Gestire i bucket S3

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-118/tenant/creating-s3-bucket.html on November 04, 2025. Always check docs.netapp.com for the latest.

Sommario

Gestire i bucket S3 . . . 1
- Creare un bucket S3 . . . 1
  - Accedere alla procedura guidata . . . 1
  - Inserire i dettagli . . . 1
  - Gestire le impostazioni degli oggetti . . . 2
- Visualizza i dettagli del bucket . . . 3
- Applicare un tag di criterio ILM a un bucket . . . 5
- Gestire la coerenza del bucket . . . 6
  - Linee guida per la coerenza della benna . . . 6
    - modificare la coerenza del bucket . . . 6
  - Cosa accade quando si modificano le impostazioni della benna . . . 7
- Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso . . . 8
- Modificare la versione degli oggetti per un bucket . . . 10
- USA il blocco oggetti S3 per conservare gli oggetti . . . 11
  - Che cos'è il blocco oggetti S3? . . . 11
  - Workflow di blocco oggetti S3 . . . 13
  - Requisiti per i bucket con S3 Object Lock attivato . . . 14
  - Requisiti per gli oggetti nei bucket con S3 Object Lock attivato . . . 15
  - Ciclo di vita degli oggetti nei bucket con S3 Object Lock attivato . . . 15
  - Posso comunque gestire i bucket conformi alle versioni precedenti? . . . 15
- Aggiorna la conservazione predefinita del blocco oggetti S3 . . . 16
- Configurare la condivisione delle risorse tra origini (CORS) . . . 17
  - Abilitare il CORS per un bucket . . . 17
  - Modificare l'impostazione CORS . . . 18
  - Disattiva l'impostazione CORS . . . 18
- Eliminare gli oggetti nel bucket . . . 18
- Elimina bucket S3 . . . 21
- Utilizzare la console S3 . . . 22

Gestire i bucket S3

Creare un bucket S3

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

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone dell'accesso Root o di Manage All bucket (Gestisci tutti i bucket) "permesso". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

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

- Se si prevede di attivare il blocco oggetti S3 per un bucket, un amministratore della griglia ha attivato l'impostazione globale di blocco oggetti S3 per il sistema StorageGRID e sono stati esaminati i requisiti per i bucket e gli oggetti blocco oggetti S3. Vedere "USA il blocco oggetti S3 per conservare gli oggetti".

Accedere alla procedura guidata

Fasi

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

Inserire i dettagli

Fasi

1. Inserire i dettagli del bucket.

Campo	Descrizione
Nome bucket	Un nome per il bucket conforme alle seguenti regole: • Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). • Deve essere conforme al DNS. • Deve contenere almeno 3 e non più di 63 caratteri. • Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. • Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. Per ulteriori informazioni, consultare "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione del bucket". **Nota**: Non è possibile modificare il nome del bucket dopo averlo creato.

Campo	Descrizione
Regione	La regione del bucket. L'amministratore di StorageGRID gestisce le regioni disponibili. L'area di un bucket può influire sulla policy di protezione dei dati applicata agli oggetti. Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione. **Nota**: Non è possibile modificare l'area dopo aver creato il bucket.

2. Selezionare **continua**.

Gestire le impostazioni degli oggetti

Fasi

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

   Abilitare la versione degli oggetti se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto in base alle esigenze. Se il bucket verrà utilizzato per la replica cross-grid, è necessario attivare il controllo delle versioni degli oggetti.

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

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

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

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

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

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

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

Modalità di conservazione predefinita	Descrizione
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
Governance	• Utenti con `s3:BypassGovernanceRetention` l'autorizzazione può utilizzare `x-amz-bypass-governance-retention: true` richiedi intestazione per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

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

   Il **Default Retention Period** indica per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore compreso tra 1 e 36,500 giorni o tra 1 e 100 anni, inclusi.

4. Selezionare **Crea bucket**.

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

5. Facoltativamente, selezionare **Vai alla pagina dei dettagli del bucket** a. "visualizza i dettagli del bucket" ed eseguire una configurazione aggiuntiva.

Visualizza i dettagli del bucket

È possibile visualizzare i bucket nell'account tenant.

Prima di iniziare

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

Fasi

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

   Viene visualizzata la pagina Bucket.

2. Rivedere le informazioni di riepilogo per ciascun bucket.

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

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

Colonna	Descrizione
Nome	Il nome univoco del bucket, che non può essere modificato.
Funzionalità attivate	L'elenco delle funzioni attivate per il bucket.
Blocco oggetti S3	Se S3 Object Lock è attivato per il bucket. Questa colonna viene visualizzata solo se S3 Object Lock (blocco oggetti S3) è attivato per la griglia. Questa colonna mostra anche informazioni relative a qualsiasi bucket compatibile legacy.
Regione	La regione del bucket, che non può essere modificata.
Numero di oggetti	Il numero di oggetti in questo bucket. Quando gli oggetti vengono aggiunti o cancellati, questo valore potrebbe non essere aggiornato immediatamente. Se nei bucket è attivata la versione, le versioni degli oggetti non correnti vengono incluse in questo valore.
Spazio utilizzato	La dimensione logica di tutti gli oggetti nel bucket. La dimensione logica non include lo spazio effettivo richiesto per le copie replicate o codificate in cancellazione o per i metadati degli oggetti.
Data di creazione	La data e l'ora di creazione del bucket.

3. Per visualizzare i dettagli di un bucket specifico, selezionare il nome del bucket dalla tabella.

   Viene visualizzata la pagina dei dettagli del bucket. Da questa pagina, è possibile eseguire le seguenti attività se si dispone delle autorizzazioni richieste:

   - Configurare e gestire le opzioni bucket:
     - "Tag dei criteri ILM"
     - "Gestire la coerenza del bucket"
     - "Aggiornamenti dell'ora dell'ultimo accesso"
     - "Versione degli oggetti"
     - "Blocco oggetti S3"
     - "Ritenzione bucket predefinita"
   - Configurare l'accesso al bucket, ad esempio "Condivisione delle risorse tra origini (CORS)"
   - "Gestire i servizi della piattaforma" (Se consentito per il tenant), inclusa la replica di CloudMirror, le

notifiche degli eventi e l'integrazione della ricerca

- Attivare e. "gestire la replica cross-grid" (Se consentito dal tenant) per replicare gli oggetti acquisiti in questo bucket in un altro sistema StorageGRID
- Accedere a. "S3 Console" per gestire gli oggetti nel bucket
- "Elimina tutti gli oggetti in un bucket"
- "Eliminare un bucket" questo è già vuoto

Applicare un tag di criterio ILM a un bucket

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

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

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

Prima di iniziare

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

Fasi

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

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

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

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

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

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

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

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

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

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

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

Gestire la coerenza del bucket

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

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

Linee guida per la coerenza della benna

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

modificare la coerenza del bucket

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

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

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

Cosa accade quando si modificano le impostazioni della benna

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

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

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

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

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

- "Configurazione dei servizi della piattaforma: Integrazione di notifica, replica o ricerca"
- "Configurazione CORS"
- Modificare la coerenza della benna

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

Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso

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

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

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

A proposito di questa attività

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

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

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

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

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

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

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

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

Tipo di richiesta	Comportamento se l'ultimo tempo di accesso è disattivato (impostazione predefinita)		Comportamento se è attivata l'ultima ora di accesso	
	Ultimo aggiornamento dell'orario di accesso?	Oggetto aggiunto alla coda di valutazione ILM?	Ultimo aggiornamento dell'orario di accesso?	Oggetto aggiunto alla coda di valutazione ILM?
Richiesta di recuperare un oggetto, il relativo elenco di controllo degli accessi o i relativi metadati	No	No	Sì	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì	Sì	Sì
Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione
Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

Modificare la versione degli oggetti per un bucket

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

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Tutti i nodi storage sono disponibili.

A proposito di questa attività

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

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

Per ulteriori informazioni, vedere quanto segue:

- "Versione degli oggetti"
- "Regole e criteri ILM per gli oggetti con versione S3 (esempio 4)"
- "Modalità di eliminazione degli oggetti"

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

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

USA il blocco oggetti S3 per conservare gli oggetti

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

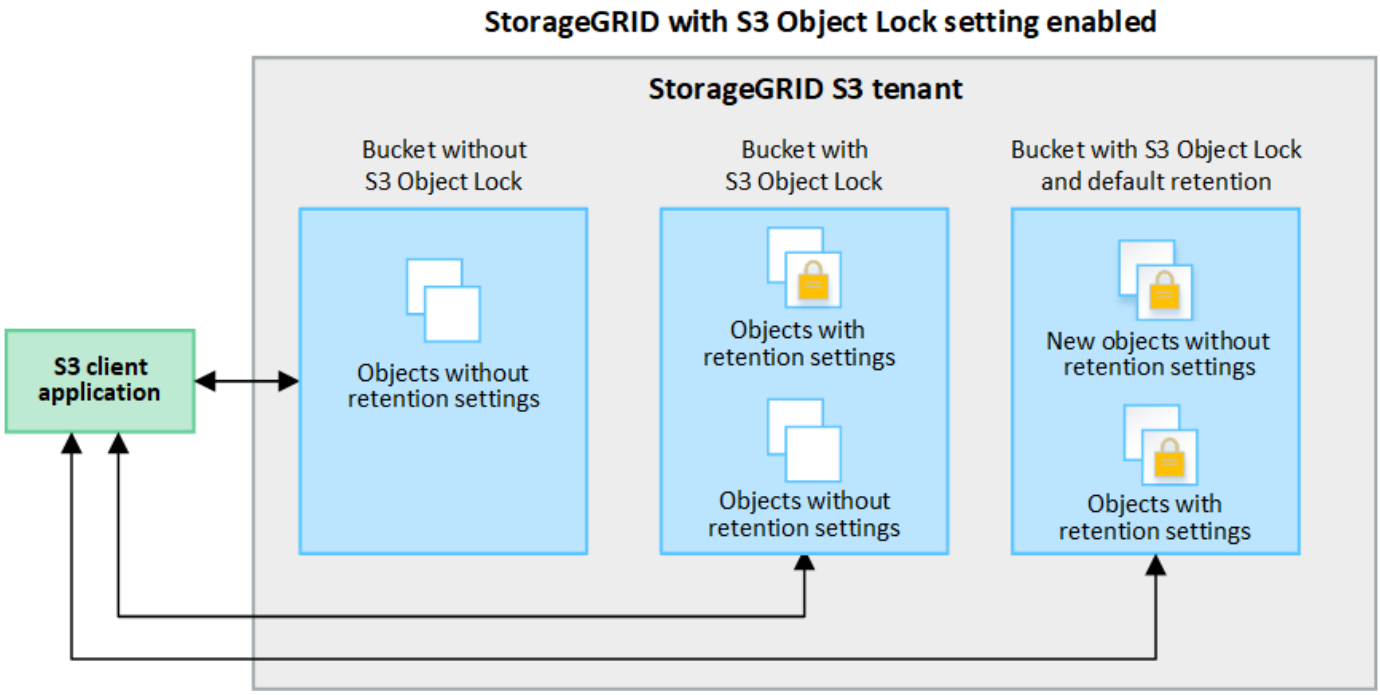
Che cos'è il blocco oggetti S3?

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

Come mostrato nella figura, quando l'impostazione globale S3 Object Lock è attivata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock attivato, è necessario il controllo della versione del bucket e viene attivato automaticamente.

Se un bucket ha attivato il blocco oggetti S3, le applicazioni client S3 possono specificare le impostazioni di conservazione per qualsiasi versione di oggetto salvata in quel bucket.

Inoltre, un bucket con S3 Object Lock attivato può avere una modalità di conservazione e un periodo di conservazione predefiniti. Le impostazioni predefinite si applicano solo agli oggetti aggiunti al bucket senza le proprie impostazioni di conservazione.



Modalità di conservazione

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

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

Impostazioni di conservazione per le versioni degli oggetti

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

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

indipendenti dalla conservazione fino alla data odierna.

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

Per ulteriori informazioni sulle impostazioni dell'oggetto, vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

Impostazione di conservazione predefinita per i bucket

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

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

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

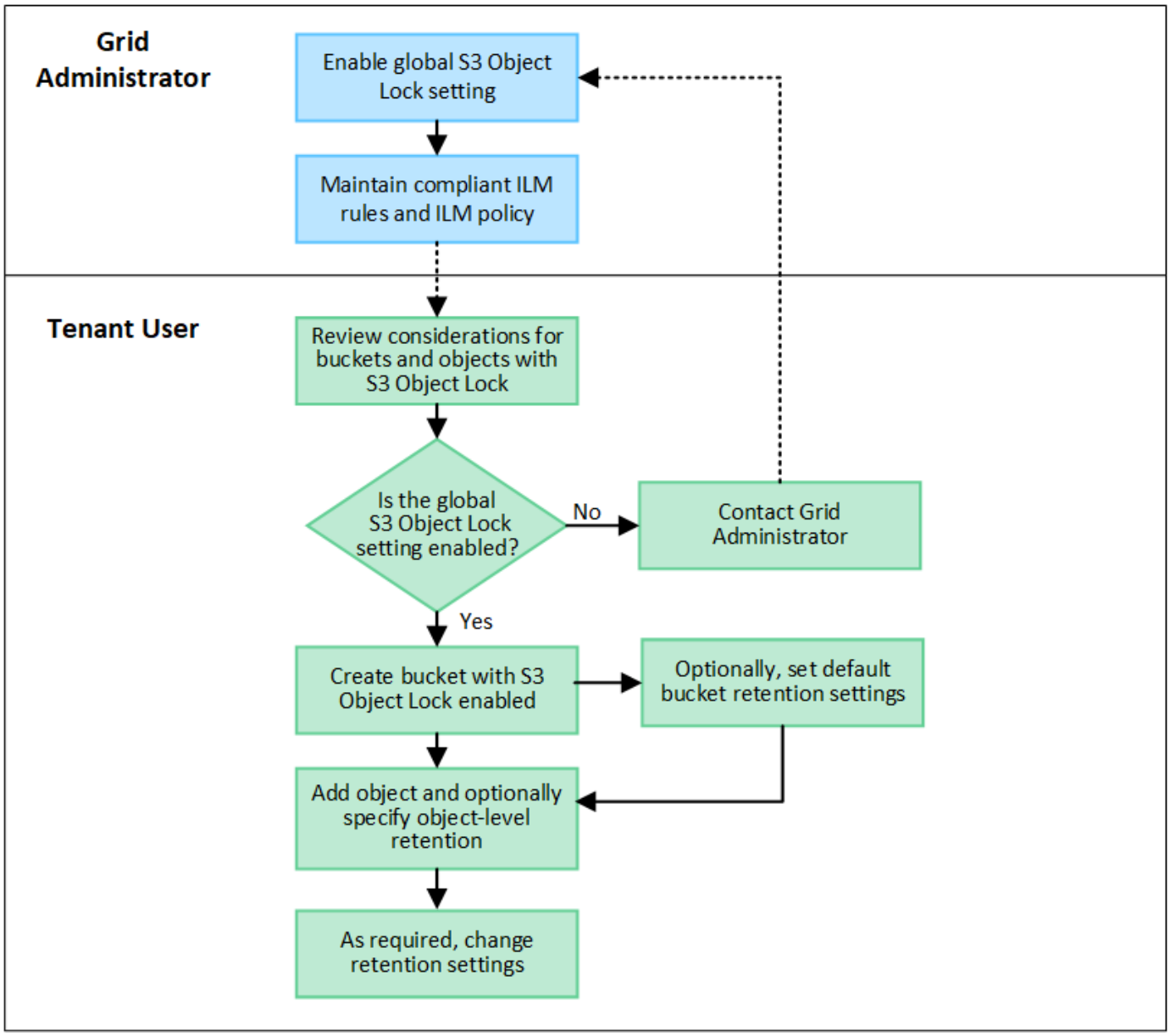
Vedere "Creare un bucket S3" e. "Aggiorna la conservazione predefinita del blocco oggetti S3".

Workflow di blocco oggetti S3

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

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

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



Requisiti per i bucket con S3 Object Lock attivato

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

- La replica di CloudMirror non è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

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

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

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

1. **Acquisizione oggetto**

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

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

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

2. **Conservazione ed eliminazione degli oggetti**

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

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

Posso comunque gestire i bucket conformi alle versioni precedenti?

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

Aggiorna la conservazione predefinita del blocco oggetti S3

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

Prima di iniziare

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

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

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

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

Modalità di conservazione predefinita	Descrizione
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
Governance	• Utenti con `s3:BypassGovernanceRetention` l'autorizzazione può utilizzare `x-amz-bypass-governance-retention: true` richiedi intestazione per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

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

   Il **Default Retention Period** indica per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore compreso tra 1 e 36,500 giorni o tra 1 e 100 anni, inclusi.

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

Configurare la condivisione delle risorse tra origini (CORS)

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

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

A proposito di questa attività

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

Abilitare il CORS per un bucket

Fasi

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

   Questo esempio mostra l'XML utilizzato per abilitare il CORS per un bucket S3. Questo XML consente a qualsiasi dominio di inviare richieste GET al bucket, ma consente solo il `http://www.example.com` Dominio per inviare richieste DI POST ed ELIMINAZIONE. Sono consentite tutte le intestazioni delle richieste.

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

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

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

Modificare l'impostazione CORS

Fasi

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

Disattiva l'impostazione CORS

Fasi

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

Eliminare gli oggetti nel bucket

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

Considerazioni e requisiti

Prima di eseguire questa procedura, tenere presente quanto segue:

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

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

- Durante l'eliminazione degli oggetti, lo stato del bucket è **eliminazione degli oggetti: Sola lettura**. In questo stato, non è possibile aggiungere nuovi oggetti al bucket.
- Una volta cancellati tutti gli oggetti, il bucket rimane in stato di sola lettura. È possibile eseguire una delle seguenti operazioni:
  - Riportare il bucket in modalità di scrittura e riutilizzarlo per nuovi oggetti
  - Eliminare il bucket
  - Mantenere il bucket in modalità di sola lettura per riservare il proprio nome per un utilizzo futuro
- Se in un bucket è attivata la versione oggetto, è possibile rimuovere i marcatori di eliminazione creati in StorageGRID 11,8 o versioni successive utilizzando le operazioni Elimina oggetti nel bucket.
- Se in un bucket è attivata la versione oggetto, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11,7 o versioni precedenti. Vedere le informazioni sull'eliminazione di oggetti in un bucket in "Modalità di eliminazione degli oggetti con versione S3".
- Se si utilizza "replica cross-grid", tenere presente quanto segue:
  - L'utilizzo di questa opzione non elimina alcun oggetto dal bucket dell'altra griglia.
  - Se si seleziona questa opzione per il bucket di origine, l'avviso **errore replica cross-grid** verrà attivato se si aggiungono oggetti al bucket di destinazione sull'altra griglia. Se non puoi garantire che nessuno aggiungerà oggetti al bucket sull'altra griglia, "disattiva la replica cross-grid" per quel bucket prima di eliminare tutti gli oggetti bucket.

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Autorizzazione di accesso root". Questa autorizzazione sovrascrive le impostazioni delle autorizzazioni nei criteri di gruppo o bucket.

Fasi

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

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

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

Menu delle azioni

a. Selezionare la casella di controllo per ciascun bucket da cui si desidera eliminare gli oggetti.

b. Selezionare **azioni** > **Elimina oggetti nel bucket**.

Pagina dei dettagli

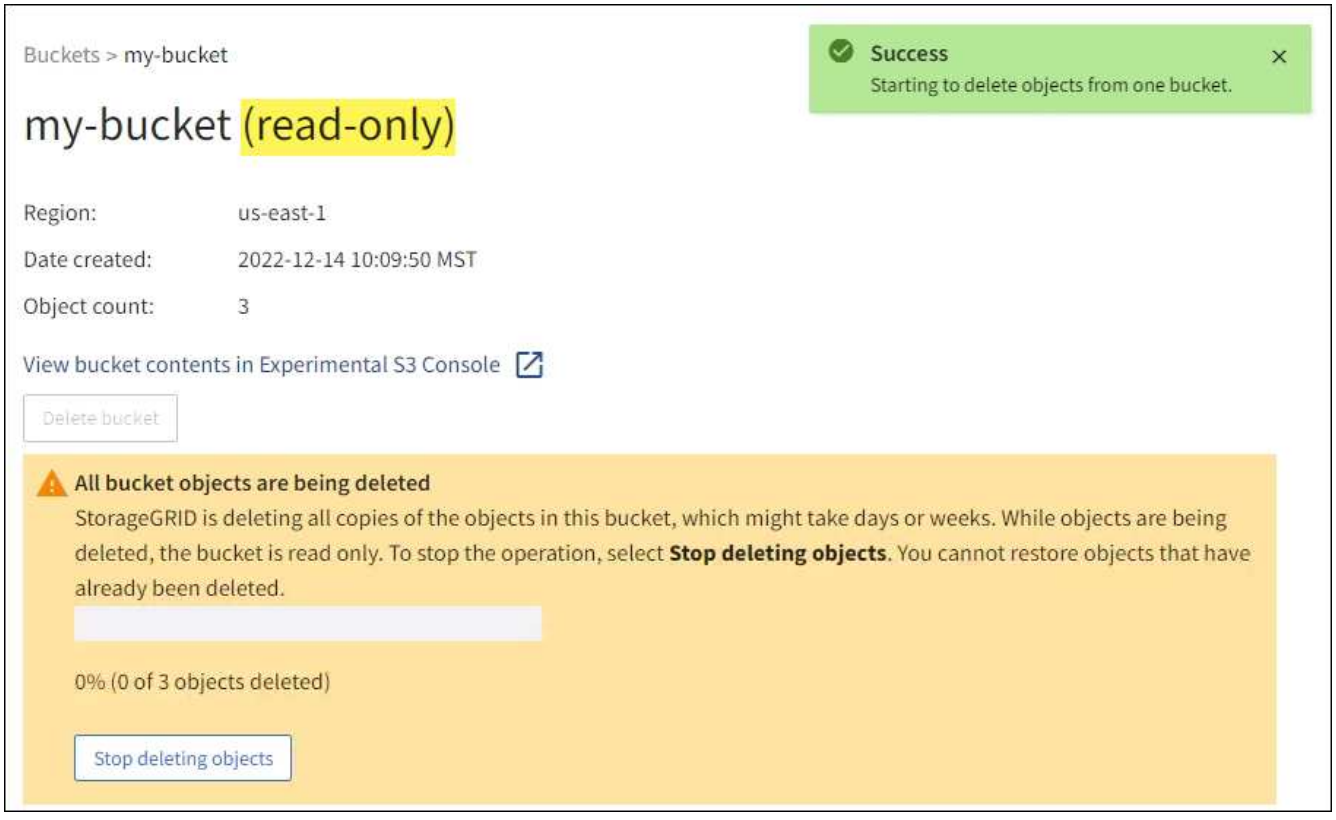
a. Selezionare il nome di un bucket per visualizzarne i dettagli.

b. Selezionare **Elimina oggetti nel bucket**.

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

   Dopo alcuni minuti:

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

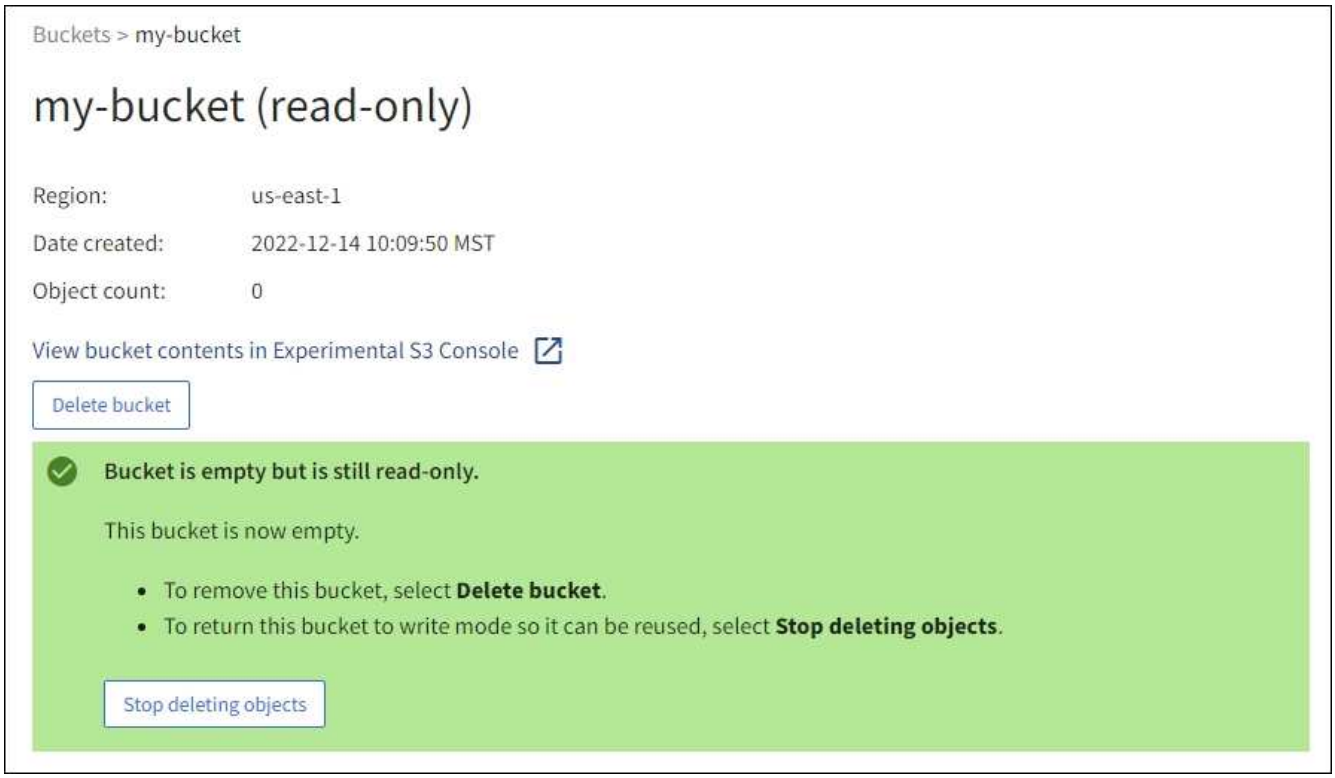


5. Quando l'operazione è in esecuzione, selezionare **Stop deleting objects** (Interrompi eliminazione oggetti) per interrompere il processo. Quindi, se si desidera, selezionare **Delete Objects in bucket** (Elimina oggetti nel bucket) per riprendere il processo.

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

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

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

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

Elimina bucket S3

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

Prima di iniziare

- Hai effettuato l'accesso al tenant manager utilizzando un "browser web supportato".
- L'utente appartiene a un gruppo di utenti che dispone di "Gestire tutti i bucket o le autorizzazioni di accesso root". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o

bucket.

- I bucket che si desidera eliminare sono vuoti. Se i bucket che si desidera eliminare sono *non* vuoti, "eliminare gli oggetti dal bucket".

A proposito di questa attività

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

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

Fasi

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

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

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

   Menu delle azioni

   a. Selezionare la casella di controllo per ciascun bucket che si desidera eliminare.

   b. Selezionare **azioni** > **Elimina bucket**.

   Pagina dei dettagli

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

   b. Selezionare **Delete bucket** (Elimina bucket).

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

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

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

Utilizzare la console S3

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

La console S3 consente di:

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

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

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

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

Prima di iniziare

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

Fasi

1. Selezionare **STORAGE** > **bucket** > ***bucket name***.
2. Selezionare la scheda Console S3.
3. Incollare l'ID della chiave di accesso e la chiave di accesso segreta nei campi. In caso contrario, selezionare **carica chiavi di accesso** e selezionare il `.csv` file.
4. Selezionare **Accedi**.
5. Viene visualizzata la tavola degli oggetti bucket. È possibile gestire gli oggetti in base alle esigenze.

Ulteriori informazioni

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

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.