se il bucket S3 di origine in StorageGRID ha il controllo delle versioni abilitato, è necessario abilitare il controllo delle versioni anche per il bucket di destinazione. Quando si utilizza il controllo delle versioni, tenere presente che l'ordinamento delle versioni degli oggetti nel bucket di destinazione è basato sul miglior sforzo possibile e non è garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3. **Nota**: gli ID versione per il bucket di origine in StorageGRID non sono correlati agli ID versione per il bucket di destinazione.

Considerazione	Dettagli
Tagging per le versioni degli oggetti	A causa delle limitazioni del protocollo S3, il servizio CloudMirror non replica alcuna richiesta PutObjectTagging o DeleteObjectTagging che fornisca un ID versione. Poiché gli ID versione per l'origine e la destinazione non sono correlati, non esiste alcun modo per garantire che un aggiornamento del tag a un ID versione specifico venga replicato. Al contrario, il servizio CloudMirror replica le richieste PutObjectTagging o DeleteObjectTagging che non specificano un ID versione. Queste richieste aggiornano i tag per la chiave più recente (o per l'ultima versione se il bucket è sottoposto a versioning). Vengono replicati anche gli ingest normali con tag (non gli aggiornamenti dei tag).
Caricamenti multiparte e `ETag` valori	Quando si esegue il mirroring di oggetti caricati tramite un caricamento multiparte, il servizio CloudMirror non conserva le parti. Di conseguenza, il `ETag` il valore per l'oggetto specchiato sarà diverso da quello `ETag` valore dell'oggetto originale.
Oggetti crittografati con SSE-C (crittografia lato server con chiavi fornite dal cliente)	Il servizio CloudMirror non supporta oggetti crittografati con SSE-C. Se si tenta di importare un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione fallisce.
Bucket con blocco oggetto S3 abilitato	La replica non è supportata per i bucket di origine o di destinazione con S3 Object Lock abilitato.

Comprendere il servizio di replica CloudMirror

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

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

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

CloudMirror e ILM

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

CloudMirror e replicazione cross-grid

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

CloudMirror e bucket S3

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

Secchi esistenti

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

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

Più bucket di destinazione

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

Bucket con o senza versione

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

Eliminazione, cicli di replicazione ed eventi

Comportamento di eliminazione

È lo stesso comportamento di eliminazione del servizio Amazon S3, Cross-Region Replication (CRR). L'eliminazione di un oggetto in un bucket di origine non elimina mai un oggetto replicato nella destinazione. Se sia il bucket di origine che quello di destinazione sono sottoposti a versioning, il marcatore di eliminazione viene replicato. Se il bucket di destinazione non è sottoposto a controllo di versione, l'eliminazione di un oggetto nel bucket di origine non replica il marcatore di eliminazione nel bucket di destinazione né elimina l'oggetto di destinazione.

Protezione dai cicli di replicazione

Quando gli oggetti vengono replicati nel bucket di destinazione, StorageGRID li contrassegna come "repliche". Un bucket StorageGRID di destinazione non replicherà più gli oggetti contrassegnati come repliche, proteggendoti da loop di replica accidentali. Questa marcatura della replica è interna a StorageGRID e non impedisce di sfruttare AWS CRR quando si utilizza un bucket Amazon S3 come destinazione.

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

Eventi nel bucket di destinazione

L'unicità e l'ordinamento degli eventi nel bucket di destinazione non sono garantiti. A seguito delle operazioni intraprese per garantire il successo della consegna, potrebbero essere consegnate alla

destinazione più copie identiche di un oggetto sorgente. In rari casi, quando lo stesso oggetto viene aggiornato simultaneamente da due o più siti StorageGRID diversi, l'ordinamento delle operazioni sul bucket di destinazione potrebbe non corrispondere all'ordinamento degli eventi sul bucket di origine.

Comprendere le notifiche per i bucket

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

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

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

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

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

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

Nome chiave	Valore StorageGRID
origineevento	`sgws:s3`
Regione aws	*non incluso*
x-amz-id-2	*non incluso*

Nome chiave	Valore StorageGRID
arn	`urn:sgws:s3:::bucket_name`

Comprendere il servizio di integrazione della ricerca

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

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

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

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

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

Integrazione della ricerca e bucket S3

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

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

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

Notifiche di ricerca

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

- Viene creato un oggetto.
- Un oggetto viene eliminato, anche quando gli oggetti vengono eliminati a seguito dell'esecuzione della politica ILM della griglia.

- I metadati o i tag degli oggetti vengono aggiunti, aggiornati o eliminati. Durante l'aggiornamento viene sempre inviato l'insieme completo di metadati e tag, non solo i valori modificati.

Dopo aver aggiunto l'XML di configurazione delle notifiche dei metadati a un bucket, le notifiche vengono inviate per tutti i nuovi oggetti creati e per tutti gli oggetti modificati aggiornandone i dati, i metadati utente o i tag. Tuttavia, le notifiche non vengono inviate per gli oggetti che erano già presenti nel bucket. Per garantire che i metadati degli oggetti per tutti gli oggetti nel bucket vengano inviati alla destinazione, è necessario effettuare una delle seguenti operazioni:

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

Servizio di integrazione della ricerca ed Elasticsearch

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

Gestire gli endpoint dei servizi della piattaforma

Configurare gli endpoint dei servizi della piattaforma

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

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

Che cos'è un endpoint dei servizi di piattaforma?

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

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

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

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

SNS) e notifiche sull'eliminazione di oggetti a un secondo argomento Amazon SNS.

Endpoint per la replica CloudMirror

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

Endpoint per le notifiche

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

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

Endpoint per il servizio di integrazione della ricerca

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

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

Informazioni correlate

"Amministra StorageGRID"

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

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

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

Elementi URN

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

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

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

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

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

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

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

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

URN per servizi ospitati su AWS e GCP

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

- Replica CloudMirror:

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

- Notifiche:

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

- Integrazione della ricerca:

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

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

URN per servizi ospitati localmente

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

- Replica CloudMirror:

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

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

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

- Notifiche:

  Specificare un endpoint Amazon Simple Notification Service:

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

  Specificare un endpoint Kafka:

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

- Integrazione della ricerca:

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

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

Crea endpoint dei servizi della piattaforma

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

Prima di iniziare

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

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

  - Nome univoco della risorsa (URN)

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

  - Credenziali di autenticazione (se richieste):

Cerca endpoint di integrazione

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

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

Endpoint di replicazione CloudMirror

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

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

Endpoint Amazon SNS

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

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

Punti finali di Kafka

Per gli endpoint Kafka, puoi utilizzare le seguenti credenziali:

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

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

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

Passi

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

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

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

   Utilizzare uno dei seguenti formati:

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

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

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

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

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

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

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

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

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

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

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

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

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

Cerca endpoint di integrazione

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

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

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

Endpoint di replicazione CloudMirror

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

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

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

Endpoint Amazon SNS

Inserisci o carica le credenziali per un endpoint Amazon SNS.

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

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

Punti finali di Kafka

Inserisci o carica le credenziali per un endpoint Kafka.

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce accesso anonimo alla destinazione. Funziona solo per gli endpoint con sicurezza disabilitata.	Nessuna autenticazione.
SASL/PLAIN	Utilizza un nome utente e una password con testo normale per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-256	Utilizza un nome utente e una password tramite un protocollo challenge-response e l'hashing SHA-256 per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-512	Utilizza un nome utente e una password tramite un protocollo challenge-response e l'hashing SHA-512 per autenticare le connessioni alla destinazione.	• Nome utente • Password

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

8. Selezionare **Continua**.

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

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

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

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

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

Informazioni correlate

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

Prova la connessione per l'endpoint dei servizi della piattaforma

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

Prima di iniziare

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

Informazioni su questo compito

StorageGRID non convalida che le credenziali abbiano le autorizzazioni corrette.

Passi

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

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

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

   Viene visualizzata la pagina dei dettagli dell'endpoint.

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

Modifica endpoint dei servizi della piattaforma

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

Prima di iniziare

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

Passi

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

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

2. Seleziona l'endpoint che vuoi modificare.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

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

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

   a. Per modificare il nome visualizzato per l'endpoint, seleziona l'icona di modifica .
   b. Se necessario, modificare l'URI.
   c. Se necessario, modificare il tipo di autenticazione.
      - Per l'autenticazione con chiave di accesso, modificare la chiave secondo necessità selezionando **Modifica chiave S3** e incollando un nuovo ID chiave di accesso e una chiave di accesso segreta. Se devi annullare le modifiche, seleziona **Annulla modifica chiave S3**.

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

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

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

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

Elimina l'endpoint dei servizi della piattaforma

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

Prima di iniziare

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

Passi

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

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

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

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

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

   Appare un messaggio di conferma.

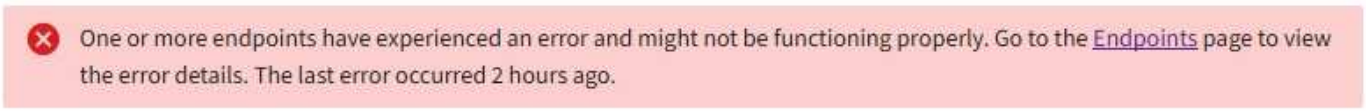
4. Selezionare **Elimina endpoint**.

Risolvere gli errori degli endpoint dei servizi della piattaforma

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

Determina se si è verificato un errore

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



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

Passi

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

Controlla se l'errore è ancora attuale

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

Passi

1. Selezionare l'endpoint.

   Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Selezionare **Connessione** > **Test connessione**.

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

Risolvi gli errori dell'endpoint

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

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

Passi

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

4. Selezionare **Connessione** > **Test connessione**.

Credenziali dell'endpoint con autorizzazioni insufficienti

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

Informazioni correlate

- **Amministra StorageGRID › Risolvi i problemi dei servizi della piattaforma**
- "Crea endpoint dei servizi della piattaforma"
- "Prova la connessione per l'endpoint dei servizi della piattaforma"
- "Modifica endpoint dei servizi della piattaforma"

Configurare la replica di CloudMirror

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

Prima di iniziare

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

Informazioni su questo compito

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

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

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

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

- Quando si crea e si applica un XML di configurazione della replica del bucket valido, è necessario utilizzare l'URN di un endpoint del bucket S3 per ogni destinazione.
- La replica non è supportata per i bucket di origine o di destinazione con S3 Object Lock abilitato.
- Se si abilita la replica CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket

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

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

Passi

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

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

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

Viene visualizzata la pagina dei dettagli del bucket.

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

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

7. Verificare che la replica sia configurata correttamente:
   a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per la replica come specificato nella configurazione della replica.

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

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

      Per gli oggetti di piccole dimensioni la replicazione avviene rapidamente.

Informazioni correlate

"Crea endpoint dei servizi della piattaforma"

Configurare le notifiche degli eventi

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

Prima di iniziare

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

Informazioni su questo compito

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

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

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

caratteristiche:

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

Passi

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

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

2. In Tenant Manager, seleziona **ARCHIVIAZIONE (S3)** > **Bucket**.
3. Selezionare il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

   a. Eseguire un'azione su un oggetto nel bucket di origine che soddisfi i requisiti per l'attivazione di una notifica come configurato nell'XML di configurazione.

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

   b. Conferma che una notifica è stata recapitata all'argomento Amazon SNS o Kafka di destinazione.

      Ad esempio, se l'argomento di destinazione è ospitato su Amazon SNS, puoi configurare il servizio in modo che ti venga inviata un'e-mail quando la notifica viene recapitata.

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

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

Informazioni correlate

"Comprendere le notifiche per i bucket"

"Utilizzare l'API REST S3"

"Crea endpoint dei servizi della piattaforma"

Configurare il servizio di integrazione della ricerca

È possibile abilitare l'integrazione della ricerca per un bucket creando un XML di integrazione della ricerca e utilizzando Tenant Manager per applicare l'XML al bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per il tuo account tenant da un amministratore StorageGRID .
- Hai già creato un bucket S3 di cui desideri indicizzare il contenuto.
- L'endpoint che intendi utilizzare come destinazione per il servizio di integrazione della ricerca esiste già e disponi del suo URN.
- Appartieni a un gruppo di utenti che ha il"Gestisci tutti i bucket o l'autorizzazione di accesso Root" . Queste autorizzazioni sostituiscono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket quando si configura il bucket tramite Tenant Manager.

Informazioni su questo compito

Dopo aver configurato il servizio di integrazione della ricerca per un bucket di origine, la creazione di un oggetto o l'aggiornamento dei metadati o dei tag di un oggetto attiva l'invio dei metadati dell'oggetto all'endpoint di destinazione.

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

Passi

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

      Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, potresti inviare metadati per oggetti con il prefisso `images` verso una destinazione e metadati per oggetti con il prefisso `videos` all'altro. Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, una configurazione che include una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2` non è consentito.

      Se necessario, fare riferimento aesempi per la configurazione dei metadati XML .

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

Elementi nel file XML di configurazione della notifica dei metadati:

Nome	Descrizione	Necessario
MetadatiNotificaConfigurazione	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati. Contiene uno o più elementi Rule.	SÌ
Regola	Tag contenitore 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 per la regola. Incluso nell'elemento Regola.	NO
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilitate. Incluso nell'elemento Regola.	SÌ
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Regola.	SÌ
Destinazione	Tag contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	SÌ

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

2. In Tenant Manager seleziona **ARCHIVIAZIONE (S3)** > **Bucket**.
3. Selezionare il nome del bucket di origine.

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

7. Verificare che il servizio di integrazione della ricerca sia configurato correttamente:
   a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per l'attivazione di una notifica di metadati come specificato nel file XML di configurazione.

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

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

Dopo aver finito

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

- Selezionare **ARCHIVIAZIONE (S3)** > **Bucket** e deselezionare la casella di controllo **Abilita integrazione ricerca**.
- Se si utilizza direttamente l'API S3, utilizzare una richiesta di notifica dei metadati DELETE Bucket. Consultare le istruzioni per l'implementazione delle applicazioni client S3.

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

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

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

Esempio: configurazione della notifica dei metadati con due regole

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

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

Formato di notifica dei metadati

Quando si abilita il servizio di integrazione della ricerca per un bucket, ogni volta che vengono aggiunti, aggiornati o eliminati metadati o tag di un oggetto, viene generato un documento JSON che viene inviato all'endpoint di destinazione.

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

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

Campi inclusi nel documento JSON

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

Informazioni su bucket e oggetti

`bucket`: Nome del bucket

`key`: Nome chiave dell'oggetto

`versionID`: Versione dell'oggetto, per gli oggetti nei bucket con versione

`region`: Regione del bucket, ad esempio `us-east-1`

Metadati di sistema

`size`: Dimensione dell'oggetto (in byte) visibile a un client HTTP

`md5`: Hash dell'oggetto

Metadati utente

`metadata`: Tutti i metadati utente per l'oggetto, come coppie chiave-valore

`key:value`

Etichette

`tags`: Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore

`key:value`

Come visualizzare i risultati in Elasticsearch

Per i tag e i metadati utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo che interpreti queste stringhe come date o

numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per la mappatura dei formati di data. Abilitare i mapping dei campi dinamici sull'indice prima di configurare il servizio di integrazione della ricerca. Dopo aver indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Utilizzare l'API REST S3

Versioni e aggiornamenti supportati dall'API REST S3

StorageGRID supporta l'API Simple Storage Service (S3), implementata come un 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 l'archiviazione di oggetti on-premise che utilizza il sistema StorageGRID . Sono necessarie modifiche minime all'uso attuale delle chiamate API REST S3 da parte di un'applicazione client.

Versioni supportate

StorageGRID supporta le seguenti versioni specifiche di S3 e HTTP.

Articolo	Versione
Specifiche API S3	"Documentazione di Amazon Web Services (AWS): Riferimento API di Amazon Simple Storage Service"
HTTP	1,1 Per ulteriori informazioni su HTTP, vedere HTTP/1.1 (RFC 7230-35). "IETF RFC 2616: Protocollo di trasferimento ipertestuale (HTTP/1.1)" **Nota**: StorageGRID non supporta il pipelining HTTP/1.1.

Aggiornamenti al supporto dell'API REST S3

Pubblicazione	Commenti
11,9	• Aggiunto supporto per valori di checksum SHA-256 precalcolati per le seguenti richieste e intestazioni supportate. Puoi utilizzare questa funzionalità per verificare l'integrità degli oggetti caricati: ◦ Caricamento multiparte completo: `x-amz-checksum-sha256` ◦ CreaCaricamentoMultiparte: `x-amz-checksum-algorithm` ◦ OttieniOggetto: `x-amz-checksum-mode` ◦ OggettoTesta: `x-amz-checksum-mode` ◦ ElencoParti ◦ MettiOggetto: `x-amz-checksum-sha256` ◦ CaricaParte: `x-amz-checksum-sha256` • Aggiunta la possibilità per l'amministratore della griglia di controllare le impostazioni di conservazione e conformità a livello di tenant. Queste impostazioni influiscono sulle impostazioni di Blocco oggetti S3. ◦ Modalità di conservazione predefinita del bucket e modalità di conservazione degli oggetti: Governance o Conformità, se consentito dall'amministratore della griglia. ◦ Periodo di conservazione predefinito del bucket e data di conservazione dell'oggetto: deve essere inferiore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia. • Supporto migliorato per `aws-chunked` codifica e streaming dei contenuti `x-amz-content-sha256` valori. Limitazioni: ◦ Se presente, `chunk-signature` è facoltativo e non convalidato ◦ Se presente, `x-amz-trailer` il contenuto viene ignorato
11,8	Aggiornati i nomi delle operazioni S3 per abbinarli ai nomi utilizzati in "Documentazione di Amazon Web Services (AWS): Riferimento API di Amazon Simple Storage Service" .
11,7	• Aggiunto"Riferimento rapido: richieste API S3 supportate" . • Aggiunto supporto per l'utilizzo della modalità GOVERNANCE con S3 Object Lock. • Aggiunto supporto per StorageGRID specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta per le richieste GET Object e HEAD Object. Questa intestazione fornisce lo stato di replicazione di un oggetto per la replica tra griglie. • Le richieste SelectObjectContent ora supportano gli oggetti Parquet.

Pubblicazione	Commenti
11,6	• Aggiunto supporto per l'utilizzo di `partNumber` parametro di richiesta nelle richieste GET Object e HEAD Object. • Aggiunto il supporto per una modalità di conservazione predefinita e un periodo di conservazione predefinito a livello di bucket per S3 Object Lock. • Aggiunto supporto per il `s3:object-lock-remaining-retention-days` chiave di condizione della policy per impostare l'intervallo di periodi di conservazione consentiti per i tuoi oggetti. • Modificata la dimensione massima *consigliata* per una singola operazione PUT Object a 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa invece il caricamento multiparte.
11,5	• Aggiunto supporto per la gestione della crittografia dei bucket. • Aggiunto supporto per S3 Object Lock e richieste di conformità legacy deprecate. • Aggiunto supporto per l'utilizzo di DELETE Multiple Objects su bucket con versione. • IL `Content-MD5` l'intestazione della richiesta è ora supportata correttamente.
11,4	• Aggiunto supporto per il tagging DELETE Bucket, GET Bucket e PUT Bucket. I tag di allocazione dei costi non sono supportati. • Per i bucket creati in StorageGRID 11.4, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le best practice in termini di prestazioni. • Aggiunto supporto per le notifiche bucket su `s3:ObjectRestore:Post` tipo di evento. • Sono ora applicati i limiti dimensionali AWS per le parti multiparte. Ogni parte di un caricamento multiparte deve avere una dimensione compresa tra 5 MiB e 5 GiB. L'ultima parte può essere inferiore a 5 MiB. • Aggiunto supporto per TLS 1.3
11,3	• Aggiunto supporto per la crittografia lato server dei dati degli oggetti con chiavi fornite dal cliente (SSE-C). • Aggiunto supporto per le operazioni del ciclo di vita del bucket DELETE, GET e PUT (solo azione di scadenza) e per `x-amz-expiration` intestazione di risposta. • Aggiornati PUT Object, PUT Object - Copia e Caricamento multiparte per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono durante l'acquisizione. • I cifrari TLS 1.1 non sono più supportati.
11,2	Aggiunto supporto per il ripristino di oggetti POST per l'uso con Cloud Storage Pool. Aggiunto supporto per l'utilizzo della sintassi AWS per ARN, chiavi di condizione della policy e variabili della policy nelle policy di gruppo e bucket. Continueranno a essere supportati i criteri di gruppo e bucket esistenti che utilizzano la sintassi StorageGRID . **Nota:** gli utilizzi di ARN/URN in altre configurazioni JSON/XML, compresi quelli utilizzati nelle funzionalità StorageGRID personalizzate, non sono cambiati.

Pubblicazione	Commenti
11,1	Aggiunto supporto per la condivisione delle risorse tra origini (CORS), HTTP per le connessioni client S3 ai nodi della griglia e impostazioni di conformità sui bucket.
11,0	Aggiunto supporto per la configurazione dei servizi della piattaforma (replica CloudMirror, notifiche e integrazione della ricerca Elasticsearch) per i bucket. È stato inoltre aggiunto il supporto per i vincoli di posizione del tagging degli oggetti per i bucket e la coerenza disponibile.
10,4	Aggiunto supporto per le modifiche alla scansione ILM relative al controllo delle versioni, aggiornamenti della pagina Nomi di dominio endpoint, condizioni e variabili nelle policy, esempi di policy e autorizzazione PutOverwriteObject.
10,3	Aggiunto supporto per il controllo delle versioni.
10,2	Aggiunto supporto per criteri di accesso a gruppi e bucket e per la copia multiparte (Carica parte - Copia).
10,1	Aggiunto supporto per caricamento multiparte, richieste in stile virtual hosted e autenticazione v4.
10,0	Supporto iniziale dell'API REST S3 da parte del sistema StorageGRID. La versione attualmente supportata del *Simple Storage Service API Reference* è 2006-03-01.

Riferimento rapido: richieste API S3 supportate

Questa pagina riassume il modo in cui StorageGRID supporta le API di Amazon Simple Storage Service (S3).

Questa pagina include solo le operazioni S3 supportate da StorageGRID.

> Per visualizzare la documentazione AWS per ciascuna operazione, selezionare il collegamento nell'intestazione.

Parametri di query URI comuni e intestazioni di richiesta

Se non diversamente specificato, sono supportati i seguenti parametri di query URI comuni:

- `versionId`(come richiesto per le operazioni sugli oggetti)

Se non diversamente specificato, sono supportate le seguenti intestazioni di richiesta comuni:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`

- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informazioni correlate

- "Dettagli di implementazione dell'API REST S3"
- "Riferimento API di Amazon Simple Storage Service: intestazioni di richiesta comuni"

"Annulla caricamento multiparte"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questo parametro di query URI aggiuntivo:

- `uploadId`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni per caricamenti multiparte"

"Caricamento multiparte completo"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questo parametro di query URI aggiuntivo:

- `uploadId`
- `x-amz-checksum-sha256`

Tag XML del corpo della richiesta

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

Documentazione StorageGRID

"Caricamento multiparte completo"

"CopiaOggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"CopiaOggetto"

"CreaBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-bucket-object-lock-enabled`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sui bucket"

"CreaCaricamentoMultiparte"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"CreaCaricamentoMultiparte"

"EliminaBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketLifecycle"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

- "Operazioni sui bucket"
- "Crea la configurazione del ciclo di vita S3"

"DeleteBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"DeleteBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"EliminaOggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questa intestazione di richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"EliminaOggetti"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questa intestazione di richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sugli oggetti"

"DeleteObjectTagging"

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"OttieniBucketAcl"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"Ottieni crittografia dei bucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketLifecycleConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

- "Operazioni sui bucket"
- "Crea la configurazione del ciclo di vita S3"

"OttieniPosizioneBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"Configurazione di notifica di GetBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"OttieniPoliticaBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"OttieniReplicazioneBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"OttieniBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"GetBucketVersioning"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"OttieniOggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri di query URI aggiuntivi:

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

E queste intestazioni di richiesta aggiuntive:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"OttieniOggetto"

"OttieniOggettoAcl"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"OttieniOggettoLegaleHold"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare S3 Object Lock"

"Ottieni configurazione blocco oggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare S3 Object Lock"

"Ottieni conservazione oggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare S3 Object Lock"

"OttieniTaggingOggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"HeadBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"HeadObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"HeadObject"

"ListBuckets"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Caricamenti multiparte di List"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Caricamenti multiparte di List"

"ElencoOggetti"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"ListObjectsV2"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`

- `max-keys`
- `prefix`
- `start-after`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"ListObjectVersions"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"ElencoParti"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri aggiuntivi:

- `max-parts`
- `part-number-marker`
- `uploadId`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Caricamenti multiparte di List"

"PutBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentazione StorageGRID

"Operazioni sui bucket"

"Configurazione del ciclo di vita di PutBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- `And`
- `Days`
- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`

- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentazione StorageGRID

- "Operazioni sui bucket"
- "Crea la configurazione del ciclo di vita S3"

"Configurazione della notifica PutBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta i seguenti tag XML del corpo della richiesta:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Per i dettagli sui campi del corpo JSON supportati, vedere"Utilizzare criteri di accesso a bucket e gruppi" .

"PutBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Tag XML del corpo della richiesta

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketVersioning"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Parametri del corpo della richiesta

StorageGRID supporta i seguenti parametri del corpo della richiesta:

- `VersioningConfiguration`
- `Status`

Documentazione StorageGRID

"Operazioni sui bucket"

"MettiOggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più queste intestazioni aggiuntive:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corpo della richiesta

- Dati binari dell'oggetto

Documentazione StorageGRID

"MettiOggetto"

"PutObjectLegalHold"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare S3 Object Lock"

"PutObjectLockConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare S3 Object Lock"

"PutObjectRetention"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questa intestazione aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare S3 Object Lock"

"PutObjectTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sugli oggetti"

"Ripristina oggetto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Per i dettagli sui campi del corpo supportati, vedere"Ripristina oggetto" .

"SelezionaOggettoContenuto"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta.

Corpo della richiesta

Per maggiori dettagli sui campi del corpo supportati, vedere quanto segue:

- "Utilizzare S3 Select"
- "SelezionaOggettoContenuto"

"CaricaParte"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri di query URI aggiuntivi:

- `partNumber`
- `uploadId`

E queste intestazioni di richiesta aggiuntive:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corpo della richiesta

- Dati binari della parte

Documentazione StorageGRID

"CaricaParte"

"CaricaParteCopia"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tuttiparametri e intestazioni comuni per questa richiesta, più questi parametri di query URI aggiuntivi:

- `partNumber`
- `uploadId`

E queste intestazioni di richiesta aggiuntive:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`

- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"CaricaParteCopia"

Testare la configurazione dell'API REST S3

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

Prima di iniziare

- Hai scaricato e installato AWS CLI da "aws.amazon.com/cli" .
- Facoltativamente, hai"creato un endpoint del bilanciatore del carico" . In caso contrario, è necessario conoscere l'indirizzo IP del nodo di archiviazione a cui si desidera connettersi e il numero di porta da utilizzare. Vedere "Indirizzi IP e porte per le connessioni client" .
- Hai"creato un account tenant S3" .
- Hai effettuato l'accesso al tenant e"ha creato una chiave di accesso" .

Per i dettagli su questi passaggi, vedere"Configurare le connessioni client" .

Passi

1. Configura le impostazioni AWS CLI per utilizzare l'account creato nel sistema StorageGRID :
   a. Entra nella modalità di configurazione: `aws configure`
   b. Inserisci l'ID della chiave di accesso per l'account che hai creato.
   c. Inserisci la chiave di accesso segreta per l'account che hai creato.
   d. Inserisci 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. Crea un bucket.

   In questo esempio si presuppone che sia stato configurato un endpoint del bilanciatore del carico per utilizzare l'indirizzo IP 10.96.101.17 e la porta 10443.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   Se il bucket viene creato correttamente, viene restituita la posizione del bucket, come mostrato nell'esempio seguente:

```
"Location": "/testbucket"
```

3. Carica 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, ovvero un hash dei dati dell'oggetto.

4. Elenca il contenuto 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. Elimina l'oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Elimina il bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Come StorageGRID implementa l'API REST S3

Richieste dei clienti in conflitto

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins".

La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Valori di coerenza

La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti tra diversi nodi di archiviazione e siti. È possibile modificare la coerenza in base alle esigenze dell'applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET successivo a un PUT completato con successo sarà in grado di leggere i dati

appena scritti. Le sovrascritture di oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni alla fine risultano coerenti. In genere, la propagazione delle sovrascritture richiede secondi o minuti, ma può richiedere fino a 15 giorni.

Se si desidera eseguire operazioni sugli oggetti con una consistenza diversa, è possibile:

- Specificare una coerenza perogni secchio .
- Specificare una coerenza perogni operazione API .
- Modificare la coerenza predefinita dell'intera griglia eseguendo una delle seguenti attività:
  - In Grid Manager, vai su **CONFIGURAZIONE** > **Sistema** > **Impostazioni di archiviazione** > **Coerenza predefinita**.
  - .

> Una modifica alla coerenza a livello di griglia si applica solo ai bucket creati dopo la modifica dell'impostazione. Per determinare i dettagli di una modifica, consultare il registro di controllo situato in `/var/local/log` (cerca **consistencyLevel**).

Valori di coerenza

La coerenza influisce sul modo in cui i metadati utilizzati da StorageGRID per tracciare gli oggetti vengono distribuiti tra i nodi e, di conseguenza, sulla disponibilità degli oggetti per le richieste dei client.

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

- **Tutti**: tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
- **Strong-global**: garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti.
- **Strong-site**: garantisce la coerenza di lettura e scrittura per tutte le richieste client all'interno di un sito.
- **Lettura dopo nuova scrittura**: (predefinito) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
- **Disponibile**: fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool .

Utilizzare la coerenza "Lettura dopo nuova scrittura" e "Disponibile"

Quando un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write", StorageGRID esegue la ricerca in più passaggi, come segue:

- Per prima cosa cerca l'oggetto utilizzando una bassa coerenza.
- Se la ricerca fallisce, la ripete al valore di coerenza successivo finché non raggiunge una coerenza equivalente al comportamento di strong-global.

Se un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write" ma l'oggetto non esiste, la ricerca dell'oggetto raggiungerà sempre una coerenza equivalente al comportamento per strong-global. Poiché questa coerenza richiede che siano disponibili più copie dei metadati dell'oggetto in ogni sito, è possibile ricevere un numero elevato di errori 500 Internal Server se due o più nodi di archiviazione nello stesso sito non sono disponibili.

A meno che non siano necessarie garanzie di coerenza simili ad Amazon S3, è possibile prevenire questi errori per le operazioni HEAD e GET impostando la coerenza su "Disponibile". Quando un'operazione HEAD o GET utilizza la coerenza "Disponibile", StorageGRID fornisce solo la coerenza finale. Non riprova un'operazione non riuscita aumentando la coerenza, quindi non richiede che siano disponibili più copie dei metadati dell'oggetto.

Specifica la coerenza per l'operazione API

Per impostare la coerenza per una singola operazione API, i valori di coerenza devono essere supportati per l'operazione ed è necessario specificare la coerenza nell'intestazione della richiesta. In questo esempio la coerenza viene impostata su "Strong-site" per un'operazione GetObject.

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

È necessario utilizzare la stessa coerenza per entrambe le operazioni PutObject e GetObject.

Specifica la coerenza per il bucket

Per impostare la coerenza per il bucket, puoi utilizzare StorageGRID"PUT Consistenza del secchio" richiesta. Oppure puoi"modificare la consistenza di un bucket" dal gestore dell'affitto.

Quando si imposta la consistenza di un bucket, tenere presente quanto segue:

- L'impostazione della coerenza per un bucket determina quale coerenza viene utilizzata per le operazioni S3 eseguite sugli oggetti nel bucket o sulla configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- La coerenza di una singola operazione API prevale sulla coerenza del bucket.
- In generale, i bucket dovrebbero utilizzare la coerenza predefinita, "Lettura dopo nuova scrittura". Se le richieste non funzionano correttamente, modificare, se possibile, il comportamento del client dell'applicazione. Oppure, configura il client in modo che specifichi la coerenza per ogni richiesta API. Impostare la coerenza a livello di bucket solo come ultima risorsa.

Come interagiscono la coerenza e le regole ILM per influenzare la protezione dei dati

Sia la scelta della coerenza sia la regola ILM influiscono sul modo in cui gli oggetti vengono protetti. Queste impostazioni possono interagire.

Ad esempio, la coerenza utilizzata quando un oggetto viene archiviato 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 sia ai suoi dati per soddisfare le richieste dei client, la selezione di livelli di protezione corrispondenti per la coerenza e il comportamento di acquisizione può garantire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Il seguente"opzioni di ingestione" sono disponibili per le regole ILM:

Doppio impegno

StorageGRID crea immediatamente copie provvisorie dell'oggetto e restituisce l'esito positivo al client. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

Rigoroso

Tutte le copie specificate nella regola ILM devono essere effettuate prima che il successo venga restituito al cliente.

Equilibrato

StorageGRID tenta di effettuare tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono effettuate copie provvisorie e il client riceve un messaggio di conferma dell'operazione riuscita. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

Esempio di come la coerenza e la regola ILM possono interagire

Supponiamo di avere una griglia a due siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM**: creare due copie dell'oggetto, una nel sito locale e una in un sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **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 dell'oggetto e distribuisce i metadati a entrambi i siti prima di restituire l'esito positivo al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione corretta del messaggio. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, copie sia dei dati dell'oggetto sia dei metadati dell'oggetto sono ancora presenti nel sito remoto. L'oggetto è completamente recuperabile.

Se invece si utilizzasse la stessa regola ILM e la coerenza del sito forte, il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati sul sito remoto, ma prima che i metadati dell'oggetto vengano distribuiti lì. In questo caso, il livello di protezione dei metadati degli oggetti non corrisponde al livello di protezione dei dati degli oggetti. Se il sito locale viene perso subito dopo l'acquisizione, anche i metadati dell'oggetto vengono persi. L'oggetto non può essere recuperato.

L'interrelazione tra coerenza e regole ILM può essere complessa. Se hai bisogno di assistenza, contatta NetApp .

Versionamento degli oggetti

È possibile impostare lo stato di controllo delle versioni di un bucket se si desidera conservare più versioni di ciascun oggetto. Abilitare il controllo delle versioni per un bucket può contribuire a proteggere gli oggetti dall'eliminazione accidentale e consente di recuperare e ripristinare le versioni precedenti di un oggetto.

Il sistema StorageGRID implementa il controllo delle versioni con supporto per la maggior parte delle funzionalità e con alcune limitazioni. StorageGRID supporta fino a 10.000 versioni di ciascun oggetto.

Il controllo delle versioni degli oggetti può essere combinato con la gestione del ciclo di vita delle informazioni (ILM) StorageGRID o con la configurazione del ciclo di vita del bucket S3. È necessario abilitare esplicitamente il controllo delle versioni per ogni bucket. Quando il controllo delle versioni è abilitato per un bucket, a ogni oggetto aggiunto al bucket viene assegnato un ID versione, generato dal sistema StorageGRID .

L'eliminazione tramite MFA (autenticazione a più fattori) non è supportata.

Il controllo delle versioni può essere abilitato solo sui bucket creati con StorageGRID versione 10.3 o successiva.

ILM e controllo delle versioni

Le policy ILM vengono applicate a ciascuna versione di un oggetto. Un processo di scansione ILM analizza continuamente tutti gli oggetti e li rivaluta in base alla politica ILM corrente. Tutte le modifiche apportate ai criteri ILM vengono applicate a tutti gli oggetti precedentemente acquisiti. Sono incluse le versioni precedentemente acquisite se è abilitato il controllo delle versioni. La scansione ILM applica le nuove modifiche ILM agli oggetti precedentemente acquisiti.

Per gli oggetti S3 nei bucket abilitati per il controllo delle versioni, il supporto del controllo delle versioni consente di creare regole ILM che utilizzano "Ora non corrente" come ora di riferimento (selezionare **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti?" in"Passaggio 1 della procedura guidata Crea una regola ILM"). Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. Utilizzando un filtro "Tempo non corrente" è possibile creare criteri che riducono l'impatto sull'archiviazione delle versioni precedenti degli oggetti.

Quando si carica una nuova versione di un oggetto utilizzando un'operazione di caricamento multiparte, il tempo non corrente per la versione originale dell'oggetto riflette il momento in cui è stato creato il caricamento multiparte per la nuova versione, non il momento in cui è stato completato il caricamento multiparte. In casi limitati, l'orario non aggiornato della versione originale potrebbe essere precedente di ore o giorni rispetto all'orario della versione corrente.

Informazioni correlate

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

Utilizzare l'API REST S3 per configurare S3 Object Lock

Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID , è possibile creare bucket con S3 Object Lock abilitato. È possibile specificare la conservazione predefinita per ogni bucket o le impostazioni di conservazione per ogni versione dell'oggetto.

Come abilitare S3 Object Lock per un bucket

Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID , è possibile abilitare facoltativamente S3 Object Lock quando si crea ogni bucket.

S3 Object Lock è un'impostazione permanente che può essere abilitata solo quando si crea un bucket. Non è possibile aggiungere o disabilitare S3 Object Lock dopo aver creato un bucket.

Per abilitare S3 Object Lock per un bucket, utilizzare uno dei seguenti metodi:

- Creare il bucket utilizzando Tenant Manager. Vedere "Crea bucket S3" .
- Crea il bucket utilizzando una richiesta CreateBucket con `x-amz-bucket-object-lock-enabled` intestazione della richiesta. Vedere "Operazioni sui bucket" .

S3 Object Lock richiede il controllo delle versioni dei bucket, che viene abilitato automaticamente al momento della creazione del bucket. Non è possibile sospendere il controllo delle versioni per il bucket. Vedere "Versionamento degli oggetti" .

Impostazioni di conservazione predefinite per un bucket

Quando S3 Object Lock è abilitato per un bucket, è possibile abilitare facoltativamente la conservazione predefinita per il bucket e specificare una modalità di conservazione predefinita e un periodo di conservazione predefinito.

Modalità di conservazione predefinita

- In modalità CONFORMITÀ:
  - L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.
  - La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.
  - La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità GOVERNANCE:
  - Utenti con il `s3:BypassGovernanceRetention` il permesso può utilizzare il `x-amz-bypass-governance-retention: true` intestazione della richiesta per ignorare le impostazioni di conservazione.
  - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.
  - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

Periodo di conservazione predefinito

Ogni bucket può avere un periodo di conservazione predefinito specificato in anni o giorni.

Come impostare la conservazione predefinita per un bucket

Per impostare la conservazione predefinita per un bucket, utilizzare uno dei seguenti metodi:

- Gestisci le impostazioni del bucket da Tenant Manager. Vedere"Crea un bucket S3" E"Aggiorna la conservazione predefinita del blocco degli oggetti S3" .
- Inviare una richiesta PutObjectLockConfiguration al bucket per specificare la modalità predefinita e il numero predefinito di giorni o anni.

PutObjectLockConfiguration

La richiesta PutObjectLockConfiguration consente di impostare e modificare la modalità di conservazione predefinita e il periodo di conservazione predefinito per un bucket in cui è abilitato S3 Object Lock. È anche possibile rimuovere le impostazioni di conservazione predefinite configurate in precedenza.

Quando nuove versioni di oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` E `x-amz-object-lock-retain-until-date` non sono specificati. Il periodo di conservazione predefinito viene utilizzato per calcolare la data di conservazione fino a se `x-amz-object-lock-retain-until-date` non è specificato.

Se il periodo di conservazione predefinito viene modificato dopo l'acquisizione di una versione dell'oggetto, la data di conservazione fino alla versione dell'oggetto rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.

Devi avere il `s3:PutBucketObjectLockConfiguration` autorizzazione, oppure essere l'account root, per completare questa operazione.

IL `Content-MD5` l'intestazione della richiesta deve essere specificata nella richiesta PUT.

Richiedi esempio

Questo esempio abilita S3 Object Lock per un bucket e imposta la modalità di conservazione predefinita su CONFORMITÀ e il periodo di conservazione predefinito su 6 anni.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Come determinare la conservazione predefinita per un bucket

Per determinare se S3 Object Lock è abilitato per un bucket e per visualizzare la modalità di conservazione predefinita e il periodo di conservazione, utilizzare uno di questi metodi:

- Visualizza il bucket in Tenant Manager. Vedere "Visualizza i bucket S3" .
- Inviare una richiesta GetObjectLockConfiguration.

Ottieni configurazione blocco oggetto

La richiesta GetObjectLockConfiguration consente di determinare se S3 Object Lock è abilitato per un bucket e, in tal caso, di verificare se sono configurati una modalità di conservazione predefinita e un periodo di conservazione per il bucket.

Quando nuove versioni di oggetti vengono acquisite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` non è specificato. Il periodo di conservazione predefinito viene utilizzato per calcolare la data di conservazione fino a se `x-amz-object-lock-retain-until-date` non è specificato.

Devi avere il `s3:GetBucketObjectLockConfiguration` autorizzazione, oppure essere l'account root, per completare questa operazione.

Richiedi esempio

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Esempio di risposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Come specificare le impostazioni di conservazione per un oggetto

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza impostazioni di conservazione S3 Object Lock.

Le impostazioni di conservazione a livello di oggetto vengono specificate tramite l'API REST S3. Le impostazioni di conservazione per un oggetto sostituiscono tutte le impostazioni di conservazione predefinite per il bucket.

Per ogni oggetto è possibile specificare le seguenti impostazioni:

- **Modalità di conservazione**: CONFORMITÀ o GOVERNANCE.
- **Retain-until-date**: data che specifica per quanto tempo la versione dell'oggetto deve essere conservata da

StorageGRID.

  - In modalità CONFORMITÀ, se la data di conservazione è futura, l'oggetto può essere recuperato, ma non può essere modificato o eliminato. La data di conservazione può essere aumentata, ma questa data non può essere diminuita o rimossa.
  - In modalità GOVERNANCE, gli utenti con autorizzazione speciale possono ignorare l'impostazione di conservazione fino alla data indicata. Possono eliminare una versione di un oggetto prima che scada il periodo di conservazione. Possono anche aumentare, diminuire o addirittura rimuovere la data di conservazione.

- **Sospensione legale**: l'applicazione di una sospensione legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di scadenza, ma rimane in vigore finché non viene rimossa esplicitamente.

  L'impostazione di conservazione legale per un oggetto è indipendente dalla modalità di conservazione e dalla data di conservazione fino alla data di scadenza. Se una versione di un oggetto è sottoposta a blocco legale, nessuno può eliminarla.

Per specificare le impostazioni di blocco degli oggetti S3 quando si aggiunge una versione dell'oggetto a un bucket, emettere un"MettiOggetto" ,"CopiaOggetto" , O"CreaCaricamentoMultiparte" richiesta.

Puoi usare quanto segue:

- `x-amz-object-lock-mode`, che può essere COMPLIANCE o GOVERNANCE (con distinzione tra maiuscole e minuscole).

  > Se specifichi `x-amz-object-lock-mode` , devi anche specificare `x-amz-object-lock-retain-until-date` .

- `x-amz-object-lock-retain-until-date`
  - Il valore retain-til-date deve essere nel formato `2020-08-10T21:46:00Z` . Sono consentite frazioni di secondo, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Altri formati ISO 8601 non sono consentiti.
  - La data di conservazione deve essere futura.
- `x-amz-object-lock-legal-hold`

  Se la conservazione legale è ATTIVA (sensibile alle maiuscole e alle minuscole), l'oggetto viene sottoposto a conservazione legale. Se la conservazione legale è disattivata, non verrà applicata alcuna conservazione legale. 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 PutObject. `Content-MD5` non è richiesto per CopyObject o CreateMultipartUpload.
- Se il bucket non ha S3 Object Lock abilitato e un `x-amz-object-lock-*` Se è presente l'intestazione della richiesta, viene restituito un errore 400 Bad Request (InvalidRequest).
- La richiesta PutObject supporta l'uso di `x-amz-storage-class: REDUCED_REDUNDANCY` per adattarsi al comportamento di AWS. Tuttavia, quando un oggetto viene inserito in un bucket con S3 Object Lock abilitato, StorageGRID eseguirà sempre un inserimento a doppio commit.

- Una successiva risposta alla versione GET o HeadObject includerà le intestazioni `x-amz-object-lock-mode` , `x-amz-object-lock-retain-until-date` , E `x-amz-object-lock-legal-hold` , se configurato e se il mittente della richiesta ha il corretto `s3:Get*` permessi.

Puoi usare il `s3:object-lock-remaining-retention-days` chiave di condizione della policy per limitare i periodi di conservazione minimi e massimi consentiti per i tuoi oggetti.

Come aggiornare le impostazioni di conservazione per un oggetto

Se è necessario aggiornare le impostazioni di conservazione o di blocco legale per una versione esistente di un oggetto, è possibile eseguire le seguenti operazioni sulle sottorisorse dell'oggetto:

- `PutObjectLegalHold`

  Se il nuovo valore di conservazione legale è impostato su ON, l'oggetto viene sottoposto a conservazione legale. Se il valore di sospensione legale è OFF, la sospensione legale viene revocata.

- `PutObjectRetention`
  - Il valore della modalità può essere COMPLIANCE o GOVERNANCE (con distinzione tra maiuscole e minuscole).
  - Il valore retain-til-date deve essere nel formato `2020-08-10T21:46:00Z` . Sono consentite frazioni di secondo, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Altri formati ISO 8601 non sono consentiti.
  - Se una versione di un oggetto ha una data di conservazione (retain-til-date) esistente, è possibile solo aumentarla. Il nuovo valore deve essere nel futuro.

Come utilizzare la modalità GOVERNANCE

Gli utenti che hanno il `s3:BypassGovernanceRetention` l'autorizzazione può ignorare le impostazioni di conservazione attive di un oggetto che utilizza la modalità GOVERNANCE. Tutte le operazioni DELETE o PutObjectRetention devono includere `x-amz-bypass-governance-retention:true` intestazione della richiesta. Questi utenti possono eseguire le seguenti operazioni aggiuntive:

- Eseguire le operazioni DeleteObject o DeleteObjects per eliminare una versione dell'oggetto prima che scada il periodo di conservazione.

  Gli oggetti sottoposti a conservazione legale non possono essere eliminati. La conservazione legale deve essere DISATTIVATA.

- Eseguire operazioni PutObjectRetention che modificano la modalità di una versione dell'oggetto da GOVERNANCE a COMPLIANCE prima che sia trascorso il periodo di conservazione dell'oggetto.

  Non è mai consentito cambiare la modalità da COMPLIANCE a GOVERNANCE.

- Eseguire operazioni PutObjectRetention per aumentare, diminuire o rimuovere il periodo di conservazione di una versione dell'oggetto.

Informazioni correlate

- "Gestisci gli oggetti con S3 Object Lock"
- "Utilizzare S3 Object Lock per conservare gli oggetti"
- "Guida per l'utente di Amazon Simple Storage Service: blocco degli oggetti"

Crea la configurazione del ciclo di vita S3

È possibile creare una configurazione del ciclo di vita S3 per controllare quando oggetti specifici vengono eliminati dal sistema StorageGRID .

Il semplice esempio in questa sezione illustra come una configurazione del ciclo di vita S3 può controllare quando determinati oggetti vengono eliminati (scadono) da specifici bucket S3. L'esempio in questa sezione è solo a scopo illustrativo. Per i dettagli completi sulla creazione di configurazioni del ciclo di vita S3, vedere "Guida per l'utente di Amazon Simple Storage Service: gestione del ciclo di vita degli oggetti" . Si noti che StorageGRID supporta solo azioni di scadenza; non supporta azioni di transizione.

Qual è la configurazione del ciclo di vita?

Una configurazione del ciclo di vita è un insieme di regole applicate agli oggetti in bucket S3 specifici. Ogni regola specifica quali oggetti sono interessati e quando tali oggetti 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: elimina un oggetto quando viene raggiunta una data specificata o quando viene raggiunto un numero di giorni specificato, a partire dal momento in cui l'oggetto è stato acquisito.
- NoncurrentVersionExpiration: elimina un oggetto quando viene raggiunto un numero di giorni specificato, a partire dal momento in cui l'oggetto è diventato non corrente.
- Filtro (Prefisso, Tag)
- Stato
- ID

Ogni oggetto segue le impostazioni di conservazione del ciclo di vita di un bucket S3 o di una policy ILM. Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti che corrispondono al filtro del ciclo di vita del bucket. Gli oggetti che non corrispondono al filtro del ciclo di vita del bucket utilizzano le impostazioni di conservazione del criterio ILM. Se un oggetto corrisponde a un filtro del ciclo di vita del bucket e non vengono specificate esplicitamente azioni di scadenza, le impostazioni di conservazione del criterio ILM non vengono utilizzate e si implica che le versioni dell'oggetto vengano conservate per sempre. Vedere "Esempio di priorità per il ciclo di vita del bucket S3 e la policy ILM" .

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora valide per l'oggetto. Oppure, un oggetto potrebbe essere mantenuto sulla griglia anche dopo che tutte le istruzioni di posizionamento ILM per l'oggetto sono scadute. Per maggiori dettagli, vedere "Come funziona l'ILM durante la vita di un oggetto" .

> La configurazione del ciclo di vita del bucket può essere utilizzata con bucket in cui è abilitato S3 Object Lock, ma la configurazione del ciclo di vita del bucket non è supportata per i bucket Compliant legacy.

StorageGRID supporta l'utilizzo delle seguenti operazioni bucket per gestire le configurazioni del ciclo di vita:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- Configurazione del ciclo di vita di PutBucket

Crea la configurazione del ciclo di vita

Come primo passaggio nella creazione di una configurazione del ciclo di vita, si crea un file JSON che include 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` Il parametro specifica che gli oggetti che corrispondono al filtro scadranno a mezzanotte del 22 agosto 2020.
2. La regola 2 si applica solo agli oggetti che corrispondono al prefisso `category2` /. IL `Expiration` Il parametro specifica che gli oggetti che corrispondono al filtro scadranno 100 giorni dopo essere stati acquisiti.

   > Le regole che specificano un numero di giorni sono relative al momento in cui l'oggetto è stato ingerito. 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` Il parametro specifica che tutte le versioni non correnti degli oggetti corrispondenti scadranno 50 giorni dopo essere diventate non correnti.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Applica la configurazione del ciclo di vita al bucket

Dopo aver creato il file di configurazione del ciclo di vita, puoi applicarlo a un bucket inviando una richiesta PutBucketLifecycleConfiguration.

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

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Per convalidare che una configurazione del ciclo di vita sia stata applicata correttamente al bucket, inviare una richiesta GetBucketLifecycleConfiguration. Per esempio:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Una risposta positiva elenca la configurazione del ciclo di vita appena applicata.

Convalida che la scadenza del ciclo di vita del bucket si applichi all'oggetto

È possibile determinare se una regola di scadenza nella configurazione del ciclo di vita si applica a un oggetto specifico quando si invia una richiesta PutObject, HeadObject o GetObject. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando scade l'oggetto e quale regola di scadenza è stata rispettata.

> Poiché il ciclo di vita del bucket sostituisce ILM, `expiry-date` viene mostrata la data effettiva in cui l'oggetto verrà eliminato. Per maggiori dettagli, vedere "Come viene determinata la ritenzione dell'oggetto" .

Ad esempio, questa richiesta PutObject è stata emessa il 22 giugno 2020 e inserisce un oggetto nel `testbucket` secchio.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La risposta di successo indica che l'oggetto scadrà tra 100 giorni (01 ottobre 2020) e che corrisponde alla Regola 2 della configurazione del ciclo di vita.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Ad esempio, questa richiesta HeadObject è stata utilizzata per ottenere metadati per lo stesso oggetto nel bucket testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La risposta di successo include i metadati dell'oggetto e indica che l'oggetto scadrà tra 100 giorni e che soddisfa la Regola 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Per i bucket abilitati al controllo delle versioni, `x-amz-expiration` l'intestazione di risposta si applica solo alle versioni correnti degli oggetti.

Raccomandazioni per l'implementazione dell'API REST S3

Quando si implementa l'API REST S3 per l'uso con StorageGRID, è necessario seguire queste raccomandazioni.

Raccomandazioni per HEAD su oggetti inesistenti

Se la tua applicazione controlla regolarmente se un oggetto esiste in un percorso in cui non ti aspetti che l'oggetto esista effettivamente, dovresti usare "Disponibile""coerenza" . Ad esempio, dovresti usare la coerenza "Disponibile" se la tua applicazione esegue l'HEAD di una posizione prima di eseguirvi un PUT.

In caso contrario, se l'operazione HEAD non trova l'oggetto, è possibile che venga visualizzato un numero elevato di errori 500 Internal Server se due o più nodi di archiviazione nello stesso sito non sono disponibili o un sito remoto non è raggiungibile.

È possibile impostare la coerenza "Disponibile" per ogni bucket utilizzando"PUT Consistenza del secchio" richiesta oppure è possibile specificare la coerenza nell'intestazione della richiesta per una singola operazione

API.

Raccomandazioni per le chiavi degli oggetti

Seguire questi consigli per i nomi delle chiavi degli oggetti, in base al momento in cui il bucket è stato creato per la prima volta.

Bucket creati in StorageGRID 11.4 o versioni precedenti

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi degli oggetti. Ciò è in contrasto con la precedente raccomandazione di AWS per i prefissi delle chiavi. Utilizzare invece prefissi non casuali e non univoci, come ad esempio `image` .
- Se si segue la precedente raccomandazione di AWS di utilizzare caratteri casuali e univoci nei prefissi delle chiavi, aggiungere un nome di directory come prefisso alle chiavi degli oggetti. Cioè, usa questo formato:

  `mybucket/mydir/f8e3-image3132.jpg`

  Invece di questo formato:

  `mybucket/f8e3-image3132.jpg`

Bucket creati in StorageGRID 11.4 o versioni successive

Non è necessario limitare i nomi delle chiavi degli oggetti per soddisfare le migliori pratiche in termini di prestazioni. Nella maggior parte dei casi, è possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi degli oggetti.

> Un'eccezione è il carico di lavoro S3 che rimuove continuamente tutti gli oggetti dopo un breve periodo di tempo. Per ridurre al minimo l'impatto sulle prestazioni in questo caso d'uso, modificare una parte iniziale del nome della chiave ogni diverse migliaia di oggetti con qualcosa come la data. Ad esempio, supponiamo che un client S3 scriva in genere 2.000 oggetti al secondo e che la policy ILM o del ciclo di vita del bucket rimuova tutti gli oggetti dopo tre giorni. Per ridurre al minimo l'impatto sulle prestazioni, potresti denominare le chiavi utilizzando uno schema come questo: `/mybucket/mydir/`*`yyyymmddhhmmss-random_UUID`*`.jpg`

Consigli per le "letture di intervallo"

Se il"opzione globale per comprimere gli oggetti memorizzati" è abilitato, le applicazioni client S3 dovrebbero evitare di eseguire operazioni GetObject che specificano un intervallo di byte da restituire. Queste operazioni di "lettura di intervallo" sono inefficienti perché StorageGRID deve effettivamente decomprimere gli oggetti per accedere ai byte richiesti. Le operazioni GetObject che richiedono un intervallo ridotto di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, non è efficiente 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 potrebbero scadere.

> Se è necessario comprimere oggetti e l'applicazione client deve utilizzare letture di intervallo, aumentare il timeout di lettura per l'applicazione.

Supporto per l'API REST di Amazon S3

Dettagli di implementazione dell'API REST S3

Il sistema StorageGRID implementa l'API Simple Storage Service (versione API 2006-03-01) con supporto per la maggior parte delle operazioni e con alcune limitazioni. Quando si integrano applicazioni client S3 REST API, è necessario comprendere i dettagli di implementazione.

Il sistema StorageGRID supporta sia le richieste in stile host virtuale sia quelle in stile percorso.

Gestione delle date

L'implementazione StorageGRID dell'API REST S3 supporta solo formati di data HTTP validi.

Il sistema StorageGRID supporta solo formati di data HTTP validi per tutte le intestazioni che accettano valori di data. La parte oraria della data può essere specificata nel formato Greenwich Mean Time (GMT) o nel formato Universal Coordinated Time (UTC) senza differenza di fuso orario (è necessario specificare +0000). Se includi il `x-amz-date` nell'intestazione della richiesta, sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza AWS Signature versione 4, `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 le intestazioni di richiesta comuni definite da "Riferimento API di Amazon Simple Storage Service: intestazioni di richiesta comuni" , con una eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per AWS Signature versione 2 Supporto per AWS Signature versione 4, con le seguenti eccezioni: • Quando si fornisce il valore effettivo del checksum del payload in `x-amz-content-sha256` , il valore viene accettato senza convalida, come se il valore `UNSIGNED-PAYLOAD` era stato fornito per l'intestazione. Quando fornisci un `x-amz-content-sha256` valore dell'intestazione che implica `aws-chunked` streaming (ad esempio, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), le firme dei blocchi non vengono verificate rispetto ai dati dei blocchi.
token di sicurezza x-amz	Non implementato. Resi `XNotImplemented` .

Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite da *Simple Storage Service API Reference*, con un'eccezione.

Intestazione di risposta	Implementazione
x-amz-id-2	Non utilizzato

Autenticare le richieste

Il sistema StorageGRID supporta sia l'accesso autenticato che quello anonimo agli oggetti tramite l'API S3.

L'API S3 supporta la versione 2 e la versione 4 della firma 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 utilizzando parametri di query.

Utilizzare l'intestazione di autorizzazione HTTP

L'HTTP `Authorization` L'intestazione viene utilizzata da tutte le operazioni API S3, ad eccezione delle richieste anonime, ove consentito dalla policy del bucket. IL `Authorization` L'intestazione contiene tutte le informazioni di firma necessarie per autenticare una richiesta.

Utilizzare i parametri di query

È possibile utilizzare i parametri di query per aggiungere informazioni di autenticazione a un URL. Questa operazione è nota come prefirma dell'URL e può essere utilizzata per concedere l'accesso temporaneo a risorse specifiche. Gli utenti con l'URL prefirmato non hanno bisogno di conoscere la chiave di accesso segreta per accedere alla risorsa, il che consente di fornire a terze parti un accesso limitato a una risorsa.

Operazioni sul servizio

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
ListBuckets (precedentemente denominato Servizio GET)	Implementato con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
Utilizzo dello spazio di archiviazione GET	StorageGRID"Utilizzo dello spazio di archiviazione GET" La richiesta indica la quantità totale di spazio di archiviazione utilizzato da un account e per ogni bucket associato all'account. Questa è un'operazione sul servizio con un percorso di / e un parametro di query personalizzato(`?x-ntap-sg-usage`) aggiunto.
OPZIONI /	Le applicazioni client possono emettere `OPTIONS /` richieste alla porta S3 su un nodo di archiviazione, senza fornire credenziali di autenticazione S3, per determinare se il nodo di archiviazione è disponibile. È possibile utilizzare questa richiesta per il monitoraggio o per consentire ai bilanciatori di carico esterni di identificare quando un nodo di archiviazione è inattivo.

Operazioni sui bucket

Il sistema StorageGRID supporta un massimo di 5.000 bucket per ogni account tenant S3.

Ogni griglia può avere un massimo di 100.000 bucket.

Per supportare 5.000 bucket, ogni nodo di archiviazione nella griglia deve disporre di almeno 64 GB di RAM.

Le restrizioni sui nomi dei bucket seguono le restrizioni della regione AWS US Standard, ma è opportuno limitarle ulteriormente alle convenzioni di denominazione DNS per supportare le richieste in stile hosting virtuale S3.

Per maggiori informazioni vedere quanto segue:

- "Guida per l'utente di Amazon Simple Storage Service: quote, restrizioni e limitazioni dei bucket"
- "Configurare i nomi di dominio degli endpoint S3"

Le operazioni ListObjects (GET Bucket) e ListObjectVersions (GET Bucket object versions) supportano StorageGRID"valori di coerenza" .

È possibile verificare se gli aggiornamenti all'orario dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket. Vedere "GET Ora dell'ultimo accesso al bucket" .

La tabella seguente descrive come StorageGRID implementa le operazioni del bucket S3 REST API. Per eseguire una qualsiasi di queste operazioni, è necessario fornire le credenziali di accesso necessarie per l'account.

Operazione	Implementazione
CreaBucket	Crea un nuovo bucket. Creando il bucket, ne diventi il proprietario. • I nomi dei bucket devono rispettare le seguenti regole: ◦ Deve essere univoco 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 contenere solo lettere minuscole, numeri e trattini. ◦ Non deve avere l'aspetto di un indirizzo IP formattato come testo. ◦ Non utilizzare punti nelle richieste in stile ospitato virtuale. I punti causeranno problemi con la verifica dei certificati jolly del server. • Per impostazione predefinita, i bucket vengono creati in `us-east-1` regione; tuttavia, è possibile utilizzare il `LocationConstraint` elemento di richiesta nel corpo della richiesta per specificare una regione diversa. Quando si utilizza il `LocationConstraint` elemento, è necessario specificare il nome esatto di una regione definita tramite Grid Manager o Grid Management API. Se non conosci il nome della regione da utilizzare, contatta l'amministratore di sistema. **Nota**: si verificherà un errore se la richiesta CreateBucket utilizza una regione non definita in StorageGRID. • Puoi includere il `x-amz-bucket-object-lock-enabled` intestazione della richiesta per creare un bucket con S3 Object Lock abilitato. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" . Quando si crea il bucket, è necessario abilitare S3 Object Lock. Non è possibile aggiungere o disabilitare S3 Object Lock dopo aver creato un bucket. S3 Object Lock richiede il controllo delle versioni dei bucket, che viene abilitato automaticamente quando si crea il bucket.
EliminaBucket	Elimina il bucket.
DeleteBucketCors	Elimina la configurazione CORS per il bucket.
DeleteBucketEncryption	Elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma tutti i nuovi oggetti aggiunti al bucket non vengono crittografati.
DeleteBucketLifecycle	Elimina la configurazione del ciclo di vita dal bucket. Vedere "Crea la configurazione del ciclo di vita S3" .
DeleteBucketPolicy	Elimina la policy associata al bucket.

Operazione	Implementazione
DeleteBucketReplication	Elimina la configurazione di replica associata al bucket.
DeleteBucketTagging	Utilizza il `tagging` sottorisorsa per rimuovere tutti i tag da un bucket. **Attenzione**: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è assegnato un valore. Non inviare una richiesta DeleteBucketTagging se è presente un `NTAP-SG-ILM-BUCKET-TAG` etichetta del secchio. Invece, emetti una richiesta PutBucketTagging con solo `NTAP-SG-ILM-BUCKET-TAG` tag e il valore assegnato per rimuovere tutti gli altri tag dal bucket. Non modificare o rimuovere il `NTAP-SG-ILM-BUCKET-TAG` etichetta del secchio.
OttieniBucketAcl	Restituisce una risposta positiva e l'ID, il DisplayName e l'autorizzazione del proprietario del bucket, a indicare che il proprietario ha accesso completo al bucket.
GetBucketCors	Restituisce il `cors` configurazione per il bucket.
Ottieni crittografia dei bucket	Restituisce la configurazione di crittografia predefinita per il bucket.
GetBucketLifecycleConfiguration (in precedenza denominato ciclo di vita del bucket GET)	Restituisce la configurazione del ciclo di vita per il bucket. Vedere "Crea la configurazione del ciclo di vita S3" .
OttieniPosizioneBucket	Restituisce la regione impostata utilizzando `LocationConstraint` elemento nella richiesta CreateBucket. Se la regione del bucket è `us-east-1` , viene restituita una stringa vuota per la regione.
Configurazione di notifica di GetBucket (in precedenza denominata notifica GET Bucket)	Restituisce la configurazione delle notifiche allegata al bucket.
OttieniPoliticaBucket	Restituisce la policy associata al bucket.
OttieniReplicazioneBucket	Restituisce la configurazione di replica associata al bucket.

Operazione	Implementazione
OttieniBucketTagging	Utilizza il `tagging` sottorisorsa per restituire tutti i tag per un bucket. **Attenzione**: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è assegnato un valore. Non modificare o rimuovere questo tag.
GetBucketVersioning	Questa implementazione utilizza il `versioning` sottorisorsa per restituire lo stato di controllo delle versioni di un bucket. • *blank*: il controllo delle versioni non è mai stato abilitato (il bucket è "Senza controllo delle versioni") • Abilitato: il controllo delle versioni è abilitato • Sospeso: il controllo delle versioni era precedentemente abilitato ed è sospeso
Ottieni configurazione blocco oggetto	Restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurati. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" .
HeadBucket	Determina se esiste un bucket e se si dispone dell'autorizzazione per accedervi. Questa operazione restituisce: • `x-ntap-sg-bucket-id`: L'UUID del bucket nel formato UUID. • `x-ntap-sg-trace-id`: ID traccia univoco della richiesta associata.
ListObjects e ListObjectsV2 (precedentemente denominato GET Bucket)	Restituisce alcuni o tutti (fino a 1.000) gli oggetti in un bucket. La classe di archiviazione per gli oggetti può avere uno dei due valori, anche se l'oggetto è stato ingerito con `REDUCED_REDUNDANCY` opzione classe di archiviazione: • `STANDARD`, che indica che l'oggetto è archiviato in un pool di archiviazione costituito da nodi di archiviazione. • `GLACIER`, che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool. Se il bucket contiene un numero elevato di chiavi eliminate che hanno lo stesso prefisso, la risposta potrebbe includere alcune `CommonPrefixes` che non contengono chiavi.
ListObjectVersions (precedentemente denominate versioni GET Bucket Object)	Con accesso READ su un bucket, utilizzando questa operazione con `versions` La sottorisorsa elenca i metadati di tutte le versioni degli oggetti nel bucket.

Operazione	Implementazione
PutBucketCors	Imposta la configurazione CORS per un bucket in modo che il bucket possa gestire richieste multiorigine. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni web client in un dominio di accedere alle risorse in un dominio diverso. Ad esempio, supponiamo di utilizzare un bucket S3 denominato `images` per memorizzare la grafica. Impostando la configurazione CORS per `images` bucket, puoi consentire che le immagini in quel bucket vengano visualizzate sul sito web `http://www.example.com` .
PutBucketEncryption	Imposta lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è abilitata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati. StorageGRID supporta la crittografia lato server con chiavi gestite StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare `SSEAlgorithm` parametro a `AES256` e non usare il `KMSMasterKeyID` parametro. La configurazione di crittografia predefinita del bucket viene ignorata se la richiesta di caricamento dell'oggetto specifica già la crittografia (ovvero, se la richiesta include `x-amz-server-side-encryption-*` intestazione della richiesta).
Configurazione del ciclo di vita di PutBucket (in precedenza denominato ciclo di vita del bucket PUT)	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: • Scadenza (Giorni, Data, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtro (Prefisso, Tag) • Stato • ID StorageGRID non supporta queste azioni: • AnnullaIncompletoCaricamento multiparte • Transizione Vedere "Crea la configurazione del ciclo di vita S3" . Per comprendere come l'azione di scadenza nel ciclo di vita di un bucket interagisce con le istruzioni di posizionamento ILM, vedere"Come funziona l'ILM durante la vita di un oggetto" . **Nota**: la configurazione del ciclo di vita del bucket può essere utilizzata con bucket in cui è abilitato S3 Object Lock, ma la configurazione del ciclo di vita del bucket non è supportata per i bucket Compliant legacy.

Operazione	Implementazione

Configurazione della notifica PutBucket
 	
(in precedenza denominata notifica PUT Bucket)
	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:
	
	• StorageGRID supporta come destinazioni gli argomenti Amazon Simple Notification Service (Amazon SNS) o Kafka. Gli endpoint Simple Queue Service (SQS) o Amazon Lambda non sono supportati.
	• La destinazione delle notifiche deve essere specificata come URN di un endpoint StorageGRID . Gli endpoint possono essere creati utilizzando Tenant Manager o Tenant Management API.
	
	Affinché la configurazione della notifica abbia esito positivo, è necessario che l'endpoint esista. Se l'endpoint non esiste, un `400 Bad Request` l'errore viene restituito con il codice `InvalidArgument` .
	
	• Non è possibile configurare una notifica per i seguenti tipi di eventi. Questi tipi di eventi **non** sono supportati.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, con la differenza che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente:
	◦ **fonteevento**
	
	`sgws:s3`
	
	◦ **awsRegion**
	
	non incluso
	
	◦ **x-amz-id-2**
	
	non incluso
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Imposta la policy associata al bucket. Vedere "Utilizzare criteri di accesso a bucket e gruppi" .

Operazione	Implementazione
PutBucketReplication	Configura"Replica StorageGRID CloudMirror" per il bucket utilizzando l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica CloudMirror, è necessario conoscere i seguenti dettagli di implementazione: • StorageGRID supporta solo la versione 1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'uso di `Filter` elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per i dettagli, vedere "Guida per l'utente di Amazon Simple Storage Service: configurazione della replica" . • La replica dei bucket può essere configurata su bucket con o senza versione. • È possibile specificare un bucket di destinazione diverso in ogni regola del file XML di configurazione della replica. Un bucket di origine può replicarsi su più di un bucket di destinazione. • I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID come specificato in Tenant Manager o nell'API Tenant Management. Vedere "Configurare la replica di CloudMirror" . Affinché la configurazione della replica abbia esito positivo, è necessario che l'endpoint esista. Se l'endpoint non esiste, la richiesta fallisce come `400 Bad Request` Il messaggio di errore afferma: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Non è necessario specificare un `Role` nell'XML di configurazione. Questo valore non viene utilizzato da StorageGRID e verrà ignorato se inviato. • Se si omette la classe di archiviazione dall'XML di configurazione, StorageGRID utilizza `STANDARD` classe di archiviazione predefinita. • Se si elimina un oggetto dal bucket di origine o si elimina il bucket di origine stesso, il comportamento della replica tra regioni è il seguente: ◦ Se elimini l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non verrà replicato e non riceverai alcuna notifica. ◦ Se si elimina l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento di eliminazione standard di Amazon S3 per la V1 della replica tra regioni.

Operazione	Implementazione
PutBucketTagging	Utilizza il `tagging` sottorisorsa per aggiungere o aggiornare un set di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni: • Sia StorageGRID che Amazon S3 supportano fino a 50 tag per ogni bucket. • I tag associati a un bucket devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode. • I valori dei tag possono avere una lunghezza massima di 256 caratteri Unicode. • Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole. **Attenzione**: se per questo bucket è impostato un tag di policy ILM non predefinito, si verificherà un `NTAP-SG-ILM-BUCKET-TAG` tag bucket a cui è assegnato un valore. Assicuratevi che il `NTAP-SG-ILM-BUCKET-TAG` Il tag bucket è incluso con il valore assegnato in tutte le richieste PutBucketTagging. Non modificare o rimuovere questo tag. **Nota**: questa operazione sovrascriverà tutti i tag correnti già presenti nel bucket. Se vengono omessi tag esistenti dal set, tali tag verranno rimossi dal bucket.
PutBucketVersioning	Utilizza il `versioning` sottorisorsa per impostare lo stato di controllo delle versioni di un bucket esistente. È possibile impostare lo stato di controllo delle versioni con uno dei seguenti valori: • Abilitato: abilita il controllo delle versioni per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID versione univoco. • Sospeso: disattiva il controllo delle versioni per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione `null` .
PutObjectLockConfiguration	Configura o rimuove la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito. Se il periodo di conservazione predefinito viene modificato, la data di conservazione fino alle versioni esistenti degli oggetti rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito. Vedere"Utilizzare l'API REST S3 per configurare S3 Object Lock" per informazioni dettagliate.

Operazioni sugli oggetti

Operazioni sugli oggetti

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

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

- StorageGRID"valori di coerenza" sono supportati da tutte le operazioni sugli oggetti, ad eccezione delle

seguenti:

  - OttieniOggettoAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelezionaOggettoContenuto

- Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata 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, compresi gli oggetti creati da un utente anonimo o da un altro account.
- Gli oggetti dati acquisiti nel sistema StorageGRID tramite Swift non sono accessibili tramite S3.

La tabella seguente descrive come StorageGRID implementa le operazioni degli oggetti S3 REST API.

Operazione	Implementazione
EliminaOggetto	Autenticazione a più fattori (MFA) e intestazione di risposta `x-amz-mfa` non sono supportati. Durante l'elaborazione di una richiesta DeleteObject, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni archiviate. In caso di esito positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e quindi segnala l'esito positivo al client. **Controllo delle versioni** Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare `versionId` sottorisorsa. L'utilizzo di questa sottorisorsa elimina definitivamente la versione. Se il `versionId` corrisponde a un marcatore di eliminazione, l'intestazione della risposta `x-amz-delete-marker` viene restituito impostato su `true` . • Se un oggetto viene eliminato senza `versionId` sottorisorsa su un bucket con controllo delle versioni abilitato, si traduce nella generazione di un marcatore di eliminazione. IL `versionId` per il marcatore di eliminazione viene restituito utilizzando il `x-amz-version-id` intestazione di risposta e `x-amz-delete-marker` l'intestazione di risposta viene restituita impostata su `true` . • Se un oggetto viene eliminato senza `versionId` sottorisorsa su un bucket con controllo delle versioni sospeso, si traduce nell'eliminazione permanente di una versione 'null' già esistente o di un marcatore di eliminazione 'null' e nella generazione di un nuovo marcatore di eliminazione 'null'. IL `x-amz-delete-marker` l'intestazione di risposta viene restituita impostata su `true` . **Nota**: in alcuni casi, potrebbero esistere più marcatori di eliminazione per un oggetto. Vedere"Utilizzare l'API REST S3 per configurare S3 Object Lock" per scoprire come eliminare le versioni degli oggetti in modalità GOVERNANCE.
EliminaOggetti (in precedenza denominato DELETE Multiple Objects)	Autenticazione a più fattori (MFA) e intestazione di risposta `x-amz-mfa` non sono supportati. È possibile eliminare più oggetti nello stesso messaggio di richiesta. Vedere"Utilizzare l'API REST S3 per configurare S3 Object Lock" per scoprire come eliminare le versioni degli oggetti in modalità GOVERNANCE.

Operazione	Implementazione
DeleteObjectTagging	Utilizza il `tagging` sottorisorsa per rimuovere tutti i tag da un oggetto. **Controllo delle versioni** Se il `versionId` Se il parametro di 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 marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con `x-amz-delete-marker` intestazione di risposta impostata su `true` .
OttieniOggetto	"OttieniOggetto"
OttieniOggettoAcl	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, a indicare che il proprietario ha accesso completo all'oggetto.
OttieniOggettoLegaleHold	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
Ottieni conservazione oggetto	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
OttieniTaggingOggetto	Utilizza il `tagging` sottorisorsa per restituire tutti i tag per un oggetto. **Controllo delle versioni** Se il `versionId` Se il parametro query non è specificato nella richiesta, l'operazione restituisce tutti i tag dalla versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con `x-amz-delete-marker` intestazione di risposta impostata su `true` .
HeadObject	"HeadObject"
Ripristina oggetto	"Ripristina oggetto"
MettiOggetto	"MettiOggetto"
CopiaOggetto (in precedenza denominato PUT Object - Copy)	"CopiaOggetto"
PutObjectLegalHold	"Utilizzare l'API REST S3 per configurare S3 Object Lock"
PutObjectRetention	"Utilizzare l'API REST S3 per configurare S3 Object Lock"

Operazione	Implementazione
PutObjectTagging	Utilizza il `tagging` sottorisorsa per aggiungere un set di tag a un oggetto esistente. **Limiti dei tag degli oggetti** Puoi aggiungere tag ai nuovi oggetti quando li carichi oppure puoi aggiungerli agli oggetti esistenti. Sia StorageGRID che Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode e i valori tag possono avere una lunghezza massima di 256 caratteri Unicode. Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole. **Aggiornamenti dei tag e comportamento di acquisizione** Quando si utilizza PutObjectTagging per aggiornare i tag di un oggetto, StorageGRID non reingestisce l'oggetto. Ciò significa che l'opzione per il comportamento di acquisizione specificata nella regola ILM corrispondente non viene utilizzata. Tutte le modifiche al posizionamento degli oggetti 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 Rigorosa per il comportamento di acquisizione, non viene intrapresa alcuna azione se non è possibile effettuare i posizionamenti degli oggetti richiesti (ad esempio perché una posizione appena richiesta non è disponibile). L'oggetto aggiornato mantiene la sua posizione attuale finché non sarà possibile il posizionamento richiesto. **Risolvere i conflitti** Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione. **Controllo delle versioni** Se il `versionId` Se 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 marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con `x-amz-delete-marker` intestazione di risposta impostata su `true` .
SelezionaOggettoContenuto	"SelezionaOggettoContenuto"

Utilizzare S3 Select

StorageGRID supporta le seguenti clausole Amazon S3 Select, tipi di dati e operatori per"Comando SelectObjectContent" .

Tutti gli elementi non elencati non sono supportati.

Per la sintassi, vedere"SelezionaOggettoContenuto" . Per ulteriori informazioni su S3 Select, vedere "Documentazione AWS per S3 Select" .

Solo gli account tenant che hanno abilitato S3 Select possono inviare query SelectObjectContent. Vedi il"considerazioni e requisiti per l'utilizzo di S3 Select" .

Clausole

- SELEZIONA elenco
- clausola FROM
- clausola WHERE
- Clausola LIMIT

Tipi di dati

- bool
- intero
- corda
- galleggiante
- decimale, numerico
- marca temporale

Operatori

Operatori logici

- E
- NON
- O

Operatori di confronto

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=
- FRA
- IN

Operatori di corrispondenza di pattern

- COME
- _
- %

Operatori unitari

- È NULLO
- NON È NULLO

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

Funzioni aggregate

- MEDIA()
- CONTARE(*)
- MAX()
- MIN()
- SOMMA()

Funzioni condizionali

- CASO
- COALESCERE
- NULLIF

Funzioni di conversione

- CAST (per i tipi di dati supportati)

Funzioni di data

- DATA_AGGIUNGI
- DATE_DIFF
- ESTRARRE
- A_STRINGA
- TO_TIMESTAMP

- UTCNOW

Funzioni stringa

- LUNGHEZZA_CARATTERE, LUNGHEZZA_CARATTERE
- INFERIORE
- SOTTOSTRINGA
- ORDINARE
- SUPERIORE

Utilizzare la crittografia lato server

La crittografia lato server consente di proteggere i dati degli oggetti quando sono inattivi. StorageGRID crittografa i dati durante la scrittura dell'oggetto e li decrittografa quando si accede all'oggetto.

Se si desidera utilizzare la crittografia lato server, è possibile scegliere una delle due opzioni reciprocamente esclusive, in base al modo in cui vengono gestite le chiavi di crittografia:

- **SSE (crittografia lato server con chiavi gestite StorageGRID)**: quando si invia una richiesta S3 per archiviare 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 decrittografare l'oggetto.
- **SSE-C (crittografia lato server con chiavi fornite dal cliente)**: quando si invia una richiesta S3 per archiviare un oggetto, si fornisce la propria chiave di crittografia. Quando recuperi un oggetto, fornisci la stessa chiave di crittografia come parte della tua 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 decrittografia 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 anche l'oggetto corrispondente.

  > Se un oggetto è crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Utilizzare SSE

Per crittografare un oggetto con una chiave univoca gestita da StorageGRID, utilizzare la seguente intestazione di richiesta:

```
x-amz-server-side-encryption
```

L'intestazione della richiesta SSE è supportata dalle seguenti operazioni sugli oggetti:

- "MettiOggetto"
- "CopiaOggetto"
- "CreaCaricamentoMultiparte"

Utilizzare SSE-C

Per crittografare un oggetto con una chiave univoca gestita da te, puoi utilizzare 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 decrittografare l'oggetto. Il valore della chiave deve essere a 256 bit, codificato in base64.
`x-amz-server-side-encryption-customer-key-MD5`	Specificare il digest MD5 della chiave di crittografia secondo RFC 1321, utilizzato per garantire che la chiave di crittografia sia stata trasmessa senza errori. Il valore per il digest MD5 deve essere codificato in base64 a 128 bit.

Le intestazioni delle richieste SSE-C sono supportate dalle seguenti operazioni sugli oggetti:

- "OttieniOggetto"
- "HeadObject"
- "MettiOggetto"
- "CopiaOggetto"
- "CreaCaricamentoMultiparte"
- "CaricaParte"
- "CaricaParteCopia"

Considerazioni sull'utilizzo della crittografia lato server con chiavi fornite dal cliente (SSE-C)

Prima di utilizzare SSE-C, tenere presente quanto segue:

- Devi usare https.

> StorageGRID rifiuta qualsiasi richiesta effettuata tramite http quando si utilizza SSE-C. Per motivi di sicurezza, è opportuno considerare compromessa qualsiasi chiave inviata accidentalmente tramite http. Scartare la chiave e ruotarla come appropriato.

- L'ETag nella risposta non è l'MD5 dei dati dell'oggetto.
- È necessario gestire la mappatura delle chiavi di crittografia sugli oggetti. StorageGRID non memorizza le chiavi di crittografia. Sei responsabile del monitoraggio della chiave di crittografia fornita per ciascun oggetto.
- Se il bucket è abilitato al controllo delle versioni, ogni versione dell'oggetto dovrebbe avere la propria chiave di crittografia. Sei responsabile del monitoraggio della chiave di crittografia utilizzata per ogni versione dell'oggetto.
- Poiché le chiavi di crittografia vengono gestite sul lato client, è necessario gestire anche eventuali misure di sicurezza 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 anche l'oggetto corrispondente.

- Se per il bucket è configurata la replica tra griglie o la replica CloudMirror, non è possibile acquisire oggetti SSE-C. L'operazione di acquisizione non andrà a buon fine.

Informazioni correlate

"Guida per l'utente di Amazon S3: utilizzo della crittografia lato server con chiavi fornite dal cliente (SSE-C)"

CopiaOggetto

È possibile utilizzare la richiesta S3 CopyObject per creare una copia di un oggetto già archiviato in S3. Un'operazione CopyObject equivale all'esecuzione di GetObject seguito da PutObject.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *consigliata* per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa"caricamento multiparte" Invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).

Se hai eseguito l'aggiornamento da StorageGRID 11.6 o da una versione precedente, verrà attivato l'avviso S3 PUT Object size too large (Dimensioni oggetto troppo grandi) se tenti di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11.7 o 11.8, in questo caso l'avviso non verrà attivato. Tuttavia, per allinearsi allo standard AWS S3, le future versioni di StorageGRID non supporteranno caricamenti di oggetti di dimensioni superiori a 5 GiB.

Caratteri UTF-8 nei metadati utente

Se una richiesta include valori UTF-8 (non sottoposti a escape) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento StorageGRID non è definito.

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 sottoposti a escape vengono trattati come caratteri ASCII:

- Le richieste hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 con escape.
- StorageGRID non restituisce il `x-amz-missing-meta` intestazione se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente
- `x-amz-metadata-directive`: Il valore predefinito è `COPY` , che consente di copiare l'oggetto e i metadati associati.

  Puoi 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.

  Puoi specificare `REPLACE` per sovrascrivere i tag esistenti durante la copia dell'oggetto o per aggiornare i tag.
- Intestazioni delle richieste di blocco degli oggetti S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se viene effettuata una richiesta senza queste intestazioni, vengono utilizzate le impostazioni di conservazione predefinite del bucket per calcolare la modalità di versione dell'oggetto e la data di conservazione fino alla data di scadenza. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" .
- Intestazioni delle richieste 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`

    VedereIntestazioni di richiesta per la crittografia lato server

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Quando si copia un oggetto, se l'oggetto di origine ha un checksum, StorageGRID non copia quel valore di checksum nel nuovo oggetto. Questo comportamento si applica indipendentemente dal fatto che tu provi o meno a utilizzare `x-amz-checksum-algorithm` nella richiesta dell'oggetto.

- `x-amz-website-redirect-location`

Opzioni di classe di archiviazione

IL `x-amz-storage-class` l'intestazione della richiesta è supportata e influisce sul numero di copie dell'oggetto che StorageGRID crea se la regola ILM corrispondente utilizza il commit doppio o bilanciato"opzione di ingestione" .

- `STANDARD`

  (Predefinito) Specifica un'operazione di acquisizione a doppio commit quando la regola ILM utilizza l'opzione Doppio commit o quando l'opzione Bilanciato ricorre alla creazione di copie provvisorie.

- `REDUCED_REDUNDANCY`

  Specifica un'operazione di acquisizione con commit singolo quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ricorre alla creazione di copie provvisorie.

  > Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Utilizzo di x-amz-copy-source in CopyObject

Se il bucket di origine e la chiave, specificati in `x-amz-copy-source` intestazione, sono diversi dal bucket di destinazione e dalla chiave, una copia dei dati dell'oggetto sorgente viene scritta nella destinazione.

Se la sorgente 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 reingerisce l'oggetto. Ciò ha due importanti conseguenze:

- Non è possibile utilizzare CopyObject per crittografare un oggetto esistente sul posto o per modificare la crittografia di un oggetto esistente sul posto. Se fornisci il `x-amz-server-side-encryption`

intestazione o il `x-amz-server-side-encryption-customer-algorithm` intestazione, StorageGRID rifiuta la richiesta e restituisce `XNotImplemented` .

- L'opzione per il comportamento di acquisizione specificata nella regola ILM corrispondente non viene utilizzata. Tutte le modifiche al posizionamento degli oggetti 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 Rigorosa per il comportamento di acquisizione, non viene intrapresa alcuna azione se non è possibile effettuare i posizionamenti degli oggetti richiesti (ad esempio perché una posizione appena richiesta non è disponibile). L'oggetto aggiornato mantiene la sua posizione attuale finché non sarà possibile il posizionamento richiesto.

Intestazioni di richiesta per la crittografia lato server

Se tu"utilizzare la crittografia lato server" , le intestazioni di richiesta fornite dipendono dal fatto che l'oggetto di origine sia crittografato e dal fatto che si intenda crittografare l'oggetto di destinazione.

- Se l'oggetto sorgente è crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta CopyObject, in modo che l'oggetto possa essere decrittografato e quindi copiato:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare `AES256` .
  - `x-amz-copy-source-server-side-encryption-customer-key`: Specifica la chiave di crittografia fornita al momento della creazione dell'oggetto sorgente.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 fornito quando hai creato l'oggetto sorgente.
- Se desideri crittografare l'oggetto di destinazione (la copia) con una chiave univoca che fornisci e gestisci, includi le seguenti tre intestazioni:
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Specificare una nuova chiave di crittografia per l'oggetto di destinazione.
  - `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della nuova chiave di crittografia.

  > Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni per"utilizzando la crittografia lato server" .

- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca gestita da StorageGRID (SSE), includere questa intestazione nella richiesta CopyObject:
  - `x-amz-server-side-encryption`

  > IL `server-side-encryption` il valore dell'oggetto non può essere aggiornato. Invece, fai una copia con un nuovo `server-side-encryption` valore utilizzando `x-amz-metadata-directive` : `REPLACE` .

Controllo delle versioni

Se il bucket di origine è sottoposto a versioning, 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 sottoposto a versioning, la versione generata viene restituita nel `x-amz-version-id` intestazione di risposta. Se il controllo delle versioni è sospeso per il bucket di destinazione, allora `x-amz-version-id` restituisce un valore "null".

OttieniOggetto

È possibile utilizzare la richiesta S3 GetObject per recuperare un oggetto da un bucket S3.

GetObject e oggetti multipart

Puoi usare il `partNumber` parametro di richiesta per recuperare una parte specifica di un oggetto multiparte o segmentato. IL `x-amz-mp-parts-count` l'elemento di risposta indica quante parti ha l'oggetto.

Puoi impostare `partNumber` a 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, il `x-amz-mp-parts-count` l'elemento response viene restituito solo per oggetti segmentati o multiparte.

Caratteri UTF-8 nei metadati utente

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape nei metadati definiti dall'utente. Le richieste GET per un oggetto con caratteri UTF-8 sfuggiti 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 supportata

È supportata la seguente intestazione di richiesta:

- `x-amz-checksum-mode`: Specificare `ENABLED`

  IL `Range` l'intestazione non è supportata con `x-amz-checksum-mode` per GetObject. Quando includi `Range` nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore di checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented` :

- `x-amz-website-redirect-location`

Controllo delle versioni

Se un `versionId` Se la sottorisorsa non è specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "Non trovato" con `x-amz-delete-marker` intestazione di risposta impostata su `true` .

Intestazioni di richiesta 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 da te fornita.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
- `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in"Utilizzare la crittografia lato server" .

Comportamento di GetObject per gli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in un"Pool di archiviazione cloud" , il comportamento di una richiesta GetObject dipende dallo stato dell'oggetto. Vedere"HeadObject" per maggiori dettagli.

> Se un oggetto è archiviato in un Cloud Storage Pool e una o più copie dell'oggetto esistono anche sulla griglia, le richieste GetObject tenteranno di recuperare i dati dalla griglia prima di recuperarli dal Cloud Storage Pool.

Stato dell'oggetto	Comportamento di GetObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto archiviato in un pool di archiviazione tradizionale o mediante codifica di cancellazione	`200 OK` Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	`200 OK` Viene recuperata una copia dell'oggetto.
Oggetto passato a uno stato non recuperabile	`403 Forbidden` , `InvalidObjectState` Utilizzare un"Ripristina oggetto" richiesta di ripristinare l'oggetto a uno stato recuperabile.
Oggetto in fase di ripristino da uno stato non recuperabile	`403 Forbidden` , `InvalidObjectState` Attendi il completamento della richiesta RestoreObject.
Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK` Viene recuperata una copia dell'oggetto.

Oggetti multiparte o segmentati in un pool di archiviazione cloud

Se hai caricato un oggetto multiparte o se StorageGRID ha suddiviso un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel Cloud Storage Pool campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta GetObject potrebbe restituire in modo errato `200 OK` quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

In questi casi:

- La richiesta GetObject potrebbe restituire alcuni dati ma interrompersi a metà del trasferimento.
- Una successiva richiesta GetObject potrebbe restituire `403 Forbidden` .

GetObject e replicazione tra griglie

Se stai usando"federazione di rete" E"replicazione cross-grid" è abilitato per un bucket, il client S3 può verificare lo stato di replicazione di un oggetto emettendo una richiesta GetObject. La risposta include StorageGRID-specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	• **COMPLETO**: La replica è riuscita. • **IN ATTESA**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

> StorageGRID non supporta il `x-amz-replication-status` intestazione.

HeadObject

È possibile utilizzare la richiesta S3 HeadObject per recuperare i metadati da un oggetto senza restituire l'oggetto stesso. Se l'oggetto è archiviato in un Cloud Storage Pool, è possibile utilizzare HeadObject per determinare lo stato di transizione dell'oggetto.

HeadObject e oggetti multiparte

Puoi usare il `partNumber` parametro di richiesta per recuperare i metadati per una parte specifica di un oggetto multiparte o segmentato. IL `x-amz-mp-parts-count` l'elemento di risposta indica quante parti ha l'oggetto.

Puoi impostare `partNumber` a 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, il `x-amz-mp-parts-count` l'elemento response viene restituito solo per oggetti segmentati o multiparte.

Caratteri UTF-8 nei metadati utente

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape nei metadati definiti dall'utente. Le

richieste HEAD per un oggetto con caratteri UTF-8 sfuggiti 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 supportata

È supportata la seguente intestazione di richiesta:

- `x-amz-checksum-mode`

  IL `partNumber` parametro e `Range` l'intestazione non è supportata con `x-amz-checksum-mode` per HeadObject. Quando li includi nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore di checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented` :

- `x-amz-website-redirect-location`

Controllo delle versioni

Se un `versionId` Se la sottorisorsa non è specificata, l'operazione recupera la versione più recente dell'oggetto in un bucket con versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "Non trovato" con `x-amz-delete-marker` intestazione di risposta impostata su `true` .

Intestazioni di richiesta 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 da te fornita.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
- `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specifica 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 anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in"Utilizzare la crittografia lato server" .

Risposte HeadObject per gli oggetti Cloud Storage Pool

Se l'oggetto è memorizzato in un"Pool di archiviazione cloud" , vengono restituite le seguenti intestazioni di risposta:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Le intestazioni di risposta forniscono informazioni sullo stato di un oggetto mentre viene spostato in un Cloud Storage Pool, facoltativamente portato a uno stato non recuperabile e ripristinato.

Stato dell'oggetto	Risposta a HeadObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM, oppure oggetto archiviato in un pool di archiviazione tradizionale o mediante codifica di cancellazione	`200 OK`(Non viene restituita alcuna intestazione di risposta speciale.)

Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Finché l'oggetto non viene portato in uno stato non recuperabile, il valore per `expiry-date` è ambientato in un lontano futuro. Il momento esatto della transizione non è controllato dal sistema StorageGRID .

L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche sulla griglia	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Il valore per `expiry-date` è ambientato in un lontano futuro.
	
	Nota: se la copia sulla griglia non è disponibile (ad esempio, un nodo di archiviazione è inattivo), è necessario emettere un"Ripristina oggetto" richiedere di ripristinare la copia dal Cloud Storage Pool prima di poter recuperare correttamente l'oggetto.

L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia sulla griglia	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Oggetto in fase di ripristino da uno stato non recuperabile	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Stato dell'oggetto	Risposta a HeadObject

Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	IL `expiry-date` indica quando l'oggetto nel Cloud Storage Pool tornerà a uno stato non recuperabile.

Oggetti multiparte o segmentati in Cloud Storage Pool

Se hai caricato un oggetto multiparte o se StorageGRID ha suddiviso un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel Cloud Storage Pool campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta HeadObject potrebbe restituire in modo errato `x-amz-restore: ongoing-request="false"` quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono ancora state ripristinate.

HeadObject e replicazione cross-grid

Se stai usando"federazione di rete" E"replicazione cross-grid" è abilitato per un bucket, il client S3 può verificare lo stato di replicazione di un oggetto inviando una richiesta HeadObject. La risposta include StorageGRID-specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	• **COMPLETO**: La replica è riuscita. • **IN ATTESA**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

> StorageGRID non supporta il `x-amz-replication-status` intestazione.

MettiOggetto

È possibile utilizzare la richiesta S3 PutObject per aggiungere un oggetto a un bucket.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *consigliata* per una singola operazione PutObject è 5 GiB (5.368.709.120 byte). Se hai oggetti più grandi di 5 GiB, usa"caricamento multiparte" Invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).

> Se hai eseguito l'aggiornamento da StorageGRID 11.6 o da una versione precedente, verrà attivato l'avviso S3 PUT Object size too large (Dimensioni oggetto troppo grandi) se tenti di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11.7 o 11.8, in questo caso l'avviso non verrà attivato. Tuttavia, per allinearsi allo standard AWS S3, le future versioni di StorageGRID non supporteranno caricamenti di oggetti di dimensioni superiori a 5 GiB.

Dimensione dei metadati 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 utente a 24 KiB. La dimensione dei metadati definiti dall'utente viene misurata sommando il numero di byte nella codifica UTF-8 di ciascuna chiave e valore.

Caratteri UTF-8 nei metadati utente

Se una richiesta include valori UTF-8 (non sottoposti a escape) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento StorageGRID non è definito.

StorageGRID non analizza né interpreta i caratteri UTF-8 con escape inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 sottoposti a escape vengono trattati come caratteri ASCII:

- Le richieste PutObject, CopyObject, GetObject e HeadObject hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 con escape.
- StorageGRID non restituisce il `x-amz-missing-meta` intestazione se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Limiti dei tag degli oggetti

Puoi aggiungere tag ai nuovi oggetti quando li carichi oppure puoi aggiungerli agli oggetti esistenti. Sia StorageGRID che Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave tag può avere una lunghezza massima di 128 caratteri Unicode e i valori tag possono avere una lunghezza massima di 256 caratteri Unicode. Le chiavi e i valori sono sensibili alle maiuscole e alle minuscole.

Proprietà dell'oggetto

In StorageGRID, tutti gli oggetti sono di proprietà dell'account proprietario del bucket, compresi 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 specifichi `aws-chunked` per`Content-Encoding` StorageGRID non verifica i seguenti elementi:

  - StorageGRID non verifica il `chunk-signature` rispetto ai dati in blocco.
  - StorageGRID non verifica il valore fornito per `x-amz-decoded-content-length` contro l'oggetto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  La codifica di trasferimento in blocchi è supportata se `aws-chunked` viene utilizzata anche la firma del payload.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente.

  Quando si specifica la coppia nome-valore per i metadati definiti dall'utente, utilizzare questo formato generale:

  ```
  x-amz-meta-name: value
  ```

  Se si desidera utilizzare l'opzione **Ora di creazione definita dall'utente** come ora di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano quando è stato creato l'oggetto. Per esempio:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  Il valore per `creation-time` viene valutato in secondi a partire dal 1° gennaio 1970.

  > Una regola ILM non può utilizzare sia un **orario di creazione definito dall'utente** per l'orario di riferimento sia l'opzione di acquisizione bilanciata o rigorosa. Viene restituito un errore quando viene creata la regola ILM.
- `x-amz-tagging`
- Intestazioni di richiesta di blocco degli oggetti S3
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

Se viene effettuata una richiesta senza queste intestazioni, vengono utilizzate le impostazioni di conservazione predefinite del bucket per calcolare la modalità di versione dell'oggetto e la data di conservazione fino alla data di scadenza. Vedere "Utilizzare l'API REST S3 per configurare S3 Object Lock" .

- Intestazioni delle richieste 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`

  VedereIntestazioni di richiesta per la crittografia lato server

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  IL `x-amz-website-redirect-location` intestazione ritorna `XNotImplemented` .

Opzioni di classe di archiviazione

IL `x-amz-storage-class` è supportata l'intestazione della richiesta. 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 archiviate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto ingerito utilizza l'opzione di ingestione rigorosa, `x-amz-storage-class` l'intestazione non ha alcun effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class` :

- `STANDARD`(Predefinito)
  - **Doppio commit**: se la regola ILM specifica l'opzione Doppio commit per Comportamento di acquisizione, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita a un diverso nodo di archiviazione (doppio commit). Quando l'ILM viene valutato, StorageGRID determina se queste copie provvisorie iniziali soddisfano le istruzioni di posizionamento nella regola. In caso contrario, potrebbe essere necessario creare nuove copie dell'oggetto in posizioni diverse e le copie provvisorie iniziali potrebbero dover essere eliminate.
  - **Bilanciato**: se la regola ILM specifica l'opzione Bilanciato e StorageGRID non riesce a effettuare immediatamente tutte le copie specificate nella regola, StorageGRID effettua due copie provvisorie su nodi di archiviazione diversi.

    Se StorageGRID può creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), `x-amz-storage-class` l'intestazione non ha alcun effetto.

- `REDUCED_REDUNDANCY`
  - **Doppio commit**: se la regola ILM specifica l'opzione Doppio commit per Comportamento di acquisizione, StorageGRID crea una singola copia provvisoria durante l'acquisizione dell'oggetto (singolo commit).
  - **Bilanciato**: se la regola ILM specifica l'opzione Bilanciato, StorageGRID esegue una singola copia provvisoria solo se il sistema non riesce a eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID può eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. IL `REDUCED_REDUNDANCY` L'opzione è più indicata quando la regola ILM che corrisponde all'oggetto crea una singola copia replicata. In questo caso utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia extra dell'oggetto per ogni operazione di acquisizione.

  Utilizzando il `REDUCED_REDUNDANCY` questa opzione non è consigliata in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, si potrebbero perdere dati se la singola copia viene inizialmente archiviata su un nodo di archiviazione che si guasta prima che possa aver luogo la valutazione ILM.

> Disporre di una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

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 effettuate quando l'oggetto viene valutato dai criteri ILM attivi e non determina l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID .

> Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio 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 la crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE**: utilizzare la seguente intestazione se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID.
  - `x-amz-server-side-encryption`

    Quando il `x-amz-server-side-encryption` l'intestazione non è inclusa nella richiesta PutObject, la griglia"impostazione di crittografia degli oggetti memorizzati" viene omesso dalla risposta PutObject.
- **SSE-C**: utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per il nuovo

oggetto.

- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni per"utilizzando la crittografia lato server" .

> Se un oggetto è crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Controllo delle versioni

Se il controllo delle versioni è abilitato per un bucket, univoco `versionId` viene generato automaticamente per la versione dell'oggetto memorizzato. Questo `versionId` viene restituito anche nella risposta utilizzando il `x-amz-version-id` intestazione di risposta.

Se il controllo delle versioni è sospeso, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, questa verrà sovrascritta.

Calcoli della firma per l'intestazione di autorizzazione

Quando si utilizza il `Authorization` intestazione per autenticare le richieste, StorageGRID differisce da AWS nei seguenti modi:

- StorageGRID non richiede `host` intestazioni da includere all'interno `CanonicalHeaders` .
- StorageGRID non richiede `Content-Type` da includere all'interno `CanonicalHeaders` .
- StorageGRID non richiede `x-amz-*` intestazioni da includere all'interno `CanonicalHeaders` .

> Come buona pratica generale, includi sempre queste intestazioni all'interno `CanonicalHeaders` per garantire che siano verificati; tuttavia, se si escludono queste intestazioni, StorageGRID non restituisce un errore.

Per i dettagli, fare riferimento a "Calcoli della firma per l'intestazione di autorizzazione: trasferimento del payload in un singolo blocco (AWS Signature versione 4)" .

Informazioni correlate

- "Gestire gli oggetti con ILM"
- "Riferimento API di Amazon Simple Storage Service: PutObject"

Ripristina oggetto

È possibile utilizzare la richiesta S3 RestoreObject per ripristinare un oggetto archiviato in un Cloud Storage Pool.

Tipo di richiesta supportato

StorageGRID supporta solo le richieste RestoreObject per ripristinare un oggetto. Non supporta il `SELECT` tipo

di restauro. Seleziona le richieste di ritorno `XNotImplemented` .

Controllo delle versioni

Facoltativamente, specificare `versionId` per ripristinare una versione specifica di un oggetto in un bucket con versione. Se non specifichi `versionId` , viene ripristinata la versione più recente dell'oggetto

Comportamento di RestoreObject sugli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in un"Pool di archiviazione cloud" , una richiesta RestoreObject ha il seguente comportamento, in base allo stato dell'oggetto. Vedere"HeadObject" per maggiori dettagli.

> Se un oggetto è archiviato in un Cloud Storage Pool e sulla griglia sono presenti anche una o più copie dell'oggetto, non è necessario ripristinare l'oggetto inviando una richiesta RestoreObject. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando una richiesta GetObject.

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto inserito in StorageGRID ma non ancora valutato da ILM oppure l'oggetto non si trova in un Cloud Storage Pool	`403 Forbidden` , `InvalidObjectState`
Oggetto nel Cloud Storage Pool ma non ancora trasferito a uno stato non recuperabile	`200 OK`Non vengono apportate modifiche. **Nota**: prima che un oggetto sia passato a uno stato non recuperabile, non è possibile modificarne lo stato. `expiry-date` .
Oggetto passato a 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 torna a uno stato non recuperabile. Facoltativamente, utilizzare il `Tier` elemento di richiesta per determinare quanto tempo impiegherà il processo di ripristino per essere completato(`Expedited` , `Standard` , O `Bulk`). Se non specifichi `Tier` , IL `Standard` viene utilizzato il livello. **Importante**: se un oggetto è stato trasferito a S3 Glacier Deep Archive o il pool di archiviazione cloud utilizza l'archiviazione BLOB di Azure, non è possibile ripristinarlo utilizzando `Expedited` livello. Viene restituito il seguente errore `403 Forbidden` , `InvalidTier` : `Retrieval option is not supported by this storage class` .
Oggetto in fase di ripristino da uno stato non recuperabile	`409 Conflict` , `RestoreAlreadyInProgress`

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto completamente ripristinato nel Cloud Storage Pool	`200 OK` **Nota:** se un oggetto è stato ripristinato in uno stato recuperabile, è possibile modificarne lo stato `expiry-date` riemettendo la richiesta RestoreObject con un nuovo valore per `Days` . La data di ripristino viene aggiornata in base al momento della richiesta.

SelezionaOggettoContenuto

È possibile utilizzare la richiesta S3 SelectObjectContent per filtrare il contenuto di un oggetto S3 in base a una semplice istruzione SQL.

Per maggiori informazioni vedere "Riferimento API di Amazon Simple Storage Service: SelectObjectContent" .

Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 Select.
- Hai `s3:GetObject` autorizzazione per l'oggetto che si desidera interrogare.
- L'oggetto che si desidera interrogare deve essere in uno dei seguenti formati:
  - **CSV**. Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
  - **Parquet**. Requisiti aggiuntivi per gli oggetti Parquet:
    - S3 Select supporta solo la compressione colonnare tramite GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti Parquet.
    - S3 Select non supporta l'output Parquet. È necessario specificare il formato di output come CSV o JSON.
    - La dimensione massima del gruppo di righe non compresso è 512 MB.
    - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
    - Non è possibile utilizzare i tipi logici INTERVAL, JSON, LIST, TIME o UUID.
- La lunghezza massima dell'espressione SQL è di 256 KB.
- Ogni record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi della richiesta CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Esempio di sintassi della richiesta Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Esempio di query SQL

Questa query ricava il nome dello stato, la popolazione del 2010, la popolazione stimata del 2015 e la percentuale di variazione dai dati del censimento degli Stati Uniti. I record nel file che non sono stati vengono ignorati.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Le prime righe del file da interrogare, `SUB-EST2020_ALL.csv` , assomiglia a questo:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Esempio di utilizzo di AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Le prime righe del file di output, `changes.csv` , assomiglia a questo:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Esempio di utilizzo di AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Le prime righe del file di output, changes.csv, hanno questo aspetto:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operazioni per caricamenti multiparte

Operazioni per caricamenti multiparte

Questa sezione descrive come StorageGRID supporta le operazioni per i caricamenti multiparte.

Le seguenti condizioni e note si applicano a tutte le operazioni di caricamento multiparte:

- Non dovresti superare i 1.000 caricamenti multipart simultanei in un singolo bucket perché i risultati delle query ListMultipartUploads per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID impone limiti dimensionali AWS per le parti multiparte. I client S3 devono seguire queste linee guida:
  - Ogni parte di un caricamento multiparte deve avere una dimensione 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 dovrebbero essere le più grandi possibile. Ad esempio, utilizzare dimensioni di parti pari a 5 GiB per un oggetto da 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce il sovraccarico dei metadati StorageGRID .
  - Per oggetti di dimensioni inferiori a 5 GiB, si consiglia di utilizzare il caricamento non multiparte.
- ILM viene valutato per ogni parte di un oggetto multiparte mentre viene ingerito e per l'oggetto nel suo complesso quando il caricamento multiparte viene completato, se la regola ILM utilizza Bilanciato o Rigoroso"opzione di ingestione" . È necessario essere consapevoli di come ciò influisce sul posizionamento di oggetti e parti:
  - Se ILM cambia mentre è in corso un caricamento multiparte S3, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. Ogni parte non posizionata

correttamente viene messa in coda per la rivalutazione ILM e successivamente spostata nella posizione corretta.

    - Quando si valuta l'ILM per una parte, StorageGRID filtra in base alle dimensioni della parte, non in base alle dimensioni dell'oggetto. Ciò significa che parti di un oggetto possono essere archiviate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più grandi vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene archiviata in DC2 al momento dell'acquisizione. Tuttavia, quando l'ILM viene valutato per l'oggetto nel suo complesso, tutte le parti dell'oggetto vengono spostate in DC1.

- Tutte le operazioni di caricamento multiparte supportano StorageGRID"valori di coerenza" .
- Quando un oggetto viene ingerito tramite caricamento multiparte,"soglia di segmentazione degli oggetti (1 GiB)" non viene applicato.
- Se necessario, puoi utilizzare"crittografia lato server" con caricamenti in più parti. 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 CreateMultipartUpload. Per utilizzare SSE-C (crittografia lato server con chiavi fornite dal cliente), è necessario specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta CreateMultipartUpload e in ogni successiva richiesta UploadPart.

Operazione	Implementazione
Annulla caricamento multiparte	Implementato con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
Caricamento multiparte completo	Vedere"Caricamento multiparte completo"
CreaCaricamentoMultiparte (in precedenza denominato Avvia caricamento multiparte)	Vedere"CreaCaricamentoMultiparte"
Caricamenti multiparte di List	Vedere"Caricamenti multiparte di List"
ElencoParti	Implementato con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.
CaricaParte	Vedere"CaricaParte"
CaricaParteCopia	Vedere"CaricaParteCopia"

Caricamento multiparte completo

L'operazione CompleteMultipartUpload completa il caricamento multiparte di un oggetto assemblando le parti caricate in precedenza.

> StorageGRID supporta valori non consecutivi in ordine crescente per `partNumber` parametro di richiesta con CompleteMultipartUpload. Il parametro può iniziare con qualsiasi valore.

Risolvere i conflitti

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base al principio "latest-wins". La tempistica per la valutazione "latest-wins" si basa sul momento in cui il sistema StorageGRID completa una determinata richiesta e non su quando i client S3 iniziano un'operazione.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  IL `x-amz-storage-class` l'intestazione influisce sul numero di copie dell'oggetto che StorageGRID crea se la regola ILM corrispondente specifica"Opzione di commit doppio o di ingestione bilanciata" .

- `STANDARD`

  (Predefinito) Specifica un'operazione di acquisizione a doppio commit quando la regola ILM utilizza l'opzione Doppio commit o quando l'opzione Bilanciato ricorre alla creazione di copie provvisorie.

- `REDUCED_REDUNDANCY`

  Specifica un'operazione di acquisizione con commit singolo quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced ricorre alla creazione di copie provvisorie.

  > Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio 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 eliminati 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.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controllo delle versioni

Questa operazione completa un caricamento in più parti. Se per un bucket è abilitato il controllo delle versioni, la versione dell'oggetto viene creata dopo il completamento del caricamento multiparte.

Se il controllo delle versioni è abilitato per un bucket, univoco `versionId` viene generato automaticamente

per la versione dell'oggetto memorizzato. Questo `versionId` viene restituito anche nella risposta utilizzando il `x-amz-version-id` intestazione di risposta.

Se il controllo delle versioni è sospeso, la versione dell'oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, questa verrà sovrascritta.

> Quando il controllo delle versioni è abilitato per un bucket, il completamento di un caricamento multiparte crea sempre una nuova versione, anche se sono stati completati caricamenti multiparte simultanei sulla stessa chiave oggetto. Quando il controllo delle versioni non è abilitato per un bucket, è possibile avviare un caricamento multiparte e quindi avviare e completare prima un altro caricamento multiparte sulla stessa chiave dell'oggetto. Nei bucket senza controllo delle versioni, ha la precedenza il caricamento multiparte completato per ultimo.

Replicazione, notifica o notifica dei metadati non riuscita

Se il bucket in cui avviene il caricamento multiparte è configurato per un servizio di piattaforma, il caricamento multiparte riesce anche se l'azione di replica o notifica associata fallisce.

Un tenant può attivare la replica non riuscita o la notifica aggiornando i metadati o i tag dell'oggetto. Un inquilino può reinviare i valori esistenti per evitare di apportare modifiche indesiderate.

Fare riferimento a "Risolvere i problemi dei servizi della piattaforma" .

CreaCaricamentoMultiparte

L'operazione CreateMultipartUpload (in precedenza denominata Initiate Multipart Upload) avvia un caricamento multiparte per un oggetto e restituisce un ID di caricamento.

IL `x-amz-storage-class` è supportata l'intestazione della richiesta. 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 archiviate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto ingerito utilizza Strict"opzione di ingestione" , IL `x-amz-storage-class` l'intestazione non ha alcun effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class` :

- `STANDARD`(Predefinito)
  - **Doppio commit**: se la regola ILM specifica l'opzione di acquisizione Doppio commit, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita a un diverso nodo di archiviazione (doppio commit). Quando l'ILM viene valutato, StorageGRID determina se queste copie provvisorie iniziali soddisfano le istruzioni di posizionamento nella regola. In caso contrario, potrebbe essere necessario creare nuove copie dell'oggetto in posizioni diverse e le copie provvisorie iniziali potrebbero dover essere eliminate.
  - **Bilanciato**: se la regola ILM specifica l'opzione Bilanciato e StorageGRID non riesce a effettuare immediatamente tutte le copie specificate nella regola, StorageGRID effettua due copie provvisorie su nodi di archiviazione diversi.

    Se StorageGRID può creare immediatamente tutte le copie degli oggetti specificate nella regola ILM (posizionamento sincrono), `x-amz-storage-class` l'intestazione non ha alcun effetto.
- `REDUCED_REDUNDANCY`

- **Doppio commit**: se la regola ILM specifica l'opzione Doppio commit, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (singolo commit).
- **Bilanciato**: se la regola ILM specifica l'opzione Bilanciato, StorageGRID esegue una singola copia provvisoria solo se il sistema non riesce a eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID può eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. IL `REDUCED_REDUNDANCY` L'opzione è più indicata quando la regola ILM che corrisponde all'oggetto crea una singola copia replicata. In questo caso utilizzando `REDUCED_REDUNDANCY` elimina la creazione e l'eliminazione non necessarie di una copia extra dell'oggetto per ogni operazione di acquisizione.

Utilizzando il `REDUCED_REDUNDANCY` questa opzione non è consigliata in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, si potrebbero perdere dati se la singola copia viene inizialmente archiviata su un nodo di archiviazione che si guasta prima che possa aver luogo la valutazione ILM.

> Disporre di una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

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 effettuate quando l'oggetto viene valutato dai criteri ILM attivi e non determina l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID .

> Se si sta inserendo un oggetto in un bucket con S3 Object Lock abilitato, `REDUCED_REDUNDANCY` l'opzione viene ignorata. Se si sta ingerendo un oggetto in un bucket conforme legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un inserimento a doppio commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Type`
- `x-amz-checksum-algorithm`

  Attualmente, solo il valore SHA256 per `x-amz-checksum-algorithm` è supportato.

- `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 **Ora di creazione definita dall'utente** come ora di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano quando è

stato creato l'oggetto. Per esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per `creation-time` viene valutato in secondi a partire dal 1° gennaio 1970.

> Aggiunta `creation-time` poiché i metadati definiti dall'utente non sono consentiti se si aggiunge un oggetto a un bucket in cui è abilitata la conformità legacy. Verrà restituito un errore.

- Intestazioni delle richieste di blocco degli oggetti S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Se viene effettuata una richiesta senza queste intestazioni, per calcolare la versione dell'oggetto retain-until-date vengono utilizzate le impostazioni di conservazione predefinite del bucket.

"Utilizzare l'API REST S3 per configurare S3 Object Lock"

- Intestazioni delle richieste SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Intestazioni di richiesta per la crittografia lato server

> Per informazioni su come StorageGRID gestisce i caratteri UTF-8, vedere"MettiOggetto" .

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto multiparte con la crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE**: utilizzare la seguente intestazione nella richiesta CreateMultipartUpload se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C**: utilizzare tutte e tre queste intestazioni nella richiesta CreateMultipartUpload (e in ogni successiva richiesta UploadPart) se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.
  - `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Specifica la chiave di crittografia per il nuovo

oggetto.

- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni per"utilizzando la crittografia lato server" .

Intestazioni di richiesta non supportate

La seguente intestazione di richiesta non è supportata:

- `x-amz-website-redirect-location`

  IL `x-amz-website-redirect-location` intestazione ritorna `XNotImplemented` .

Controllo delle versioni

Il caricamento multiparte consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e sottoposti a controllo di versione, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

Caricamenti multiparte di List

L'operazione ListMultipartUploads elenca i caricamenti multiparte in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Controllo delle versioni

Il caricamento multiparte consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e sottoposti a controllo di versione, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

CaricaParte

L'operazione UploadPart carica una parte in un caricamento multiparte per un oggetto.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Intestazioni di richiesta per la crittografia lato server

Se hai specificato la crittografia SSE-C per la richiesta CreateMultipartUpload, devi includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
- `x-amz-server-side-encryption-customer-key`: Specificare la stessa chiave di crittografia fornita nella richiesta CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare lo stesso digest MD5 fornito nella richiesta CreateMultipartUpload.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in"Utilizzare la crittografia lato server" .

Se hai specificato un checksum SHA-256 durante la richiesta CreateMultipartUpload, devi includere anche la seguente intestazione di richiesta in ogni richiesta UploadPart:

- `x-amz-checksum-sha256`: Specificare il checksum SHA-256 per questa parte.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controllo delle versioni

Il caricamento multiparte consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e sottoposti a controllo di versione, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

CaricaParteCopia

L'operazione UploadPartCopy carica una parte di un oggetto copiando i dati da un oggetto esistente come origine dati.

L'operazione UploadPartCopy è implementata con tutti i comportamenti dell'API REST di Amazon S3. Soggetto a modifiche senza preavviso.

Questa richiesta legge e scrive i dati dell'oggetto specificati in `x-amz-copy-source-range` all'interno del sistema StorageGRID .

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Intestazioni di richiesta per la crittografia lato server

Se hai specificato la crittografia SSE-C per la richiesta CreateMultipartUpload, devi includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256` .
- `x-amz-server-side-encryption-customer-key`: Specificare la stessa chiave di crittografia fornita nella richiesta CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare lo stesso digest MD5 fornito nella richiesta CreateMultipartUpload.

Se l'oggetto sorgente è crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta UploadPartCopy, in modo che l'oggetto possa essere decrittografato e quindi copiato:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare `AES256` .
- `x-amz-copy-source-server-side-encryption-customer-key`: Specifica la chiave di crittografia fornita al momento della creazione dell'oggetto sorgente.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specifica il digest MD5 fornito quando hai creato l'oggetto sorgente.

> Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde anche l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, rivedere le considerazioni in"Utilizzare la crittografia lato server" .

Controllo delle versioni

Il caricamento multiparte consiste in operazioni separate per avviare il caricamento, elencare i caricamenti, caricare le parti, assemblare le parti caricate e completare il caricamento. Gli oggetti vengono creati (e sottoposti a controllo di versione, se applicabile) quando viene eseguita l'operazione CompleteMultipartUpload.

Risposte di errore

Il sistema StorageGRID supporta tutte le risposte di errore standard S3 REST API applicabili. Inoltre, l'implementazione StorageGRID aggiunge diverse risposte personalizzate.

Codici di errore API S3 supportati

Nome	Stato HTTP
Accesso negato	403 Proibito
BadDigest	400 Richiesta non valida
BucketAlreadyExists	409 Conflitto
BucketNotEmpty	409 Conflitto
Corpo incompleto	400 Richiesta non valida
Errore interno	500 Errore interno del server
ID chiave di accesso non valido	403 Proibito
Argomento non valido	400 Richiesta non valida
NomeBucketNonValido	400 Richiesta non valida
StatoBucketNonValido	409 Conflitto
InvalidDigest	400 Richiesta non valida
Errore algoritmo di crittografia non valido	400 Richiesta non valida
Parte non valida	400 Richiesta non valida
OrdineParteNonValido	400 Richiesta non valida
Intervallo non valido	416 Intervallo richiesto non soddisfacibile
Richiesta non valida	400 Richiesta non valida
Classe di archiviazione non valida	400 Richiesta non valida
Tag non valido	400 Richiesta non valida
URI non valido	400 Richiesta non valida
KeyTooLong	400 Richiesta non valida
XML malformato	400 Richiesta non valida

Nome	Stato HTTP
Metadati troppo grandi	400 Richiesta non valida
Metodo non consentito	405 Metodo non consentito
Lunghezza del contenuto mancante	411 Lunghezza richiesta
Errore mancante nel corpo della richiesta	400 Richiesta non valida
MissingSecurityHeader	400 Richiesta non valida
NoSuchBucket	404 Non trovato
Nessuna chiave	404 Non trovato
NoSuchUpload	404 Non trovato
Non implementato	501 Non implementato
NoSuchBucketPolicy	404 Non trovato
Errore ObjectLockConfigurationNotFound	404 Non trovato
Precondizione fallita	412 Precondizione fallita
RequestTimeTooSkewed	403 Proibito
Servizio non disponibile	503 Servizio non disponibile
Firma non corrisponde	403 Proibito
Troppi secchi	400 Richiesta non valida
UserKeyMustBeSpecified	400 Richiesta non valida

Codici di errore personalizzati StorageGRID

Nome	Descrizione	Stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket conforme legacy	400 Richiesta non valida
XBucketPolicyParseException	Impossibile analizzare il JSON del criterio del bucket ricevuto.	400 Richiesta non valida

Nome	Descrizione	Stato HTTP
XComplianceConflict	Operazione negata a causa delle impostazioni di conformità legacy.	403 Proibito
XComplianceReducedRedundancyForbidden	La ridondanza ridotta non è consentita nel bucket Compliant legacy	400 Richiesta non valida
XMaxBucketPolicyLengthExceeded	La tua policy supera la lunghezza massima consentita per il bucket.	400 Richiesta non valida
XMissingInternalRequestHeader	Manca un'intestazione di una richiesta interna.	400 Richiesta non valida
XNoSuchBucketCompliance	Nel bucket specificato non è abilitata la conformità legacy.	404 Non trovato
XNon accettabile	La richiesta contiene una o più intestazioni di accettazione che non è stato possibile soddisfare.	406 Non accettabile
XNonImplementato	La richiesta da te fornita implica una funzionalità non implementata.	501 Non implementato

Operazioni personalizzate StorageGRID

Operazioni personalizzate StorageGRID

Il sistema StorageGRID supporta operazioni personalizzate che vengono aggiunte all'API REST S3.

Nella tabella seguente sono elencate le operazioni personalizzate supportate da StorageGRID.

Operazione	Descrizione
"OTTIENI la coerenza del bucket"	Restituisce la coerenza applicata a un determinato bucket.
"PUT Consistenza del secchio"	Imposta la coerenza applicata a un determinato bucket.
"GET Ora dell'ultimo accesso al bucket"	Restituisce se gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati o disabilitati per un determinato bucket.
"Ora dell'ultimo accesso al bucket PUT"	Consente di abilitare o disabilitare gli aggiornamenti dell'ora dell'ultimo accesso per un determinato bucket.
"ELIMINA la configurazione della notifica dei metadati del bucket"	Elimina l'XML di configurazione delle notifiche dei metadati associato a un determinato bucket.

Operazione	Descrizione
"Configurazione della notifica dei metadati del bucket GET"	Restituisce il file XML di configurazione delle notifiche dei metadati associato a un determinato bucket.
"Configurazione della notifica dei metadati del bucket PUT"	Configura il servizio di notifica dei metadati per un bucket.
"Utilizzo dello spazio di archiviazione GET"	Indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account.
"Obsoleto: CreateBucket con impostazioni di conformità"	Obsoleto e non supportato: non è più possibile creare nuovi bucket con la conformità abilitata.
"Obsoleto: conformità al bucket GET"	Obsoleto ma supportato: restituisce le impostazioni di conformità attualmente in vigore per un bucket Compliant legacy esistente.
"Obsoleto: conformità al bucket PUT"	Obsoleto ma supportato: consente di modificare le impostazioni di conformità per un bucket Compliant legacy esistente.

OTTIENI la coerenza del bucket

La richiesta di coerenza del bucket GET consente di determinare la coerenza applicata a un determinato bucket.

La coerenza predefinita è impostata per garantire la lettura dopo la scrittura per gli oggetti appena creati.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:GetBucketConsistency oppure essere l'account root.

Richiedi esempio

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Nella risposta XML, `<Consistency>` restituirà uno dei seguenti valori:

Coerenza	Descrizione
Tutto	Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
forte-globale	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.

Coerenza	Descrizione
sito forte	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito.
lettura dopo nuova scrittura	(Predefinito) Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
disponibile	Fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool .

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

"Valori di coerenza"

PUT Consistenza del secchio

La richiesta di coerenza PUT Bucket consente di specificare la coerenza da applicare alle operazioni eseguite su un bucket.

La coerenza predefinita è impostata per garantire la lettura dopo la scrittura per gli oggetti appena creati.

Prima di iniziare

Per completare questa operazione è necessario disporre dell'autorizzazione s3:PutBucketConsistency oppure essere l'account root.

Richiesta

IL `x-ntap-sg-consistency` il parametro deve contenere uno dei seguenti valori:

Coerenza	Descrizione
Tutto	Tutti i nodi ricevono immediatamente i dati, altrimenti la richiesta fallirà.
forte-globale	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.
sito forte	Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito.
lettura dopo nuova scrittura	(Predefinito) Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
disponibile	Fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool .

Nota: in generale, dovresti usare la coerenza "Lettura dopo nuova scrittura". Se le richieste non funzionano correttamente, modificare, se possibile, il comportamento del client dell'applicazione. Oppure, configura il client in modo che specifichi la coerenza per ogni richiesta API. Impostare la coerenza a livello di bucket solo come ultima risorsa.

Richiedi esempio

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informazioni correlate

"Valori di coerenza"

GET Ora dell'ultimo accesso al bucket

La richiesta GET sull'orario dell'ultimo accesso al bucket consente di determinare se gli aggiornamenti dell'orario dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:GetBucketLastAccessTime oppure essere l'account root.

Richiedi esempio

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra che gli aggiornamenti dell'ora dell'ultimo accesso sono abilitati 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>
```

Ora dell'ultimo accesso al bucket PUT

La richiesta dell'orario dell'ultimo accesso al bucket PUT consente di abilitare o disabilitare gli aggiornamenti dell'orario dell'ultimo accesso per singoli bucket. La disattivazione degli aggiornamenti dell'ora dell'ultimo 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 oppure essere l'account root.

> A partire dalla versione 10.3 StorageGRID , gli aggiornamenti all'ora dell'ultimo accesso sono disabilitati per impostazione predefinita per tutti i nuovi bucket. Se si dispone di bucket creati utilizzando una versione precedente di StorageGRID e si desidera applicare il nuovo comportamento predefinito, è necessario disabilitare esplicitamente gli aggiornamenti dell'ora dell'ultimo accesso per ciascuno di tali bucket precedenti. È possibile abilitare o disabilitare gli aggiornamenti all'orario dell'ultimo accesso tramite la richiesta dell'orario dell'ultimo accesso al bucket PUT o dalla pagina dei dettagli di un bucket in Tenant Manager. Vedere "Abilita o disabilita gli aggiornamenti dell'ultimo orario di accesso" .

Se gli aggiornamenti dell'ora dell'ultimo accesso sono disabilitati per un bucket, alle operazioni sul bucket viene applicato il seguente comportamento:

- Le richieste GetObject, GetObjectAcl, GetObjectTagging e HeadObject non aggiornano l'ora dell'ultimo accesso. L'oggetto non viene aggiunto alle code per la valutazione della gestione del ciclo di vita delle informazioni (ILM).

- Le richieste CopyObject e PutObjectTagging che aggiornano solo i metadati aggiornano anche l'ora dell'ultimo accesso. L'oggetto viene aggiunto alle code per la valutazione ILM.
- Se gli aggiornamenti all'ora dell'ultimo accesso sono disabilitati per il bucket di origine, le richieste CopyObject non aggiornano l'ora dell'ultimo accesso per il bucket di origine. L'oggetto copiato non viene aggiunto alle code per la valutazione ILM per il bucket di origine. Tuttavia, per la destinazione, le richieste CopyObject aggiornano sempre l'ora dell'ultimo accesso. La copia dell'oggetto viene aggiunta alle code per la valutazione ILM.
- Le richieste CompleteMultipartUpload aggiornano l'orario dell'ultimo accesso. L'oggetto completato viene aggiunto alle code per la valutazione ILM.

Esempi di richiesta

Questo esempio abilita l'orario dell'ultimo accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Questo esempio disabilita l'orario dell'ultimo accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

ELIMINA la configurazione della notifica dei metadati del bucket

La richiesta di configurazione della notifica dei metadati DELETE Bucket consente di disabilitare il servizio di integrazione della ricerca per singoli bucket eliminando l'XML di configurazione.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:DeleteBucketMetadataNotification per un bucket oppure essere l'account root.

Richiedi esempio

Questo esempio mostra come disabilitare il servizio di integrazione della ricerca per un bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configurazione della notifica dei metadati del bucket GET

La richiesta di configurazione della notifica dei metadati del bucket GET 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 oppure essere l'account root.

Richiedi esempio

Questa richiesta recupera la configurazione della notifica dei metadati per il bucket denominato `bucket` .

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Il corpo della risposta include la configurazione della notifica dei metadati per il bucket. La configurazione della notifica dei metadati consente di determinare come configurare il bucket per l'integrazione della ricerca. Ciò significa che è possibile determinare quali oggetti sono 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 a cui StorageGRID deve inviare i metadati degli oggetti. Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID .

Nome	Descrizione	Necessario
MetadatiNotificaConfigurazione	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati. Contiene uno o più elementi Rule.	SÌ
Regola	Tag contenitore 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 per la regola. Incluso nell'elemento Regola.	NO
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilitate. Incluso nell'elemento Regola.	SÌ
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Regola.	SÌ
Destinazione	Tag contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	SÌ

Nome	Descrizione	Necessario
Urna	URN della destinazione a cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • `es`deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono archiviati i metadati, nel formato `domain-name/myindex/mytype` . Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404. L'urna è inclusa nell'elemento Destinazione.	SÌ

Esempio di risposta

L'XML incluso tra `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags mostra come l'integrazione con un endpoint di integrazione della ricerca è configurata per il bucket. In questo esempio, i metadati dell'oggetto vengono inviati a un indice Elasticsearch denominato `current` e digita denominato `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"

Configurazione della notifica dei metadati del bucket PUT

La richiesta di configurazione della notifica dei metadati del bucket PUT consente di abilitare il servizio di integrazione della ricerca per singoli bucket. Il codice 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 oppure essere l'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 a cui StorageGRID deve inviare i metadati degli oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, potresti inviare metadati per oggetti con il prefisso `/images` verso una destinazione e oggetti con il prefisso `/videos` all'altro.

Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, una configurazione che 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, altrimenti la richiesta fallisce come

`400 Bad Request` Il messaggio di errore afferma: `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 presenti nel file XML di configurazione delle notifiche dei metadati.

Nome	Descrizione	Necessario
MetadatiNotificaConfigurazione	Tag contenitore per le regole utilizzate per specificare gli oggetti e la destinazione delle notifiche dei metadati. Contiene uno o più elementi Rule.	SÌ
Regola	Tag contenitore 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 per la regola. Incluso nell'elemento Regola.	NO
Stato	Lo stato può essere "Abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disabilitate. Incluso nell'elemento Regola.	SÌ

Nome	Descrizione	Necessario
Prefisso	Gli oggetti che corrispondono al prefisso sono interessati dalla regola e i loro metadati vengono inviati alla destinazione specificata. Per trovare la corrispondenza con tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Regola.	SÌ
Destinazione	Tag contenitore per la destinazione di una regola. Incluso nell'elemento Regola.	SÌ
Urna	URN della destinazione a cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • `es`deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono archiviati i metadati, nel formato `domain-name/myindex/mytype` . Gli endpoint vengono configurati tramite Tenant Manager o Tenant Management API. Hanno la seguente forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` L'endpoint deve essere configurato prima di inviare il file XML di configurazione, altrimenti la configurazione fallirà con un errore 404. L'urna è inclusa nell'elemento Destinazione.	SÌ

Esempi di richiesta

Questo esempio mostra come abilitare l'integrazione della ricerca per un bucket. In questo esempio, i metadati di tutti gli oggetti vengono inviati alla stessa destinazione.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

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

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

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

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

JSON generato dal servizio di integrazione della ricerca

Quando si abilita il servizio di integrazione della ricerca per un bucket, ogni volta che vengono aggiunti, aggiornati o eliminati metadati o tag di un oggetto, viene generato un documento JSON che viene inviato all'endpoint di destinazione.

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

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

Metadati degli oggetti inclusi nelle notifiche dei metadati

Nella tabella sono elencati tutti i campi inclusi nel documento JSON inviato all'endpoint di destinazione quando è abilitata l'integrazione della ricerca.

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

Tipo	Nome dell'articolo	Descrizione
Informazioni su bucket e oggetti	secchio	Nome del bucket
Informazioni su bucket e oggetti	chiave	Nome chiave oggetto
Informazioni su bucket e oggetti	ID versione	Versione dell'oggetto, per gli oggetti nei bucket con versione
Informazioni su bucket e oggetti	regione	Regione del bucket, ad esempio `us-east-1`
Metadati di sistema	misurare	Dimensione dell'oggetto (in byte) visibile a un client HTTP
Metadati di sistema	md5	Hash dell'oggetto
Metadati utente	metadati *`key:value`*	Tutti i metadati utente per l'oggetto, come coppie chiave-valore
Etichette	etichette *`key:value`*	Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore

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

Informazioni correlate

"Utilizzare un account tenant"

Richiesta di utilizzo dello spazio di archiviazione GET

La richiesta GET Storage Usage indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account.

La quantità di spazio di archiviazione utilizzata da un account e dai suoi bucket può essere ottenuta tramite una richiesta ListBuckets modificata con `x-ntap-sg-usage` parametro di query. L'utilizzo dello spazio di archiviazione del bucket viene monitorato separatamente dalle richieste PUT e DELETE 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 elevato.

Per impostazione predefinita, StorageGRID tenta di recuperare le informazioni sull'utilizzo utilizzando la coerenza globale forte. Se non è possibile ottenere una coerenza globale forte, StorageGRID tenta di recuperare le informazioni sull'utilizzo con una coerenza del sito forte.

Per completare questa operazione è necessario disporre dell'autorizzazione s3:ListAllMyBuckets oppure essere l'account root.

Richiedi esempio

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra un account con quattro oggetti e 12 byte di dati in due bucket. Ogni bucket contiene due oggetti e sei byte di dati.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Controllo delle versioni

Ogni versione dell'oggetto memorizzata contribuirà a `ObjectCount` E `DataBytes` valori nella risposta. I marcatori di eliminazione non vengono aggiunti al `ObjectCount` totale.

Informazioni correlate

"Valori di coerenza"

Richieste di bucket deprecate per la conformità legacy

Richieste di bucket deprecate per la conformità legacy

Potrebbe essere necessario utilizzare l'API REST StorageGRID S3 per gestire i bucket creati utilizzando la funzionalità di conformità legacy.

Funzionalità di conformità deprecata

La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock.

Se in precedenza è stata abilitata l'impostazione Conformità globale, in StorageGRID 11.6 è abilitata l'impostazione Blocco oggetto S3 globale. Non è più possibile creare nuovi bucket con la conformità abilitata; tuttavia, se necessario, è possibile utilizzare l'API REST StorageGRID S3 per gestire eventuali bucket conformi legacy esistenti.

- "Utilizzare l'API REST S3 per configurare S3 Object Lock"
- "Gestire gli oggetti con ILM"
- "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"

Richieste di conformità deprecate:

- "Obsoleto - Modifiche alla richiesta PUT Bucket per conformità"

  L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML facoltativo delle richieste PUT Bucket per creare un bucket conforme.

- "Obsoleto - Conformità al bucket GET"

  La richiesta di conformità del bucket GET è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket Conforme legacy esistente.

- "Obsoleto - Conformità al bucket PUT"

  La richiesta di conformità del bucket PUT è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket Conforme legacy esistente. Ad esempio, è possibile mettere in attesa per motivi legali un bucket esistente o aumentarne il periodo di conservazione.

Obsoleto: modifiche alla richiesta CreateBucket per conformità

L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML facoltativa delle richieste CreateBucket per creare un bucket conforme.

> La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:
>
> - "Utilizzare l'API REST S3 per configurare S3 Object Lock"
> - "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"

Non è più possibile creare nuovi bucket con la Conformità abilitata. Se si tenta di utilizzare le modifiche alla richiesta CreateBucket per la conformità per creare un nuovo bucket conforme, viene restituito il seguente messaggio di errore:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsoleto: richiesta di conformità del bucket GET

La richiesta di conformità del bucket GET è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket Conforme legacy esistente.

> La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:
>
> - "Utilizzare l'API REST S3 per configurare S3 Object Lock"
> - "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"

Per completare questa operazione è necessario disporre dell'autorizzazione s3:GetBucketCompliance oppure essere l'account root.

Richiedi esempio

Questa richiesta di esempio consente di determinare le impostazioni di conformità per il bucket denominato `mybucket` .

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Nella risposta XML, `<SGCompliance>` elenca le impostazioni di conformità in vigore per il bucket. Questa risposta di esempio mostra le impostazioni di conformità per un bucket in cui ogni oggetto verrà conservato per un anno (525.600 minuti), a partire dal momento in cui l'oggetto viene inserito nella griglia. Al momento non esiste alcun blocco legale su questo bucket. Ogni oggetto verrà automaticamente eliminato dopo un anno.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrizione
Periodo di conservazioneMinuti	Durata del periodo di conservazione degli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella griglia.
LegalHold	• Vero: questo bucket è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché non viene revocata la sospensione legale, anche se il periodo di conservazione è scaduto. • Falso: questo bucket non è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket possono essere eliminati alla scadenza del periodo di conservazione.
Eliminazione automatica	• Vero: gli oggetti in questo bucket verranno eliminati automaticamente alla scadenza del periodo di conservazione, a meno che il bucket non sia soggetto a conservazione legale. • Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Se vuoi eliminarli, devi eliminarli manualmente.

Risposte di errore

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` .

Obsoleto: richiesta di conformità del bucket PUT

La richiesta di conformità del bucket PUT è obsoleta. Tuttavia, puoi continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket Conforme legacy esistente. Ad esempio, è possibile mettere in attesa per motivi legali un bucket esistente o aumentarne il periodo di conservazione.

> La funzionalità StorageGRID Compliance disponibile nelle precedenti versioni StorageGRID è obsoleta ed è stata sostituita da S3 Object Lock. Per maggiori dettagli vedere quanto segue:
>
> • "Utilizzare l'API REST S3 per configurare S3 Object Lock"
> • "Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"

Per completare questa operazione è necessario disporre dell'autorizzazione s3:PutBucketCompliance oppure essere l'account root.

Quando si invia una richiesta di conformità del bucket PUT, è necessario specificare un valore per ogni campo delle impostazioni di conformità.

Richiedi esempio

Questa richiesta di esempio modifica le impostazioni di conformità per il bucket denominato `mybucket` . In questo esempio, gli oggetti in `mybucket` verranno ora conservati per due anni (1.051.200 minuti) anziché uno, a partire dal momento in cui l'oggetto viene inserito nella griglia. Non esiste alcun vincolo legale su questo

secchio. Ogni oggetto verrà automaticamente eliminato dopo due anni.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrizione
Periodo di conservazioneMinuti	Durata del periodo di conservazione degli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene inserito nella griglia. **Importante** Quando si specifica un nuovo valore per RetentionPeriodMinutes, è necessario specificare un valore uguale o maggiore del periodo di conservazione corrente del bucket. Dopo aver impostato il periodo di conservazione del bucket, non è possibile diminuire tale valore; è possibile solo aumentarlo.
LegalHold	• Vero: questo bucket è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket non possono essere eliminati finché non viene revocata la sospensione legale, anche se il periodo di conservazione è scaduto. • Falso: questo bucket non è attualmente sottoposto a blocco legale. Gli oggetti in questo bucket possono essere eliminati alla scadenza del periodo di conservazione.
Eliminazione automatica	• Vero: gli oggetti in questo bucket verranno eliminati automaticamente alla scadenza del periodo di conservazione, a meno che il bucket non sia soggetto a conservazione legale. • Falso: gli oggetti in questo bucket non verranno eliminati automaticamente alla scadenza del periodo di conservazione. Se vuoi eliminarli, devi eliminarli manualmente.

Coerenza per le impostazioni di conformità

Quando si aggiornano le impostazioni di conformità per un bucket S3 con una richiesta di conformità del bucket PUT, StorageGRID tenta di aggiornare i metadati del bucket in tutta la griglia. Per impostazione predefinita, StorageGRID utilizza la coerenza **Strong-global** per garantire che tutti i siti dei data center e tutti i nodi di archiviazione che contengono metadati dei bucket abbiano coerenza di lettura dopo scrittura per le impostazioni di conformità modificate.

Se StorageGRID non riesce a raggiungere la coerenza **Strong-global** perché un sito del data center o più nodi di archiviazione in un sito non sono disponibili, il codice di stato HTTP per la risposta è `503 Service Unavailable.`

Se si riceve questa risposta, è necessario contattare l'amministratore della rete per assicurarsi che i servizi di archiviazione richiesti siano resi disponibili il prima possibile. Se l'amministratore della rete non è in grado di rendere disponibili sufficienti nodi di archiviazione in ciascun sito, il supporto tecnico potrebbe consigliarti di riprovare la richiesta non riuscita forzando la coerenza **Strong-site**.

> Non forzare mai la coerenza **Strong-site** per la conformità del bucket PUT, a meno che non ti sia stato chiesto di farlo dal supporto tecnico e a meno che tu non comprenda le potenziali conseguenze dell'utilizzo di questo livello.

Quando la coerenza viene ridotta a **Strong-site**, StorageGRID garantisce che le impostazioni di conformità aggiornate avranno coerenza di lettura dopo scrittura solo per le richieste client all'interno di un sito. Ciò significa che il sistema StorageGRID potrebbe avere temporaneamente più impostazioni incoerenti per questo bucket finché tutti i siti e i nodi di archiviazione non saranno disponibili. Impostazioni incoerenti possono dare luogo a comportamenti inaspettati e indesiderati. Ad esempio, se si sottopone un bucket a un blocco legale e si impone una minore coerenza, le precedenti impostazioni di conformità del bucket (ovvero il blocco legale) potrebbero continuare a essere valide in alcuni siti di data center. Di conseguenza, gli oggetti che ritieni siano in sospeso a fini legali potrebbero essere eliminati alla scadenza del periodo di conservazione, dall'utente o tramite l'eliminazione automatica, se abilitata.

Per forzare l'uso della coerenza **Strong-site**, riemettere la richiesta di conformità del bucket PUT e includere `Consistency-Control` Intestazione della richiesta HTTP, come segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Risposte di errore

- Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è `404 Not Found`.
- Se `RetentionPeriodMinutes` nella richiesta è inferiore al periodo di conservazione corrente del bucket, il codice di stato HTTP è `400 Bad Request`.

Informazioni correlate

"Obsoleto: modifiche alla richiesta PUT Bucket per conformità"

Criteri di accesso a bucket e gruppi

Utilizzare criteri 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 di policy dell'API REST S3. Le policy di accesso per l'API S3 sono scritte in JSON.

Panoramica della politica di accesso

StorageGRID supporta due tipi di criteri di accesso.

- **Politiche bucket**, gestite tramite le operazioni API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy oppure tramite l'API Tenant Manager o Tenant Management. I criteri dei bucket sono associati ai bucket e sono quindi configurati per controllare l'accesso degli utenti nell'account proprietario del bucket o di altri account al bucket e agli oggetti in esso contenuti. Una policy basata su bucket si applica a un solo bucket e, possibilmente, a più gruppi.
- **Criteri di gruppo**, configurati tramite Tenant Manager o Tenant Management API. I criteri di gruppo sono associati a un gruppo nell'account e sono quindi configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Un criterio di gruppo si applica a un solo gruppo e, possibilmente, a più bucket.

> Non vi è alcuna differenza di priorità tra i criteri di gruppo e quelli di bucket.

I criteri di gruppo e bucket StorageGRID seguono una grammatica specifica definita da Amazon. All'interno di ogni policy è presente una serie di dichiarazioni di policy e ciascuna dichiarazione contiene i seguenti elementi:

- ID dichiarazione (Sid) (facoltativo)
- Effetto
- Principale/Non Principale
- Risorsa/Non Risorsa
- Azione/Non azione
- Condizione (facoltativa)

Le istruzioni di policy vengono create utilizzando questa struttura per specificare le autorizzazioni: Concedi <Effetto> per consentire/negare a <Principale> di eseguire <Azione> su <Risorsa> quando si applica <Condizione>.

Ogni elemento della policy viene utilizzato per una funzione specifica:

Elemento	Descrizione
Sid	L'elemento Sid è facoltativo. Il Sid è inteso solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID .
Effetto	Utilizzare l'elemento Effetto per stabilire se le operazioni specificate sono consentite o negate. È necessario identificare le operazioni consentite (o negate) sui bucket o sugli oggetti utilizzando le parole chiave dell'elemento Azione supportate.

Elemento	Descrizione
Principale/Non Principale	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. È sufficiente specificare l'elemento Principal in un criterio bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito.
Risorsa/Non Risorsa	L'elemento Risorsa identifica bucket e oggetti. È possibile concedere o negare autorizzazioni a bucket e oggetti utilizzando l'Amazon Resource Name (ARN) per identificare la risorsa.
Azione/Non azione	Gli elementi Azione ed Effetto 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 autorizzazioni specifiche, ma è possibile utilizzare la negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio.
Condizione	L'elemento Condizione è facoltativo. Le condizioni consentono di creare espressioni per determinare quando applicare una policy.

Nell'elemento Azione, è possibile utilizzare il carattere jolly (*) per specificare tutte le operazioni o un sottoinsieme di operazioni. Ad esempio, questa azione corrisponde ad autorizzazioni quali s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

Nell'elemento Risorsa 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, tranne che per impostare l'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, si imposta il carattere jolly (*) come valore Principale.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

Nell'esempio seguente, l'istruzione utilizza gli elementi Effetto, Principale, Azione e Risorsa. Questo esempio mostra un'istruzione completa della policy del bucket che utilizza l'effetto "Consenti" per fornire ai Principals, il gruppo di amministrazione `federated-group/admin` e il gruppo finanziario `federated-group/finance` , autorizzazioni per eseguire l'azione `s3:ListBucket` sul secchio denominato `mybucket` e l'azione `s3:GetObject` su tutti gli oggetti all'interno di quel contenitore.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

Il criterio del bucket ha un limite di dimensione di 20.480 byte, mentre il criterio del gruppo ha un limite di dimensione di 5.120 byte.

Coerenza per le politiche

Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Quando un criterio di gruppo diventa coerente, le modifiche potrebbero richiedere altri 15 minuti per diventare effettive, a causa della memorizzazione nella cache dei criteri. Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri dei bucket sono fortemente coerenti.

Se necessario, è possibile modificare le garanzie di coerenza per gli aggiornamenti dei criteri dei bucket. Ad esempio, potresti voler rendere disponibile una modifica ai criteri di un bucket durante un'interruzione del sito.

In questo caso, è possibile impostare il `Consistency-Control` intestazione nella richiesta PutBucketPolicy oppure puoi utilizzare la richiesta di coerenza PUT Bucket. Quando un criterio di bucket diventa coerente, le modifiche potrebbero richiedere altri 8 secondi per diventare effettive, a causa della memorizzazione nella cache dei criteri.

> Se si imposta la coerenza su un valore diverso per risolvere una situazione temporanea, assicurarsi di ripristinare l'impostazione a livello di bucket al valore originale al termine dell'operazione. In caso contrario, tutte le future richieste di bucket utilizzeranno l'impostazione modificata.

Utilizzare ARN nelle dichiarazioni di policy

Nelle dichiarazioni di policy, l'ARN viene utilizzato negli elementi Principal e Resource.

- Utilizzare questa sintassi per specificare l'ARN della risorsa S3:

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

- Utilizzare questa sintassi per specificare l'ARN della risorsa 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 trovare la corrispondenza con zero o più caratteri all'interno della chiave dell'oggetto.
- I caratteri internazionali, che possono essere specificati nella chiave dell'oggetto, devono essere codificati utilizzando JSON UTF-8 o sequenze di escape JSON \u. La codifica percentuale non è supportata.

  "Sintassi URN RFC 2141"

  Il corpo della richiesta HTTP per l'operazione PutBucketPolicy deve essere codificato con charset=UTF-8.

Specificare le risorse in una policy

Nelle istruzioni dei criteri, è possibile utilizzare l'elemento Risorsa per specificare il bucket o l'oggetto per cui sono concesse o negate le autorizzazioni.

- Ogni dichiarazione di policy richiede un elemento Risorsa. In una policy, le risorse sono indicate dall'elemento `Resource` , o in alternativa, `NotResource` per l'esclusione.
- È possibile specificare le risorse con un ARN di risorsa S3. Per esempio:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- È anche possibile utilizzare variabili di policy all'interno della chiave dell'oggetto. Per esempio:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Il valore della risorsa può specificare un bucket che non esiste ancora al momento della creazione di un criterio di gruppo.

Specificare i principi in una policy

Utilizzare l'elemento Principal per identificare l'utente, il gruppo o l'account tenant a cui è consentito/negato

l'accesso alla risorsa in base all'istruzione di policy.

- Ogni istruzione di policy in una policy di bucket deve includere un elemento Principal. Le istruzioni di policy in un criterio di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principale.
- In una policy, i mandanti sono indicati dall'elemento "Manager" o, in alternativa, "NotManager" 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 nell'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 un gruppo federato specifico ("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 dell'utente anziché il 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 eliminato. Se un nuovo Alex si unisce all'organizzazione e gli viene assegnato lo stesso `Alex` nome utente, il nuovo utente

potrebbe ereditare involontariamente i permessi concessi all'utente originale.

- Il valore principale può specificare un nome di gruppo/utente che non esiste ancora al momento della creazione di un criterio bucket.

Specificare le autorizzazioni in una policy

In una policy, l'elemento Azione viene utilizzato per concedere/negare le autorizzazioni a una risorsa. Esiste una serie di autorizzazioni che è possibile specificare in una policy, contrassegnate dall'elemento "Azione" o, in alternativa, "NonAzione" per l'esclusione. Ciascuno di questi elementi è mappato a specifiche operazioni dell'API REST S3.

Nelle tabelle sono elencate le autorizzazioni che si applicano ai bucket e le autorizzazioni che si applicano agli oggetti.

> Amazon S3 ora utilizza l'autorizzazione s3:PutReplicationConfiguration per entrambe le azioni PutBucketReplication e DeleteBucketReplication. StorageGRID utilizza autorizzazioni separate per ogni azione, in linea con le specifiche originali di Amazon S3.

> Un'operazione di eliminazione viene eseguita quando si utilizza un'istruzione put per sovrascrivere un valore esistente.

Autorizzazioni applicabili ai bucket

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:CreaBucket	CreaBucket	Sì. **Nota**: utilizzare solo nei criteri di gruppo.
s3:EliminaBucket	EliminaBucket	
s3:DeleteBucketMetadataNotification	ELIMINA la configurazione della notifica dei metadati del bucket	SÌ
s3:EliminaBucketPolicy	DeleteBucketPolicy	
s3:EliminaConfigurazioneReplicazione	DeleteBucketReplication	Sì, autorizzazioni separate per PUT e DELETE
s3:GetBucketAcl	OttieniBucketAcl	
s3:GetBucketCompliance	Conformità GET Bucket (obsoleto)	SÌ
s3:GetBucketConsistency	OTTIENI la coerenza del bucket	SÌ
s3:GetBucketCORS	GetBucketCors	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:Ottieni configurazione crittografia	Ottieni crittografia dei bucket	
s3:GetBucketLastAccessTime	GET Ora dell'ultimo accesso al bucket	SÌ
s3:OttieniPosizioneBucket	OttieniPosizioneBucket	
s3:GetBucketMetadataNotification	Configurazione della notifica dei metadati del bucket GET	SÌ
s3:OttieniNotificaBucket	Configurazione di notifica di GetBucket	
s3:GetBucketObjectLockConfiguration	Ottieni configurazione blocco oggetto	
s3:GetBucketPolicy	OttieniPoliticaBucket	
s3:OttieniTaggingBucket	OttieniBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:OttieniConfigurazioneReplicazione	OttieniReplicazioneBucket	
s3:ElencaTuttiIMieBucket	• ListBuckets • Utilizzo dello spazio di archiviazione GET	Sì, per l'utilizzo dello spazio di archiviazione GET. **Nota**: utilizzare solo nei criteri di gruppo.
s3:ElencoBucket	• ElencoOggetti • HeadBucket • Ripristina oggetto	
s3:ListBucketMultipartUploads	• Caricamenti multiparte di List • Ripristina oggetto	
s3:ListBucketVersions	Versioni GET Bucket	
s3:PutBucketCompliance	Conformità al bucket PUT (obsoleto)	SÌ
s3:PutBucketConsistency	PUT Consistenza del secchio	SÌ

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	Ora dell'ultimo accesso al bucket PUT	SÌ
s3:PutBucketMetadataNotification	Configurazione della notifica dei metadati del bucket PUT	SÌ
s3:PutBucketNotification	Configurazione della notifica PutBucket	
s3:PutBucketObjectLockConfiguration	• CreateBucket con il `x-amz-bucket-object-lock-enabled: true` intestazione della richiesta (richiede anche l'autorizzazione s3:CreateBucket) • PutObjectLockConfiguration	
s3:PoliticaPutBucket	PutBucketPolicy	
s3:PutBucketTagging	• EliminaBucketTagging† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	• DeleteBucketLifecycle† • Configurazione del ciclo di vita di PutBucket	
s3:PutReplicationConfiguration	PutBucketReplication	Sì, autorizzazioni separate per PUT e DELETE

Autorizzazioni applicabili agli oggetti

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:AnnullaCaricamentoMultipart	• Annulla caricamento multiparte • Ripristina oggetto	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:BypassGovernanceRetention	• EliminaOggetto • EliminaOggetti • PutObjectRetention	
s3:EliminaOggetto	• EliminaOggetto • EliminaOggetti • Ripristina oggetto	
s3:EliminaTaggingOggetto	DeleteObjectTagging	
s3:EliminaObjectVersionTagging	DeleteObjectTagging (una versione specifica dell'oggetto)	
s3:EliminaVersioneOggetto	DeleteObject (una versione specifica dell'oggetto)	
s3:OttieniOggetto	• OttieniOggetto • HeadObject • Ripristina oggetto • SelezionaOggettoContenuto	
s3:GetObjectAcl	OttieniOggettoAcl	
s3:GetObjectLegalHold	OttieniOggettoLegaleHold	
s3:OttieniRitenzioneOggetto	Ottieni conservazione oggetto	
s3:OttieniTaggingOggetto	OttieniTaggingOggetto	
s3:GetObjectVersionTagging	GetObjectTagging (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GetObject (una versione specifica dell'oggetto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	

Permessi	Operazioni API REST S3	Personalizzato per StorageGRID
s3:PutObject	• MettiOggetto • CopiaOggetto • Ripristina oggetto • CreaCaricamentoMultiparte • Caricamento multiparte completo • CaricaParte • CaricaParteCopia	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (una versione specifica dell'oggetto)	
s3:PutOverwriteObject	• MettiOggetto • CopiaOggetto • PutObjectTagging • DeleteObjectTagging • Caricamento multiparte completo	SÌ
s3:RipristinaOggetto	Ripristina oggetto	

Utilizzare 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 possibili impostazioni per questa autorizzazione includono:

- **Consenti**: il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega**: Il client non può sovrascrivere un oggetto. Se impostato 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 i tag degli oggetti S3 non possono essere sovrascritti.
    - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
    - Se è abilitato il controllo delle versioni S3, l'impostazione Nega impedisce alle operazioni

PutObjectTagging o DeleteObjectTagging di modificare il TagSet per un oggetto e le sue 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 che si avrebbe se fosse impostato Consenti.

> Se l'attuale policy S3 consente la sovrascrittura e l'autorizzazione PutOverwriteObject è impostata su Nega, il client non può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o i tag degli oggetti. Inoltre, se è selezionata la casella di controllo **Impedisci modifica client** (**CONFIGURAZIONE** > **Impostazioni di sicurezza** > **Rete e oggetti**), tale impostazione sostituisce l'impostazione dell'autorizzazione PutOverwriteObject.

Specificare le condizioni in una policy

Le condizioni definiscono quando una politica entrerà in vigore. Le condizioni sono costituite da operatori e coppie chiave-valore.

Le condizioni utilizzano coppie chiave-valore per la valutazione. Un elemento Condizione può contenere più condizioni e ogni condizione può contenere più coppie chiave-valore. Il blocco di condizione utilizza il seguente formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Nell'esempio seguente, la condizione IpAddress utilizza la chiave di condizione SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operatori di condizione supportati

Gli operatori condizionali sono classificati come segue:

- Corda
- Numerico
- Booleano
- indirizzo IP
- Controllo nullo

Operatori di condizione	Descrizione
StringEquals	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (con distinzione tra maiuscole e minuscole).
Stringa non uguale	Confronta una chiave con un valore stringa in base alla corrispondenza negata (sensibile alle maiuscole e alle minuscole).
StringEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora la distinzione tra maiuscole e minuscole).
StringNotEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora la distinzione tra maiuscole e minuscole).
StringLike	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (con distinzione tra maiuscole e minuscole). Può includere i caratteri jolly * e ?.
Stringa non piace	Confronta una chiave con un valore stringa in base alla corrispondenza negata (sensibile alle maiuscole e alle minuscole). Può includere i caratteri jolly * e ?.
NumericEquals	Confronta una chiave con un valore numerico in base alla corrispondenza esatta.
NumericoNonUguale	Confronta una chiave con un valore numerico in base alla corrispondenza negata.
NumericoMaggioreDi	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore di".
NumericoMaggioreDiUguale	Confronta una chiave con un valore numerico in base alla corrispondenza "maggiore o uguale a".
NumericoMenoDi	Confronta una chiave con un valore numerico in base alla corrispondenza "minore di".
NumericoMinoreUguale	Confronta una chiave con un valore numerico in base alla corrispondenza "minore o uguale".
Bool	Confronta una chiave con un valore booleano in base alla corrispondenza "vero o falso".
Indirizzo IP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP.
NonIndirizzoIP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata.

Operatori di condizione	Descrizione
Nullo	Controlla se una chiave di condizione è presente nel contesto della richiesta corrente.

Chiavi di condizione supportate

Chiavi di condizione	Azioni	Descrizione
aws:SourceIp	operatori IP	Verrà confrontato con l'indirizzo IP da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti. **Nota:** se la richiesta S3 è stata inviata tramite il servizio Load Balancer sui nodi amministrativi e sui nodi gateway, questa verrà confrontata con l'indirizzo IP a monte del servizio Load Balancer. **Nota**: se viene utilizzato un bilanciatore del carico di terze parti non trasparente, questo verrà confrontato con l'indirizzo IP di tale bilanciatore del carico. Qualunque `X-Forwarded-For` l'intestazione verrà ignorata perché non è possibile accertarne la validità.
aws:nome utente	Risorsa/Identità	Verrà confrontato con il nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti.
s3:delimitatore	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions.

Chiavi di condizione	Azioni	Descrizione
s3:ExistingObjectTag/<chiave-tag>	s3:EliminaTaggingOggetto s3:EliminaObjectVersionTagging s3:OttieniOggetto s3:GetObjectAcl 3: Ottieni tag oggetto s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Richiederà che l'oggetto esistente abbia la chiave e il valore del tag specifici.
s3:max-chiavi	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions.
s3:giorni di conservazione rimanenti del blocco dell'oggetto	s3:PutObject	Confronta con la data di conservazione specificata in `x-amz-object-lock-retain-until-date` intestazione della richiesta o calcolata dal periodo di conservazione predefinito del bucket per assicurarsi che questi valori siano compresi nell'intervallo consentito per le seguenti richieste: • MettiOggetto • CopiaOggetto • CreaCaricamentoMultiparte
s3:giorni di conservazione rimanenti del blocco dell'oggetto	s3:PutObjectRetention	Confronta con la retain-until-date specificata nella richiesta PutObjectRetention per garantire che rientri nell'intervallo consentito.

Chiavi di condizione	Azioni	Descrizione
s3:prefisso	s3:ListBucket e s3:permessi ListBucketVersions	Verrà confrontato con il parametro prefisso specificato in una richiesta ListObjects o ListObjectVersions.
s3:RequestObjectTag/<chiave-tag>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Richiederà una chiave e un valore tag specifici quando la richiesta dell'oggetto include il tagging.

Specificare le variabili in una policy

È possibile utilizzare le variabili nelle policy per popolare le informazioni sulle policy quando sono disponibili. È possibile utilizzare le variabili di policy in `Resource` elemento e nei confronti di stringhe in `Condition` elemento.

In questo esempio, la variabile `${aws:username}` fa parte dell'elemento Risorsa:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In questo esempio, la variabile `${aws:username}` fa parte del valore della condizione nel blocco di condizioni:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variabile	Descrizione
`${aws:SourceIp}`	Utilizza la chiave SourceIp come variabile fornita.
`${aws:username}`	Utilizza la chiave nome utente come variabile fornita.
`${s3:prefix}`	Utilizza la chiave del prefisso specifico del servizio come variabile fornita.
`${s3:max-keys}`	Utilizza la chiave max-keys specifica del servizio come variabile fornita.

Variabile	Descrizione
`${*}`	Carattere speciale. Utilizza il carattere come carattere letterale *.
`${?}`	Carattere speciale. Utilizza il carattere come carattere ? letterale.
`${$}`	Carattere speciale. Utilizza il carattere come carattere $ letterale.

Creare politiche che richiedono una gestione speciale

Talvolta una policy può concedere autorizzazioni pericolose per la sicurezza o per il proseguimento delle operazioni, ad esempio bloccando l'utente root dell'account. L'implementazione dell'API REST S3 StorageGRID è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

Descrizione della politica	Tipo di polizza	Comportamento di Amazon	Comportamento StorageGRID
Nega a te stesso qualsiasi autorizzazione all'account root	Secchio	Valido e applicato, ma l'account utente root mantiene l'autorizzazione per tutte le operazioni dei criteri del bucket S3	Stesso
Nega a te stesso qualsiasi autorizzazione all'utente/gruppo	Gruppo	Valido e applicato	Stesso
Consentire qualsiasi autorizzazione a un gruppo di account esteri	Secchio	Principale non valido	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito quando consentito da una policy
Consentire a un account esterno root o utente qualsiasi autorizzazione	Secchio	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito quando consentito da una policy	Stesso

Descrizione della politica	Tipo di polizza	Comportamento di Amazon	Comportamento StorageGRID
Consenti a tutti i permessi per tutte le azioni	Secchio	Valido, ma le autorizzazioni per tutte le operazioni di policy del bucket S3 restituiscono un errore 405 Metodo non consentito per l'account esterno root e gli utenti	Stesso
Nega a tutti i permessi per tutte le azioni	Secchio	Valido e applicato, ma l'account utente root mantiene l'autorizzazione per tutte le operazioni dei criteri del bucket S3	Stesso
Il principale è un utente o un gruppo inesistente	Secchio	Principale non valido	Valido
La risorsa è un bucket S3 inesistente	Gruppo	Valido	Stesso
Principal è un gruppo locale	Secchio	Principale non valido	Valido
La policy concede a un account non proprietario (inclusi gli account anonimi) l'autorizzazione a inserire oggetti.	Secchio	Valido. Gli oggetti sono di proprietà dell'account del creatore e la policy del bucket non si applica. L'account del creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL degli oggetti.	Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la politica dei 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. È possibile configurare i bucket WORM per consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione di contenuti esistenti. Utilizzare uno degli approcci descritti qui.

Per garantire che le sovrascritture vengano sempre negate, puoi:

- Da Grid Manager, vai su **CONFIGURAZIONE** > **Sicurezza** > **Impostazioni di sicurezza** > **Rete e oggetti** e seleziona la casella di controllo **Impedisci modifiche client**.
- Applicare le seguenti regole e policy S3:
  - Aggiungere un'operazione PutOverwriteObject DENY al criterio S3.
  - Aggiungere un'operazione DeleteObject DENY al criterio S3.
  - Aggiungere un'operazione PutObject ALLOW al criterio S3.

L'impostazione di DeleteObject su DENY in un criterio S3 non impedisce a ILM di eliminare oggetti quando esiste una regola come "zero copie dopo 30 giorni".

Anche quando vengono applicate tutte queste regole e policy, non proteggono dalle scritture simultanee (vedere Situazione A). 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 (protette contro)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informazioni correlate

- "Come le regole StorageGRID ILM gestiscono gli oggetti"
- "Criteri di esempio per i bucket"
- "Criteri di gruppo di esempio"
- "Gestire gli oggetti con ILM"
- "Utilizzare un account tenant"

Criteri di esempio per i bucket

Utilizzare gli esempi in questa sezione per creare policy di accesso StorageGRID per i bucket.

I criteri dei bucket specificano le autorizzazioni di accesso per il bucket a cui è associato il criterio. È possibile configurare un criterio bucket utilizzando l'API S3 PutBucketPolicy tramite uno di questi strumenti:

- "Responsabile degli inquilini" .
- AWS CLI utilizzando questo comando (fare riferimento a"Operazioni sui bucket"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Esempio: consentire a tutti l'accesso in sola lettura a un bucket

In questo esempio, a tutti, incluso l'utente anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni saranno negate. Si noti che questa policy potrebbe non essere particolarmente utile perché nessuno, eccetto l'account root, ha i permessi per

scrivere 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 di elencare il bucket ed eseguire operazioni GetObject sugli oggetti nel bucket a partire da `shared/` prefisso della chiave dell'oggetto.

> In StorageGRID, gli oggetti creati da un account non proprietario (inclusi gli account anonimi) sono di proprietà dell'account proprietario del bucket. A questi oggetti si applica la policy bucket.

```
{
  "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 al gruppo specificato

In questo esempio, a tutti, incluso l'utente anonimo, è consentito elencare il bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket, mentre solo gli utenti appartenenti al gruppo `Marketing` nell'account specificato 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 è nell'intervallo IP

In questo esempio, a tutti, compresi gli utenti anonimi, è consentito elencare il bucket ed eseguire qualsiasi operazione sugli oggetti 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 negate e tutte le richieste al di fuori dell'intervallo IP verranno negate.

```
{
  "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 a un utente federato specificato

In questo esempio, all'utente federato Alex è consentito l'accesso completo a `examplebucket` secchio e i suoi oggetti. A tutti gli altri utenti, compreso 'root', viene esplicitamente negata qualsiasi operazione. Si noti tuttavia che a 'root' non vengono mai negati i permessi 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` L'effetto di PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e il tagging dell'oggetto S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Criteri di gruppo di esempio

Utilizzare gli esempi in questa sezione per creare criteri di accesso StorageGRID per i gruppi.

I criteri di gruppo specificano le autorizzazioni di accesso per il gruppo a cui è associato il criterio. Non c'è `Principal` elemento nella politica perché è implicito. I criteri di gruppo vengono configurati tramite Tenant Manager o API.

Esempio: impostare i criteri di gruppo utilizzando Tenant Manager

Quando aggiungi o modifichi un gruppo in Tenant Manager, puoi selezionare un criterio di gruppo per determinare quali autorizzazioni di accesso S3 avranno i membri di questo gruppo. Vedere "Creare gruppi per un tenant S3" .

- **Nessun accesso S3**: opzione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non venga concesso tramite un criterio bucket. Se si seleziona questa opzione, per impostazione predefinita solo l'utente root avrà accesso alle risorse S3.
- **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 oggetti e leggere dati, metadati e tag degli oggetti. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Non puoi modificare questa stringa.
- **Accesso completo**: gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo con accesso completo. Non puoi modificare questa stringa.
- **Mitigazione del ransomware**: questa policy di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare definitivamente gli oggetti dai bucket in cui è abilitato il controllo delle versioni degli oggetti.

  Gli utenti Tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono ignorare questo criterio di gruppo. Limitare l'autorizzazione Gestisci tutti i bucket agli utenti attendibili e utilizzare l'autenticazione a più fattori (MFA) laddove disponibile.

- **Personalizzato**: agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

Esempio: consentire al gruppo l'accesso completo 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 venga esplicitamente negato dalla policy del bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Esempio: consentire al gruppo l'accesso 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 venga esplicitamente negato dai criteri del bucket. Ad esempio, gli utenti di questo gruppo possono elencare oggetti e leggere dati, metadati e tag degli oggetti.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Esempio: consentire ai membri del gruppo l'accesso completo solo alla loro "cartella" in un bucket

In questo esempio, ai membri del gruppo è consentito solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Si noti che quando si determina la privacy di queste cartelle, è necessario prendere in considerazione le autorizzazioni di accesso provenienti da altri criteri di gruppo e dai criteri del bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Operazioni S3 tracciate nei registri di controllo

I messaggi di controllo vengono generati dai servizi StorageGRID e archiviati in file di registro di testo. È possibile esaminare i messaggi di controllo specifici di S3 nel registro di controllo per ottenere dettagli sulle operazioni di bucket e oggetti.

Operazioni del bucket monitorate nei log di controllo

- CreaBucket
- EliminaBucket
- DeleteBucketTagging
- EliminaOggetti
- OttieniBucketTagging
- HeadBucket
- ElencoOggetti
- ListObjectVersions
- Conformità del bucket PUT
- PutBucketTagging
- PutBucketVersioning

Operazioni sugli oggetti tracciate nei registri di controllo

- Caricamento multiparte completo
- CopiaOggetto
- EliminaOggetto
- OttieniOggetto
- HeadObject
- MettiOggetto
- Ripristina oggetto
- SelezionaOggetto
- UploadPart (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)
- UploadPartCopy (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)

Informazioni correlate

- "Accedi al file di registro di controllo"
- "Il cliente scrive messaggi di audit"
- "Il cliente ha letto i messaggi di controllo"

Utilizzare Swift REST API (fine del ciclo di vita)

Utilizzare Swift REST API

Il supporto per l'API Swift ha raggiunto la fine del suo ciclo di vita e verrà rimosso in una versione futura.

I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere "StorageGRID 11.8: utilizzare Swift REST API" .

Informazioni sul copyright

Informazioni sul marchio commerciale