Gestione dei bucket S3

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

Gestione dei bucket S3

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

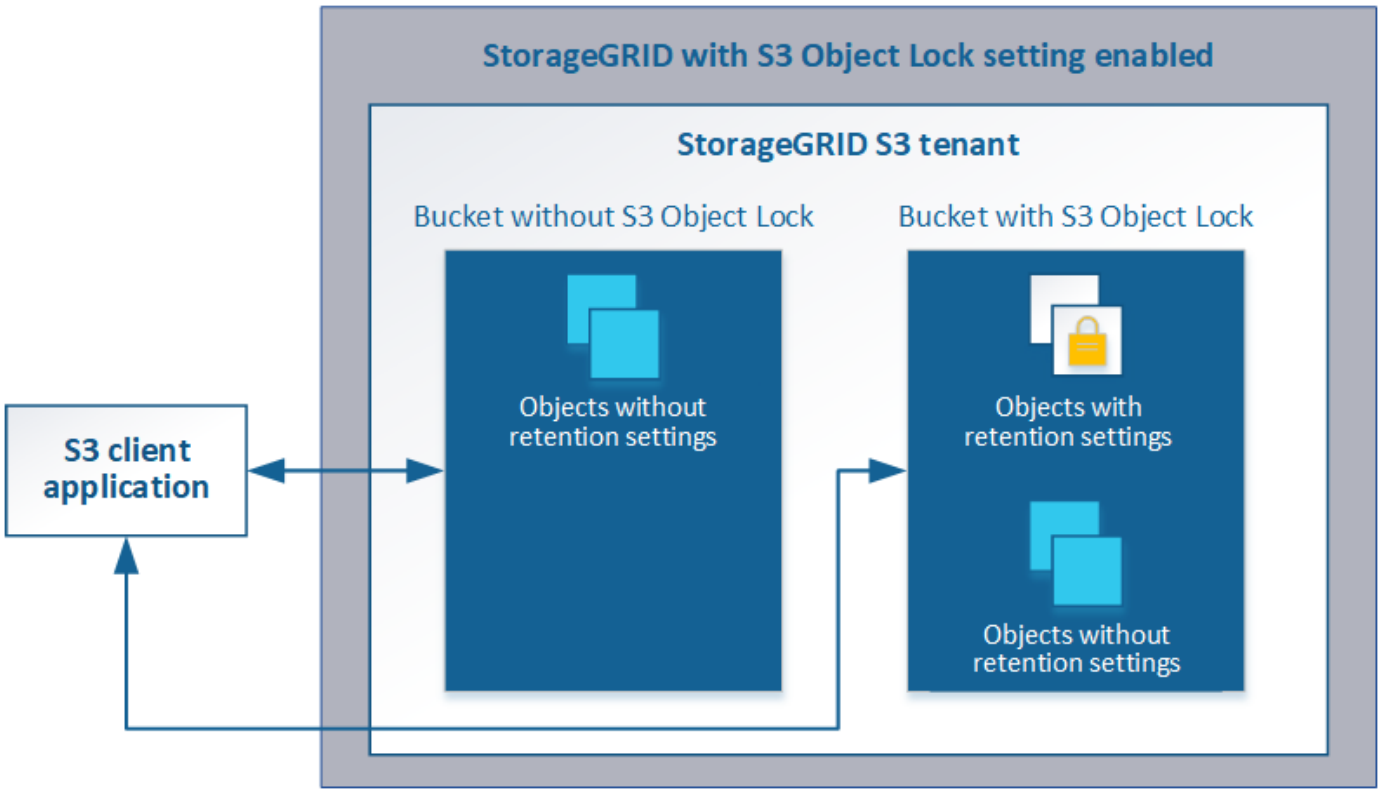
Utilizzo di S3 Object Lock

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

Che cos'è il blocco oggetti S3?

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

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



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

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

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

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

Gestione dei bucket conformi alle versioni precedenti

La funzione blocco oggetti S3 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Se sono stati creati bucket conformi utilizzando una versione precedente di StorageGRID, è possibile continuare a gestire le impostazioni di questi bucket; tuttavia, non è più possibile creare nuovi bucket conformi. Per istruzioni, consultare l'articolo della Knowledge base di NetApp.

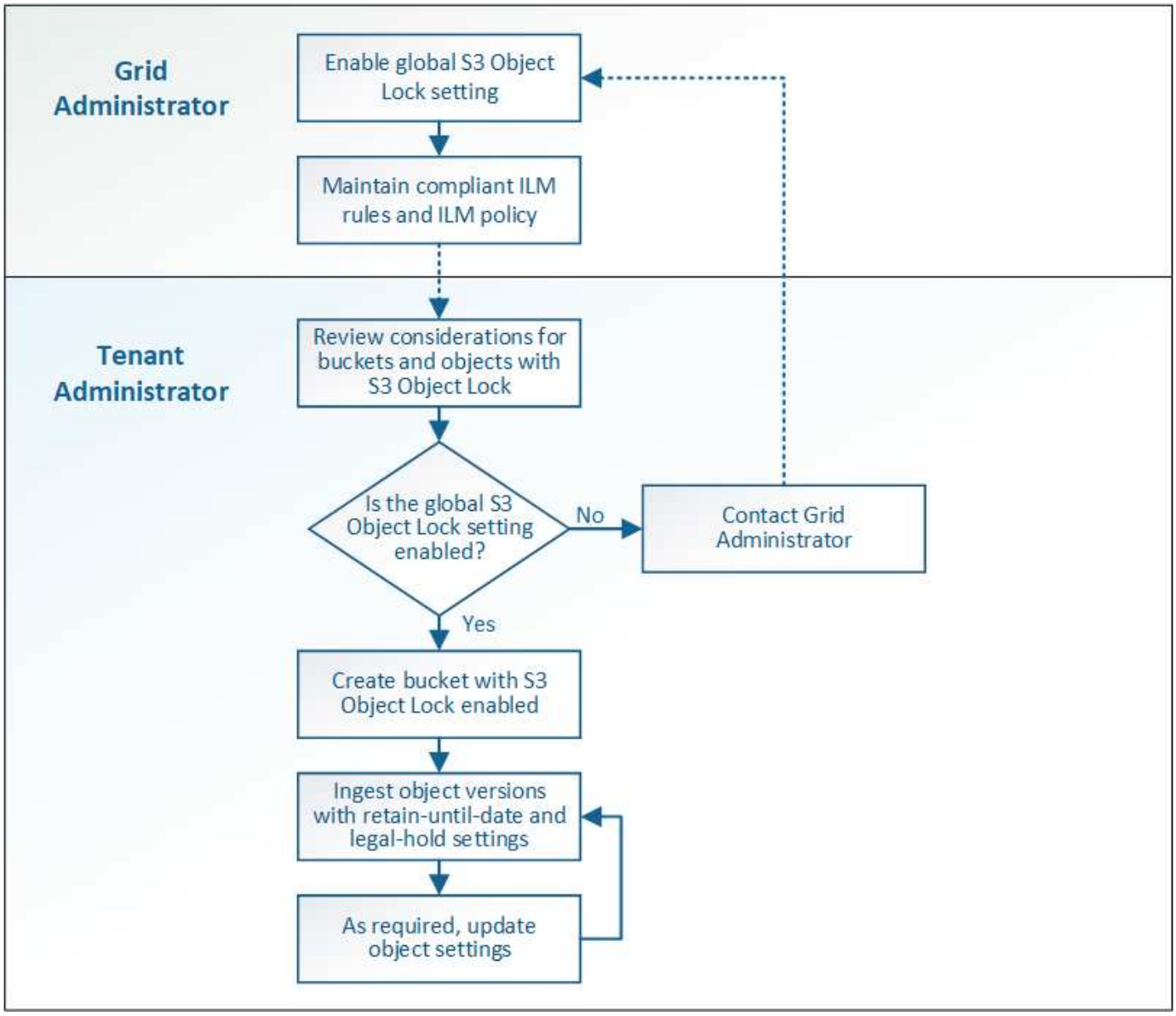
"Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"

Workflow di blocco oggetti S3

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

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

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



Informazioni correlate

"Gestire gli oggetti con ILM"

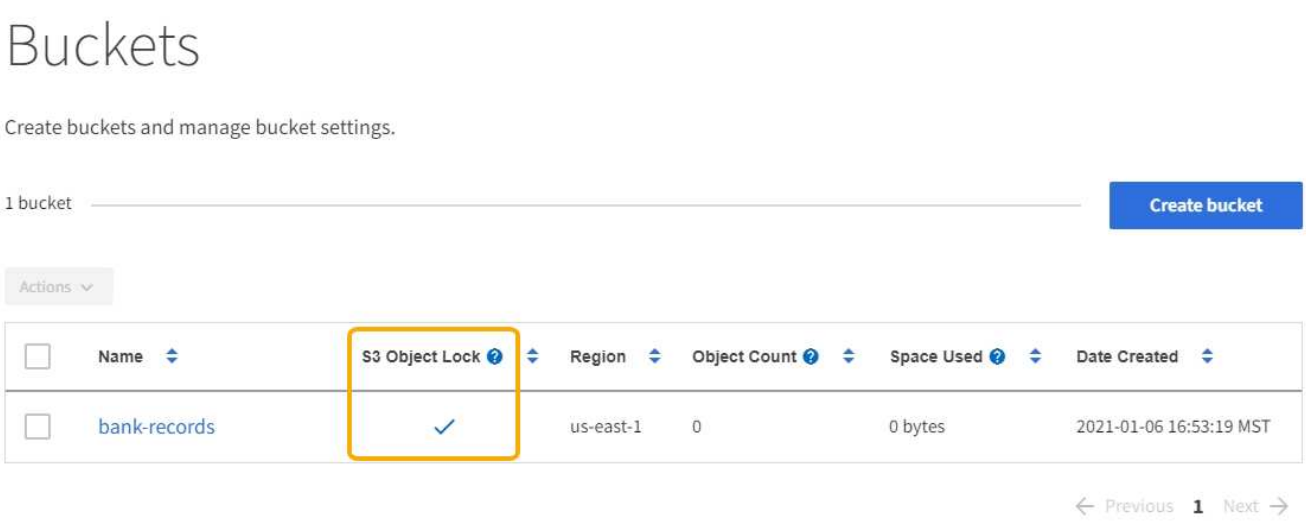
Requisiti per il blocco oggetti S3

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

Requisiti per i bucket con S3 Object Lock attivato

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

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



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

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- L'applicazione client S3 deve specificare le impostazioni di conservazione per ciascun oggetto che deve essere protetto da S3 Object Lock.
- È possibile aumentare la data di conservazione per una versione a oggetti, ma non è mai possibile diminuire questo valore.
- Se si riceve la notifica di un'azione legale o di un'indagine normativa in sospeso, è possibile conservare le informazioni pertinenti ponendo un blocco legale su una versione dell'oggetto. Quando una versione dell'oggetto è sottoposta a un blocco legale, non è possibile eliminare tale oggetto da StorageGRID, anche se ha raggiunto la data di conservazione. Non appena la conservazione legale viene revocata, la versione dell'oggetto può essere eliminata se è stata raggiunta la data di conservazione.
- S3 Object Lock richiede l'utilizzo di bucket con versione. Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di conservazione legale per un oggetto protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

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

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

1. **Acquisizione oggetto**

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

2. **Conservazione degli oggetti**
   - StorageGRID memorizza più copie dell'oggetto. Il numero e il tipo esatti di copie e le posizioni di storage sono determinati dalle regole conformi nel criterio ILM attivo.
3. **Eliminazione di oggetti**
   - È possibile eliminare un oggetto una volta raggiunta la data di conservazione.
   - Non è possibile eliminare un oggetto sottoposto a conservazione a fini giudiziari.

Creazione di un bucket S3

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

Di cosa hai bisogno

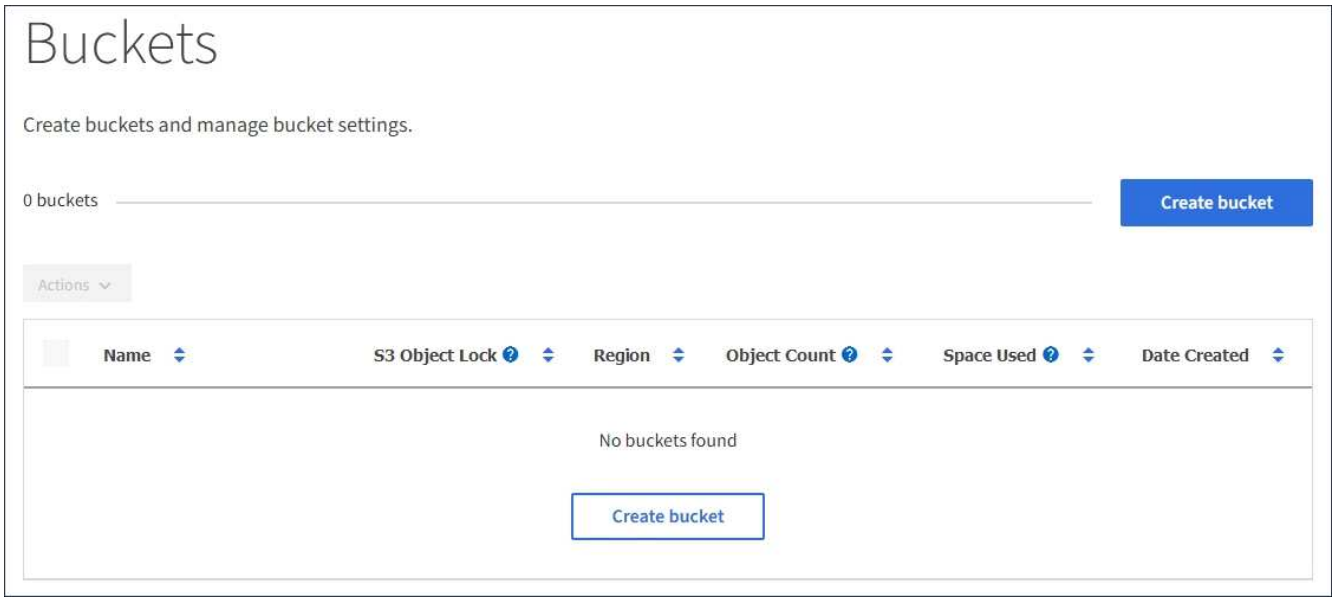
- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che disponga dell'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni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

  "Utilizzo di S3 Object Lock"

Fasi

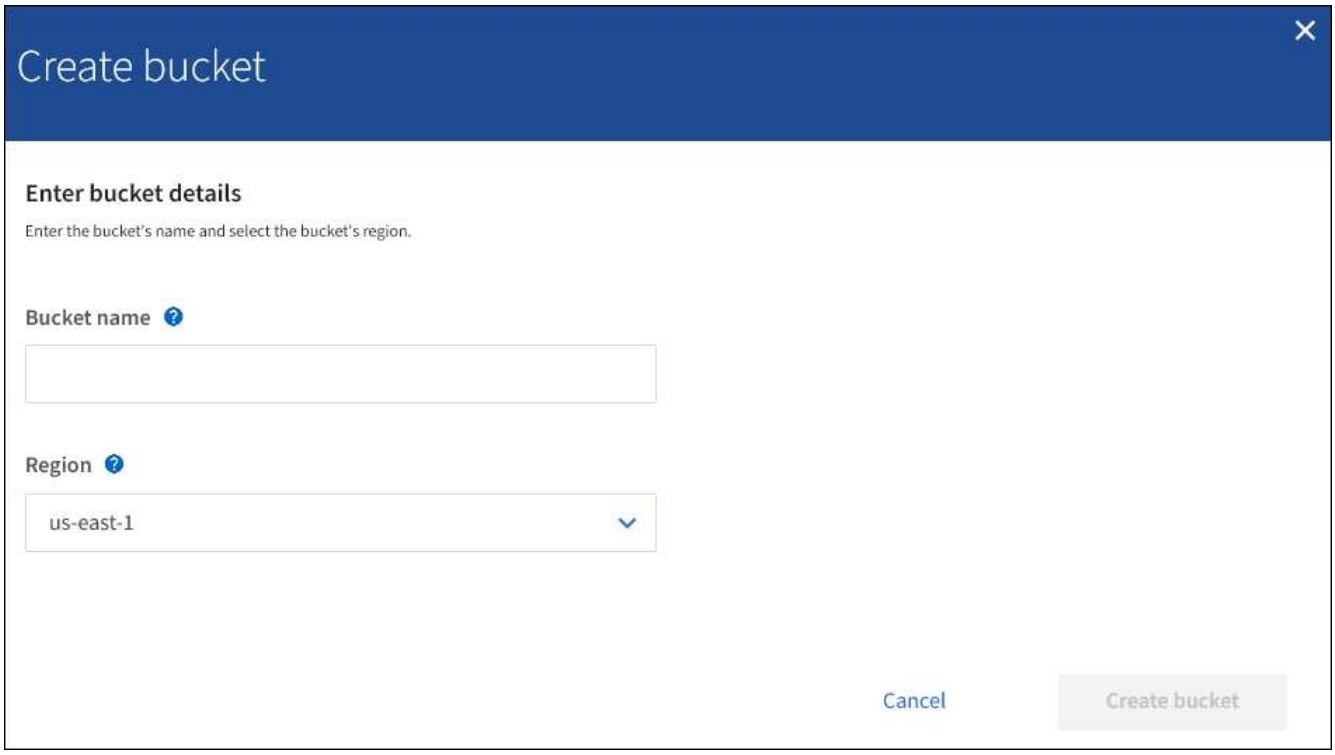
1. Selezionare **STORAGE (S3)** > **Bucket**.

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



2. Selezionare **Crea bucket**.

   Viene visualizzata la procedura guidata Create bucket.



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

3. Immettere un nome univoco per il bucket.

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

I nomi dei bucket devono essere conformi alle seguenti regole:

- Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).
- Deve essere conforme al DNS.
- Deve contenere almeno 3 e non più di 63 caratteri.
- Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini.
- Non deve essere simile a un indirizzo IP formattato con testo.
- Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server.

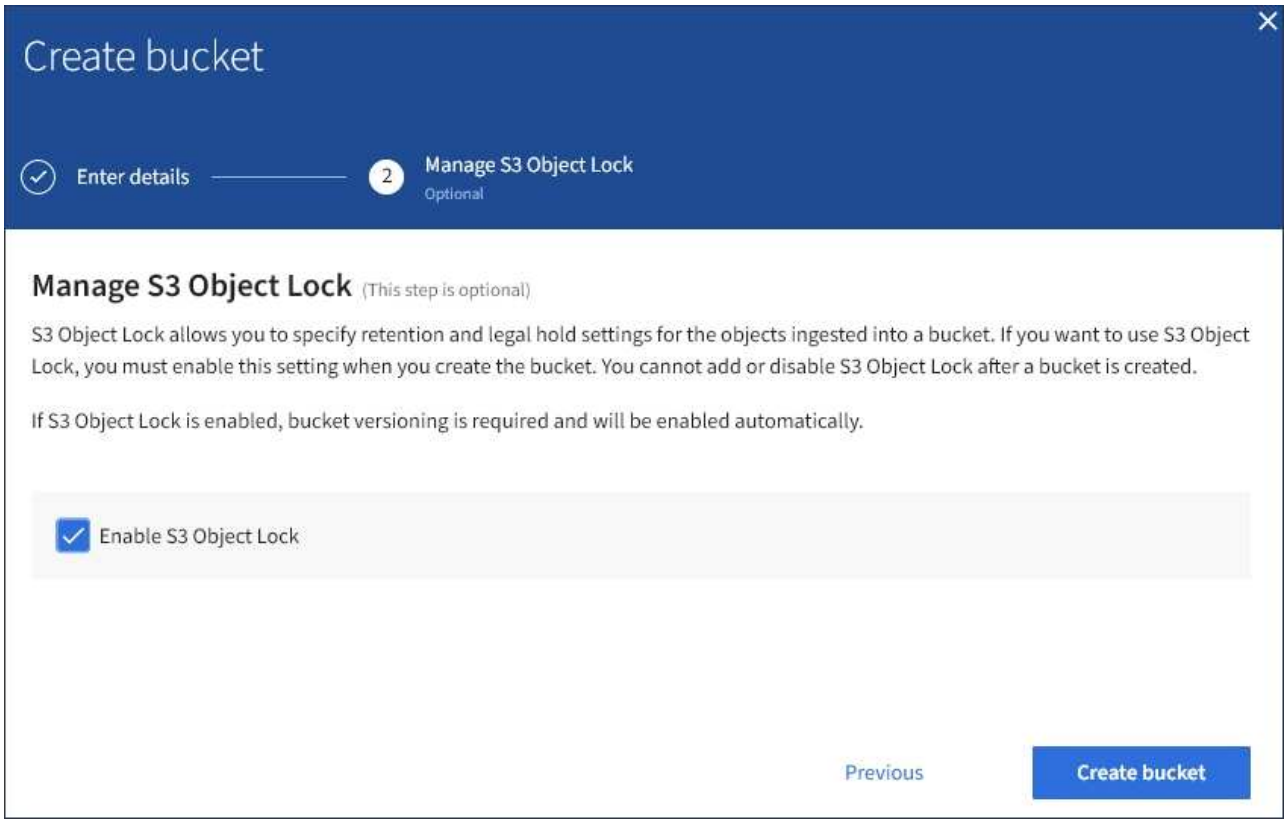
> Per ulteriori informazioni, consultare la documentazione di Amazon Web Services (AWS).

4. Selezionare la regione per questo bucket.

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

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

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



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

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

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

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

7. Selezionare **Crea bucket**.

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

Informazioni correlate

"Gestire gli oggetti con ILM"

"Informazioni sull'API di gestione del tenant"

"Utilizzare S3"

Visualizzazione dei dettagli del bucket S3

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

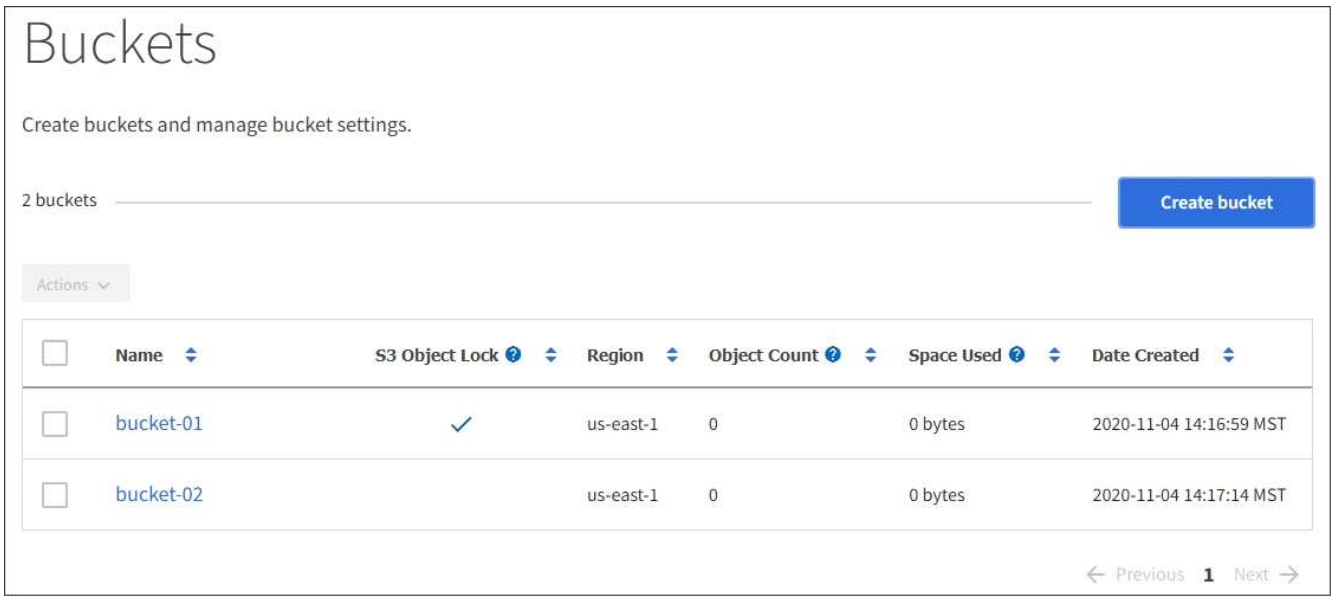
Di cosa hai bisogno

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

Fasi

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

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



2. Esaminare le informazioni relative a ciascun bucket.

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

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

     Questa colonna non viene visualizzata se l'impostazione di blocco oggetti S3 globale è disattivata. Questa colonna mostra anche informazioni relative a qualsiasi bucket compatibile legacy.

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

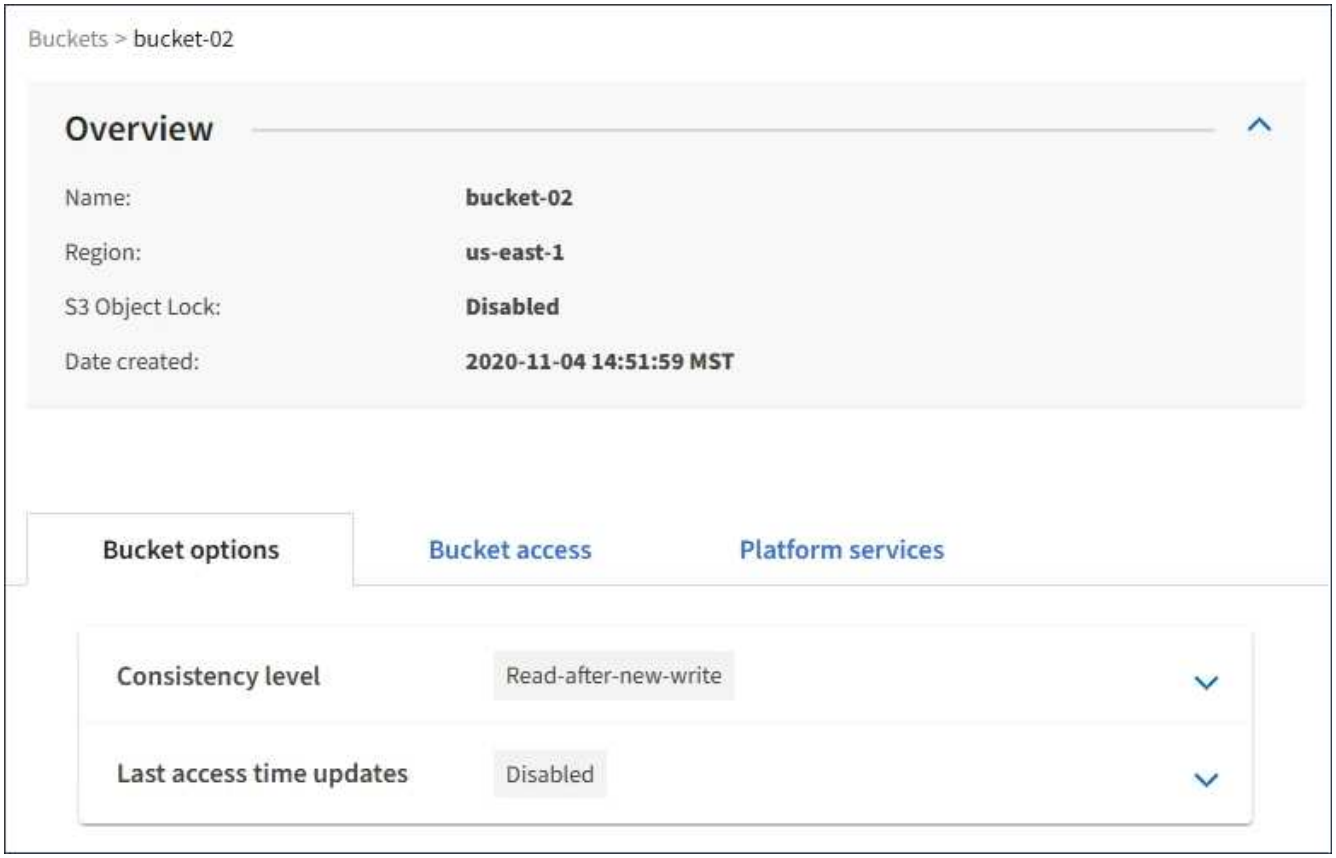
   > I valori Object Count (Conteggio oggetti) e Space used (spazio utilizzato) visualizzati sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi.

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

   Viene visualizzata la pagina dei dettagli del bucket.

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

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



Informazioni correlate

"Modifica del livello di coerenza"

"Attivazione o disattivazione degli ultimi aggiornamenti dell'orario di accesso"

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

"Configurazione della replica di CloudMirror"

"Configurazione delle notifiche degli eventi"

"Configurazione del servizio di integrazione della ricerca"

Modifica del livello di coerenza

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

Di cosa hai bisogno

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

A proposito di questa attività

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

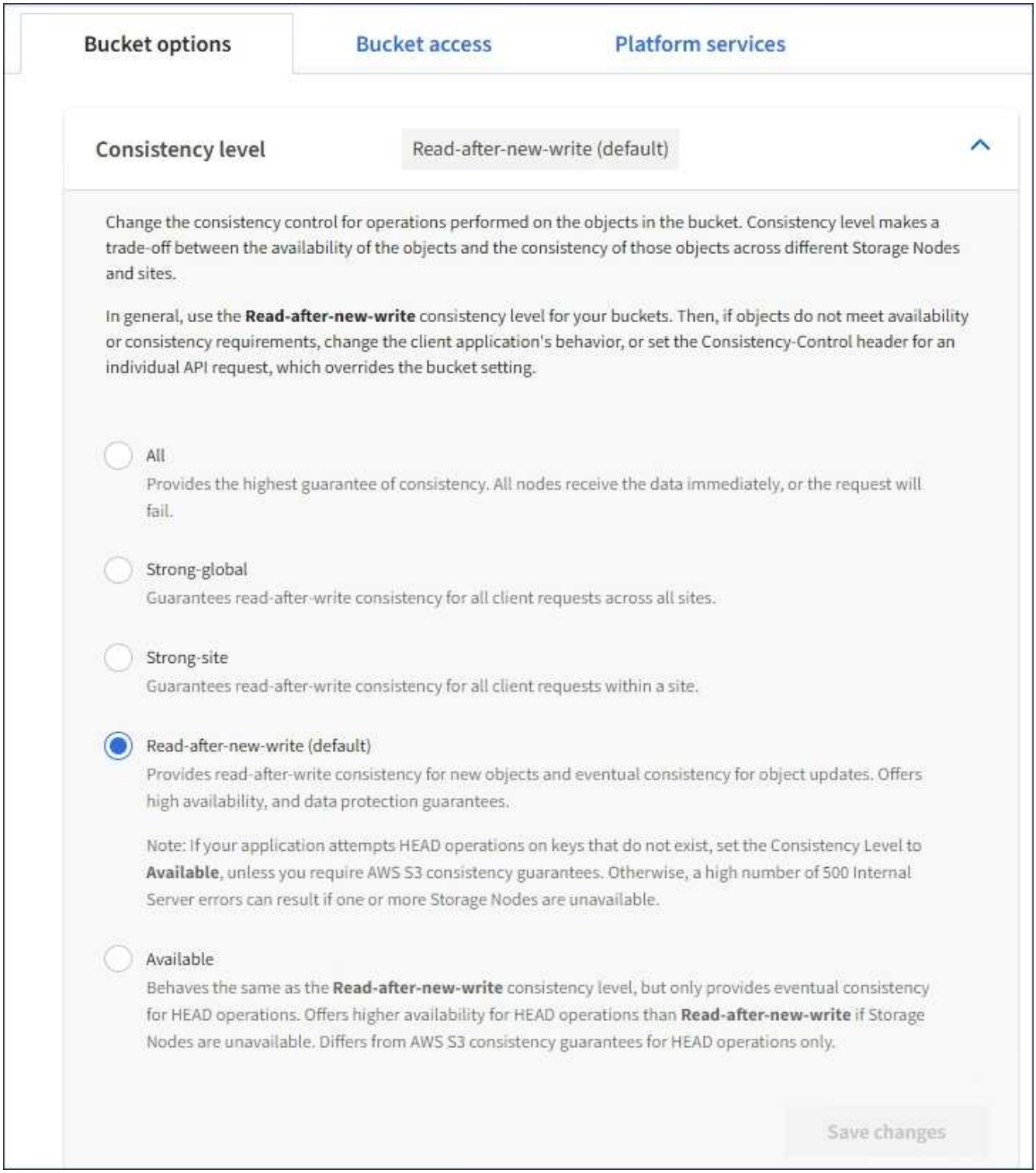
> Quando si modifica il livello di coerenza di un bucket, solo gli oggetti acquisiti dopo la modifica vengono garantiti per soddisfare il livello rivisto.

Fasi

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

   Viene visualizzata la pagina dei dettagli del bucket.

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



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

Livello di coerenza	Descrizione
Tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
Forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.

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

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

Informazioni correlate

"Permessi di gestione del tenant"

Attivazione o disattivazione degli ultimi aggiornamenti dell'orario di accesso

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

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

Di cosa hai bisogno

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

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

storage in base all'ultimo recupero (lettura o visualizzazione) di tali oggetti.

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

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

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

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

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

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

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

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

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

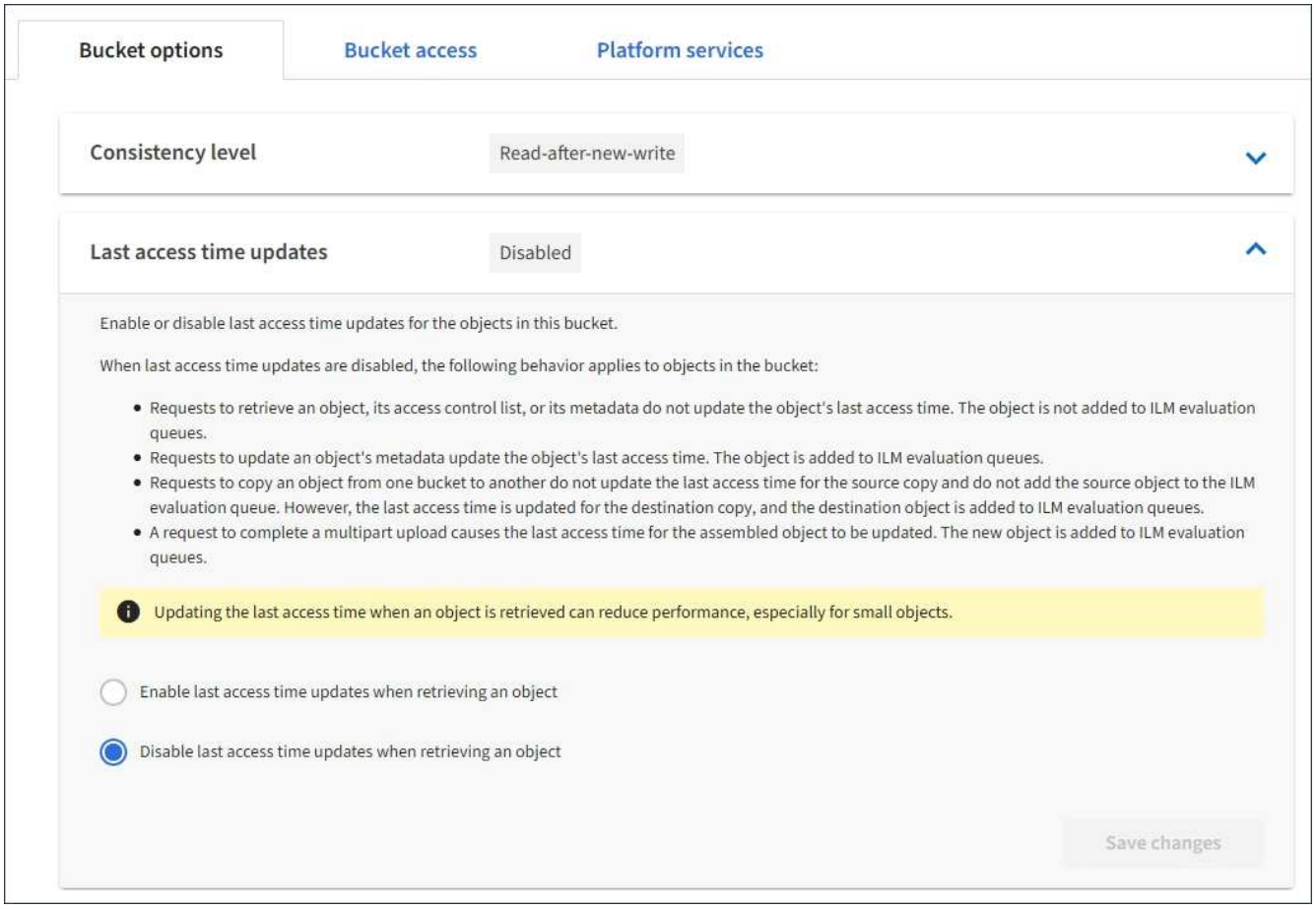
Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di 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 **STORAGE (S3)** > **Bucket**.
2. Selezionare il nome del bucket dall'elenco.

   Viene visualizzata la pagina dei dettagli del bucket.

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



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

Informazioni correlate

"Permessi di gestione del tenant"

"Gestire gli oggetti con ILM"

Configurazione di Cross-Origin Resource Sharing (CORS)

È possibile configurare Cross-Origin Resource Sharing (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini.

Di cosa hai bisogno

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

A proposito di questa attività

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

Fasi

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

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

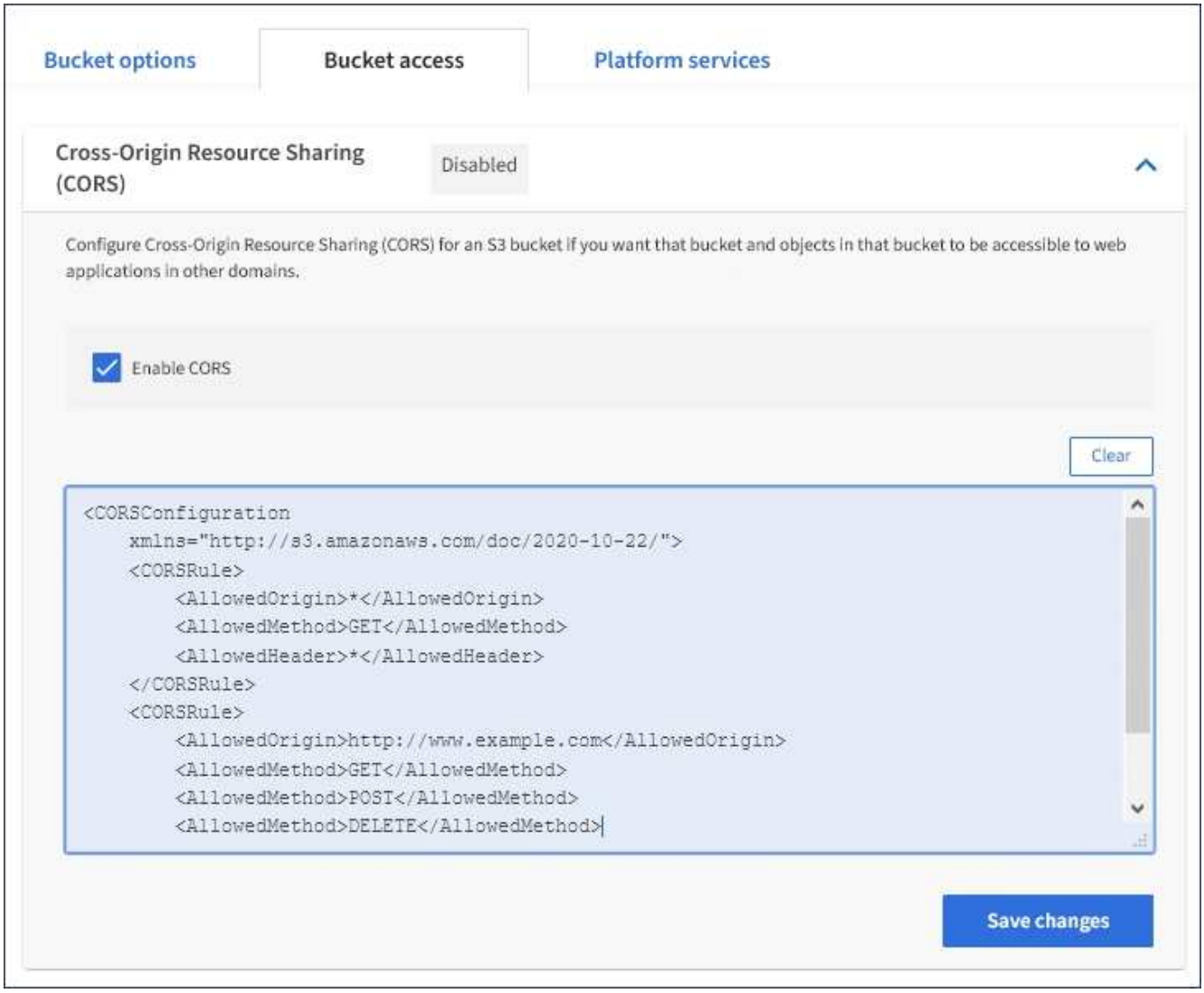
   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com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

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

2. In Tenant Manager, selezionare **STORAGE (S3)** > **Bucket**.
3. Selezionare il nome del bucket dall'elenco.

   Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **bucket access** > **Cross-Origin Resource Sharing (CORS)**.
5. Selezionare la casella di controllo **Enable CORS** (attiva CORS*).
6. Incollare l'XML di configurazione CORS nella casella di testo e selezionare **Save changes** (Salva modifiche).



7. Per modificare l'impostazione CORS per il bucket, aggiornare l'XML di configurazione CORS nella casella di testo o selezionare **Clear** per ricominciare. Quindi selezionare **Save Changes** (Salva modifiche).
8. Per disattivare il CORS per il bucket, deselezionare la casella di controllo **Enable CORS** (attiva CORS), quindi selezionare **Save Changes** (Salva modifiche).

Eliminazione di un bucket S3

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

Di cosa hai bisogno

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

A proposito di questa attività

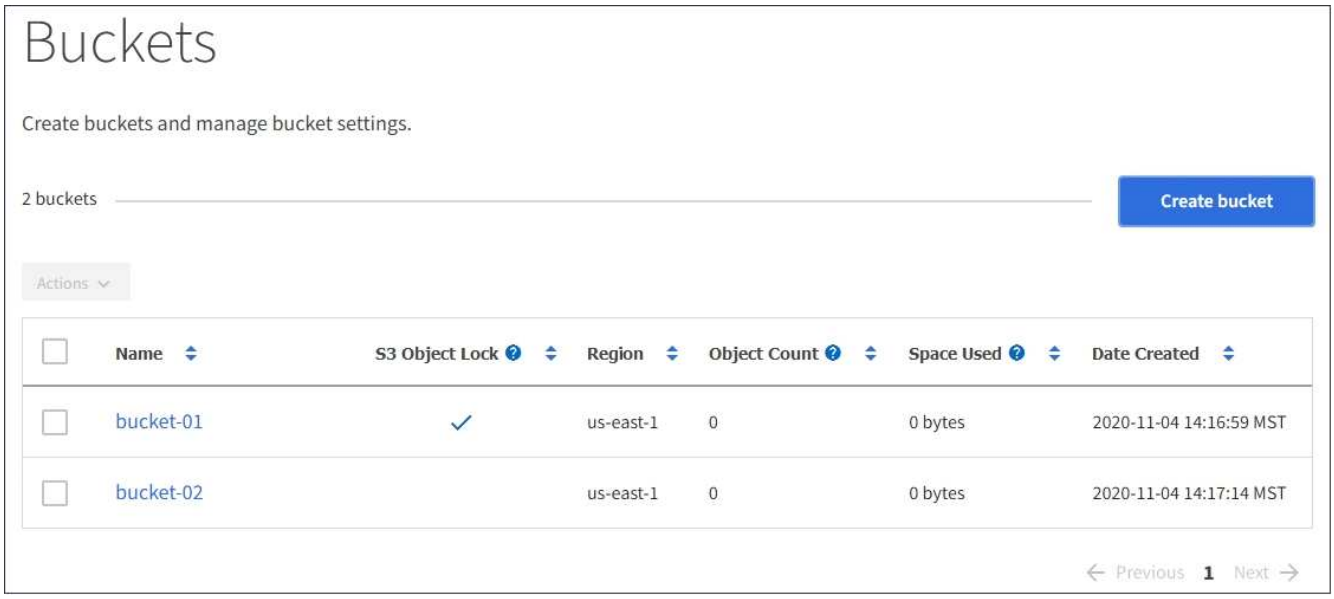
Queste istruzioni descrivono come eliminare un bucket S3 utilizzando il Tenant Manager. È inoltre possibile eliminare i bucket S3 utilizzando l'API di gestione tenant o l'API REST S3.

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

Fasi

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

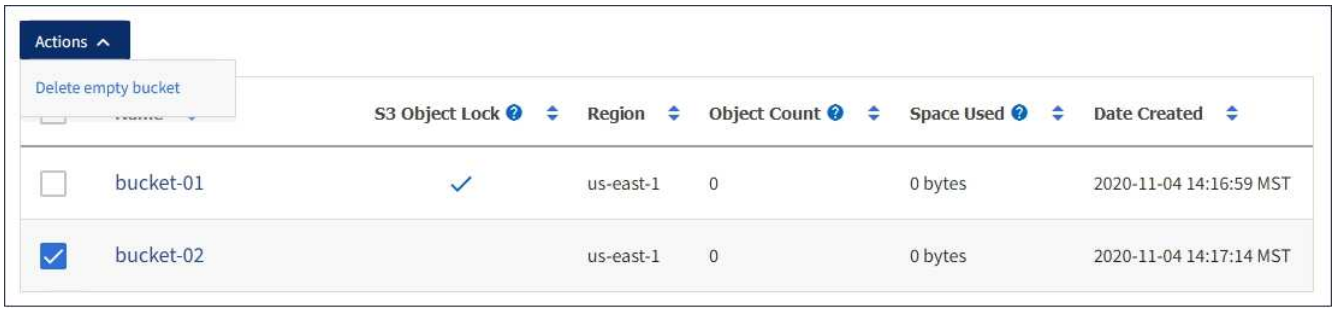
   Viene visualizzata la pagina bucket che mostra tutti i bucket S3 esistenti.



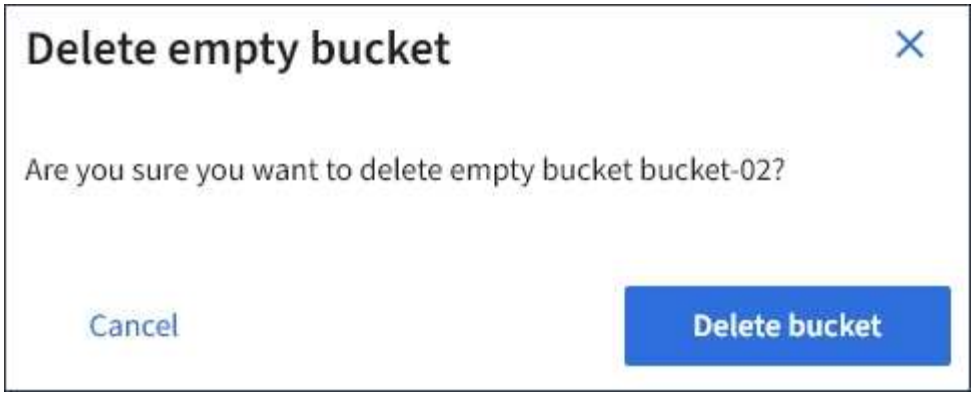
2. Selezionare la casella di controllo per il bucket vuoto che si desidera eliminare.

   Il menu Actions (azioni) è attivato.

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



   Viene visualizzato un messaggio di conferma.



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

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

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

Informazioni correlate

"Gestire gli oggetti con ILM"

Informazioni sul copyright

Informazioni sul marchio commerciale