Gestire i bucket S3

StorageGRID

NetApp
April 10, 2024

Sommario

Gestire i bucket S3 . . . 1
USA blocco oggetti S3 con tenant . . . 1
Creare un bucket S3 . . . 5
Visualizza i dettagli del bucket S3 . . . 7
Modificare il livello di coerenza . . . 9
Attiva o disattiva gli ultimi aggiornamenti dell’orario di accesso . . . 10
Modificare la versione degli oggetti per un bucket . . . 13
Configurare la condivisione delle risorse tra origini (CORS) . . . 15
Elimina bucket S3 . . . 17
Utilizzare la console S3 sperimentale . . . 19

Gestire i bucket S3

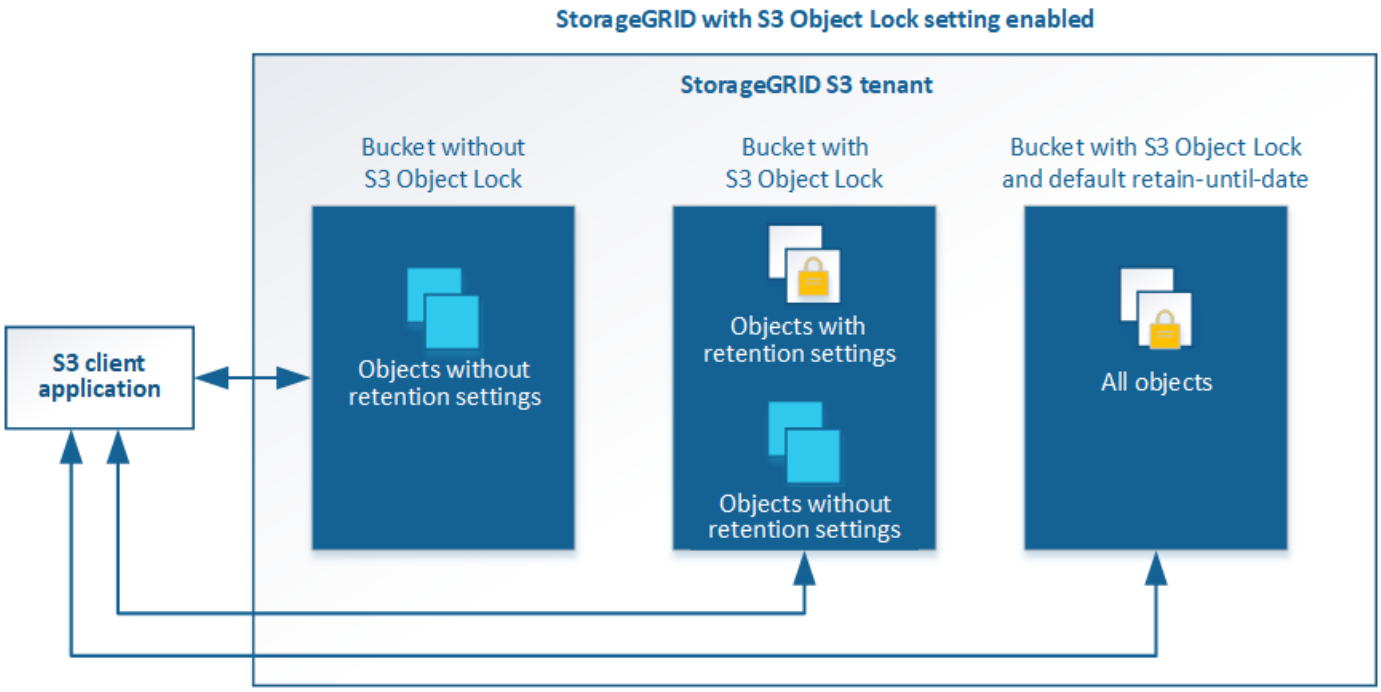
USA blocco oggetti S3 con tenant

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.

Puoi anche farlo specificare una modalità di conservazione predefinita e un periodo di conservazione predefinito per il bucket. Questi vengono applicati a ciascun oggetto aggiunto al bucket che non specifica le proprie impostazioni di conservazione.

Per ulteriori informazioni su queste impostazioni, vedere USA blocco oggetti S3.

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, consultare l'articolo della Knowledge base di NetApp.

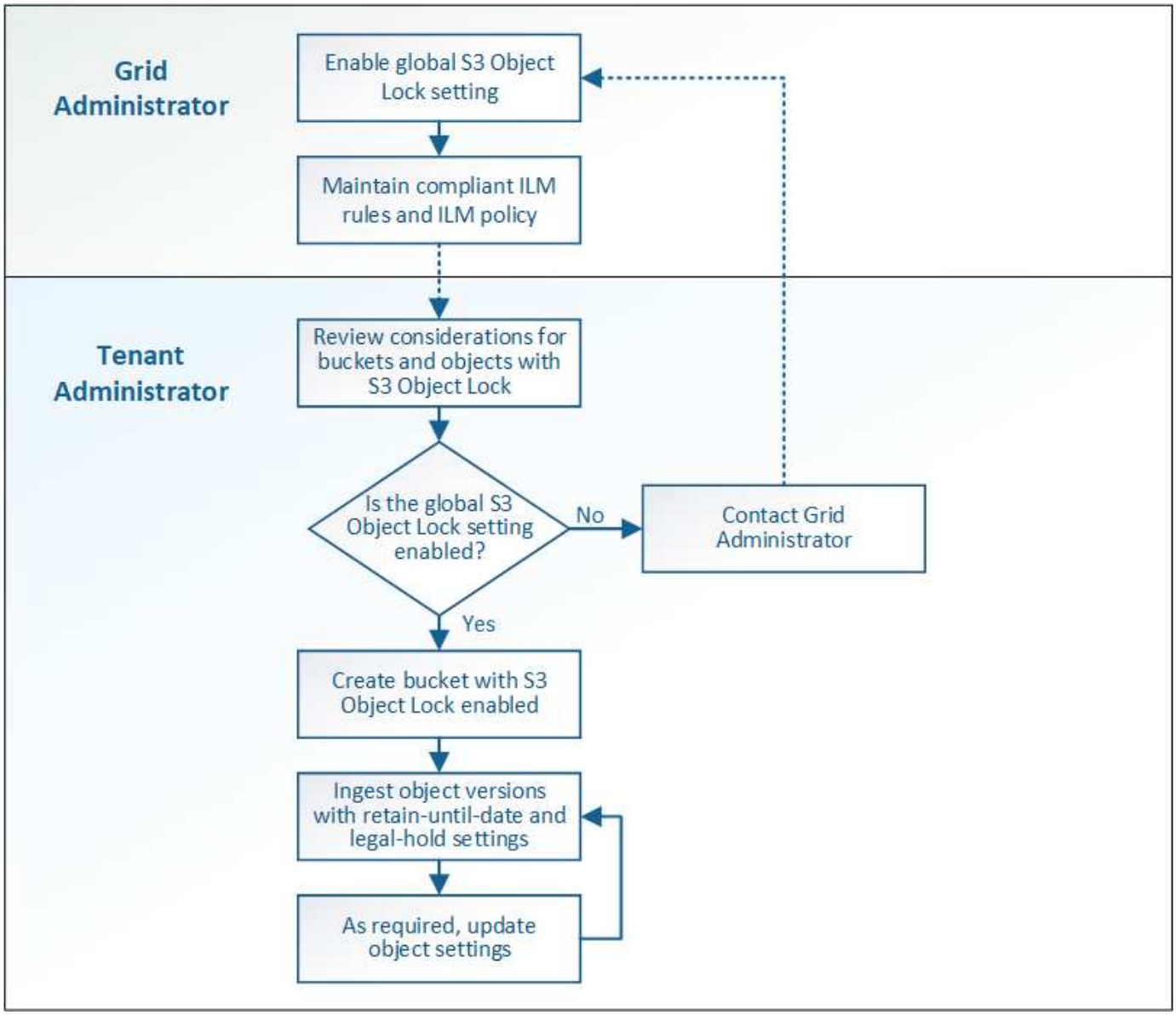
"Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"

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 assicurarsi che il Policy ILM (Information Lifecycle Management) È "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.



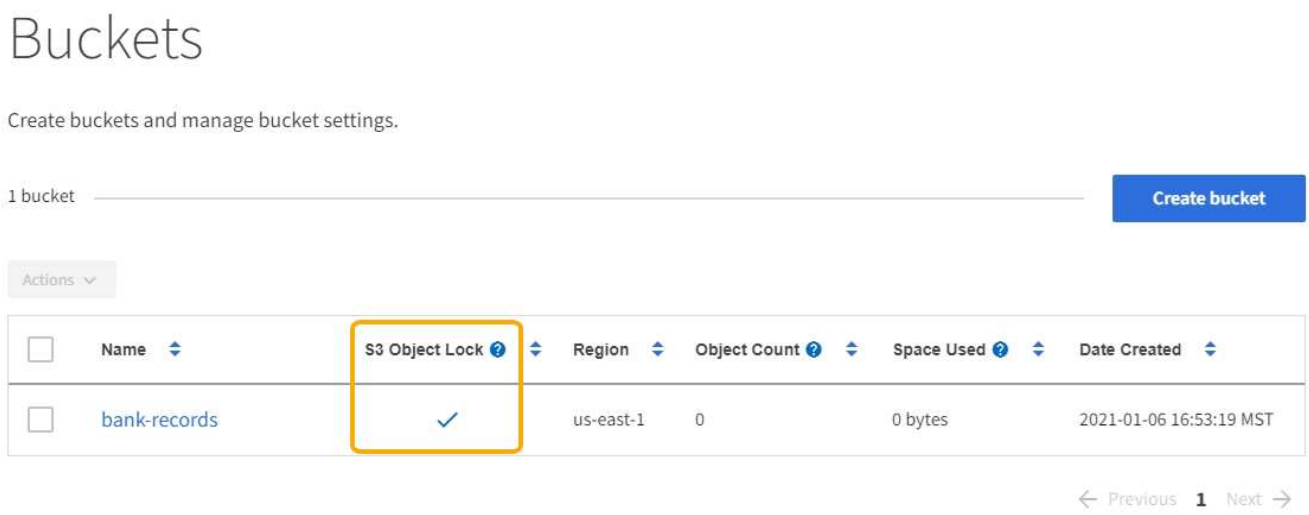
Requisiti per il blocco oggetti S3

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.
- Facoltativamente, è possibile configurare la conservazione predefinita per un bucket. Quando viene caricata una versione dell'oggetto, la conservazione predefinita viene applicata alla versione dell'oggetto. È possibile eseguire l'override del valore predefinito del bucket specificando una modalità di conservazione e conservarla fino a data nella richiesta di caricare una versione dell'oggetto.
- 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

- Per proteggere una versione a oggetti, l'applicazione client S3 deve configurare la conservazione predefinita del bucket o specificare le impostazioni di conservazione in ogni richiesta di caricamento.
- 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.

Creare 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

- Hai effettuato l'accesso al tenant manager utilizzando un browser web supportato.
- L'utente appartiene a un gruppo di utenti che dispone 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.

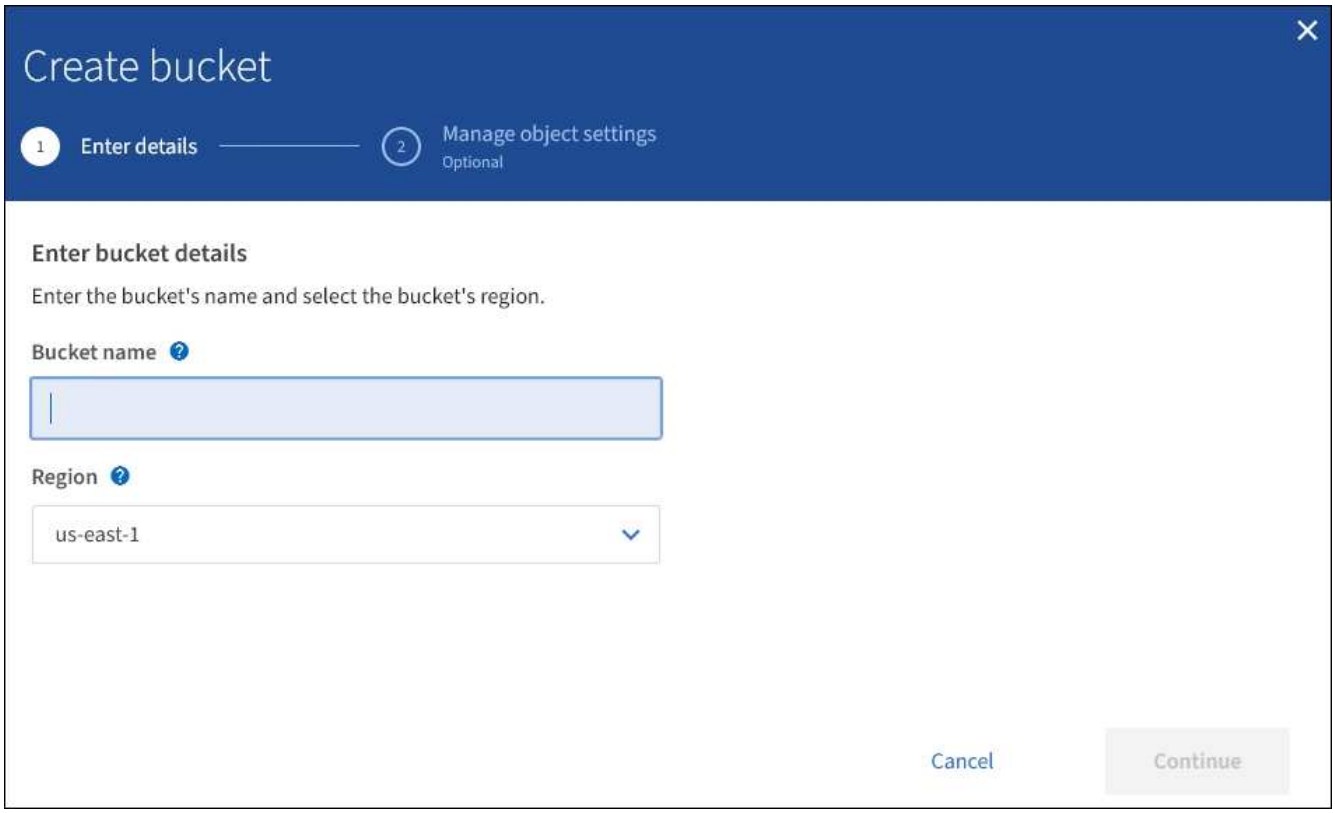
  Le autorizzazioni per impostare o modificare le proprietà di blocco oggetti S3 di bucket o oggetti possono essere concesse da policy bucket o policy di gruppo.

- Se si prevede di creare un bucket con blocco oggetti S3, è stata attivata l'impostazione di blocco oggetti S3 globale per il sistema StorageGRID e sono stati esaminati i requisiti per i bucket e gli oggetti blocco oggetti S3.

  USA blocco oggetti S3

Fasi

1. Selezionare **STORAGE (S3)** > **Bucket**.
2. Selezionare **Crea 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.
   - 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".

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 **continua**.
6. 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.

7. Se viene visualizzata la sezione S3 Object Lock (blocco oggetti S3), attivare facoltativamente S3 Object Lock (blocco oggetti S3) per il bucket.

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

   La sezione blocco oggetti S3 viene visualizzata solo se è attivata l'impostazione blocco oggetti S3 globale.

   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.

   Se si attiva il blocco oggetti S3 per un bucket, il controllo della versione del bucket viene attivato automaticamente. Puoi anche farlo specificare una modalità di conservazione predefinita e un periodo di conservazione predefinito per il bucket che vengono applicati a ciascun oggetto acquisito nel bucket che non specifica le proprie impostazioni di conservazione.

8. Selezionare **Crea bucket**.

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

Informazioni correlate

Gestire gli oggetti con ILM

Comprendere l'API di gestione dei tenant

Utilizzare S3

Visualizza i 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 al tenant manager utilizzando un browser web 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.

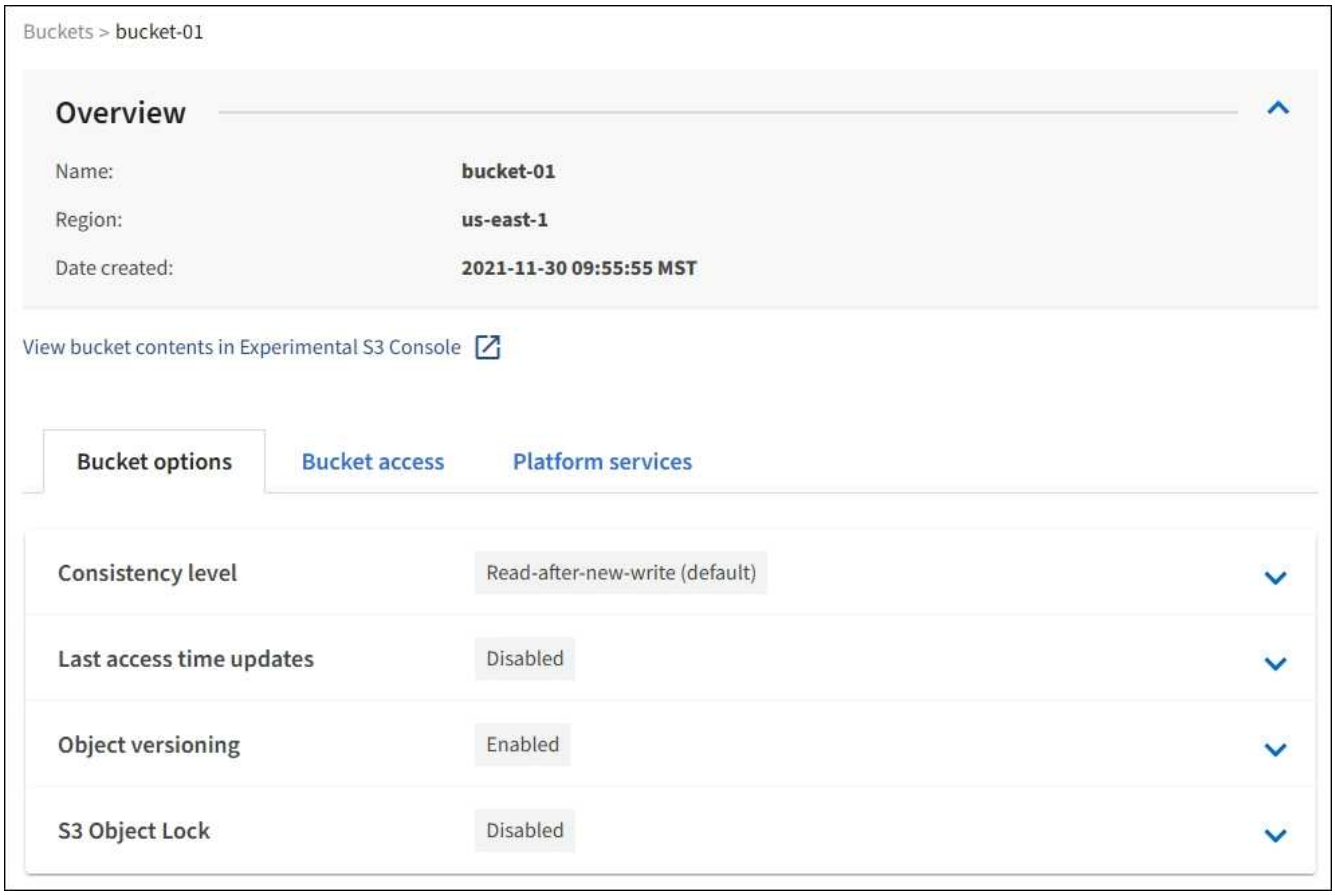
     Questa colonna non viene visualizzata se l'impostazione di blocco oggetti S3 globale è disattivata. Questa colonna mostra anche informazioni relative a qualsiasi bucket compatibile legacy.

   - 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. Se nei bucket è attivata la versione, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

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

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



Modificare il 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 al tenant manager utilizzando un browser web 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. Vedere Permessi di gestione del tenant.

A proposito di questa attività

Il livello di coerenza offre un equilibrio 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.
   - **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).

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 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 al tenant manager utilizzando un browser web 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. Vedere Permessi di gestione del tenant.

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

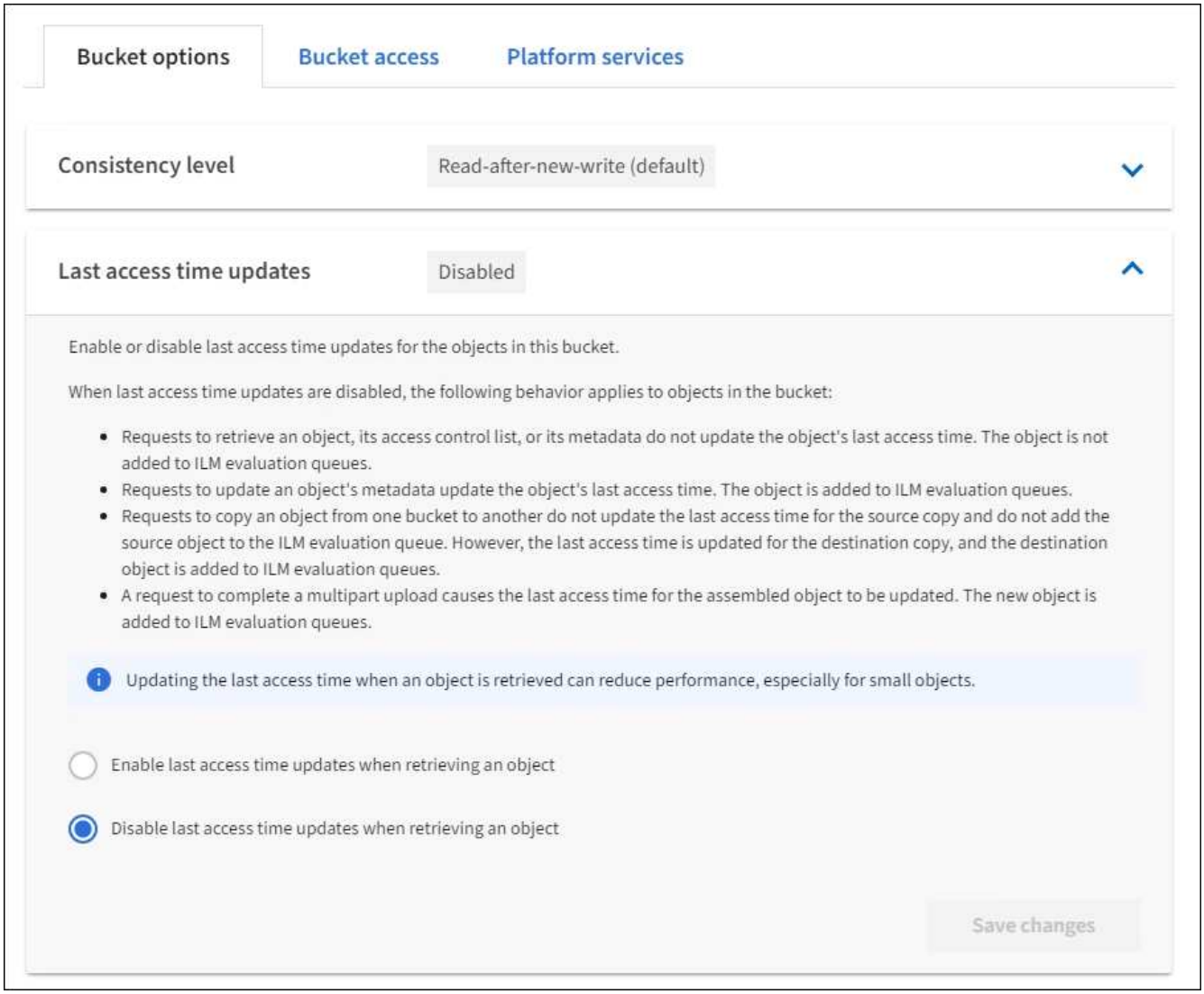
Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di 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

Modificare la versione degli oggetti per un bucket

Se si utilizza un tenant S3, è possibile utilizzare il tenant Manager o l'API di gestione tenant per modificare lo stato di versione per i bucket S3.

Di cosa hai bisogno

- Hai effettuato l'accesso al tenant manager utilizzando un browser web supportato.
- L'utente appartiene a un gruppo di utenti che dispone 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.

  Permessi di gestione del tenant

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 sarà possibile tornare allo stato senza versione. Tuttavia, è possibile sospendere il controllo delle versioni per il bucket.

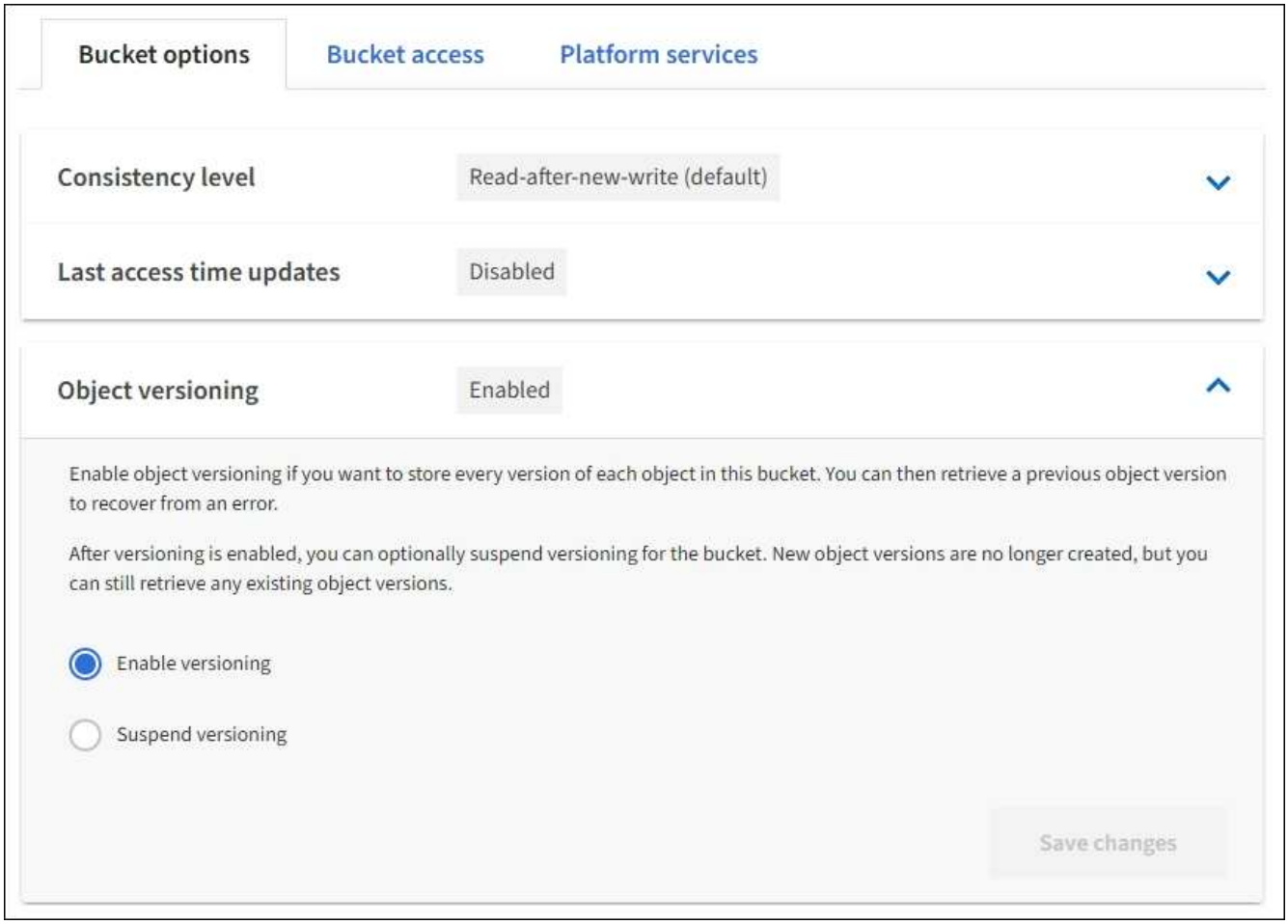
- Disabled (Disattivato): La versione non è mai stata attivata
- Enabled (attivato): Il controllo delle versioni è attivato
- Suspended (sospeso): Il controllo delle versioni era stato precedentemente attivato e sospeso

Versione degli oggetti S3

Regole e criteri ILM per gli oggetti con versione S3 (esempio 4)

Fasi

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



4. Selezionare uno stato di versione per gli oggetti in questo bucket.

> 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).

Configurare la condivisione delle risorse tra origini (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 al tenant manager utilizzando un browser web 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.

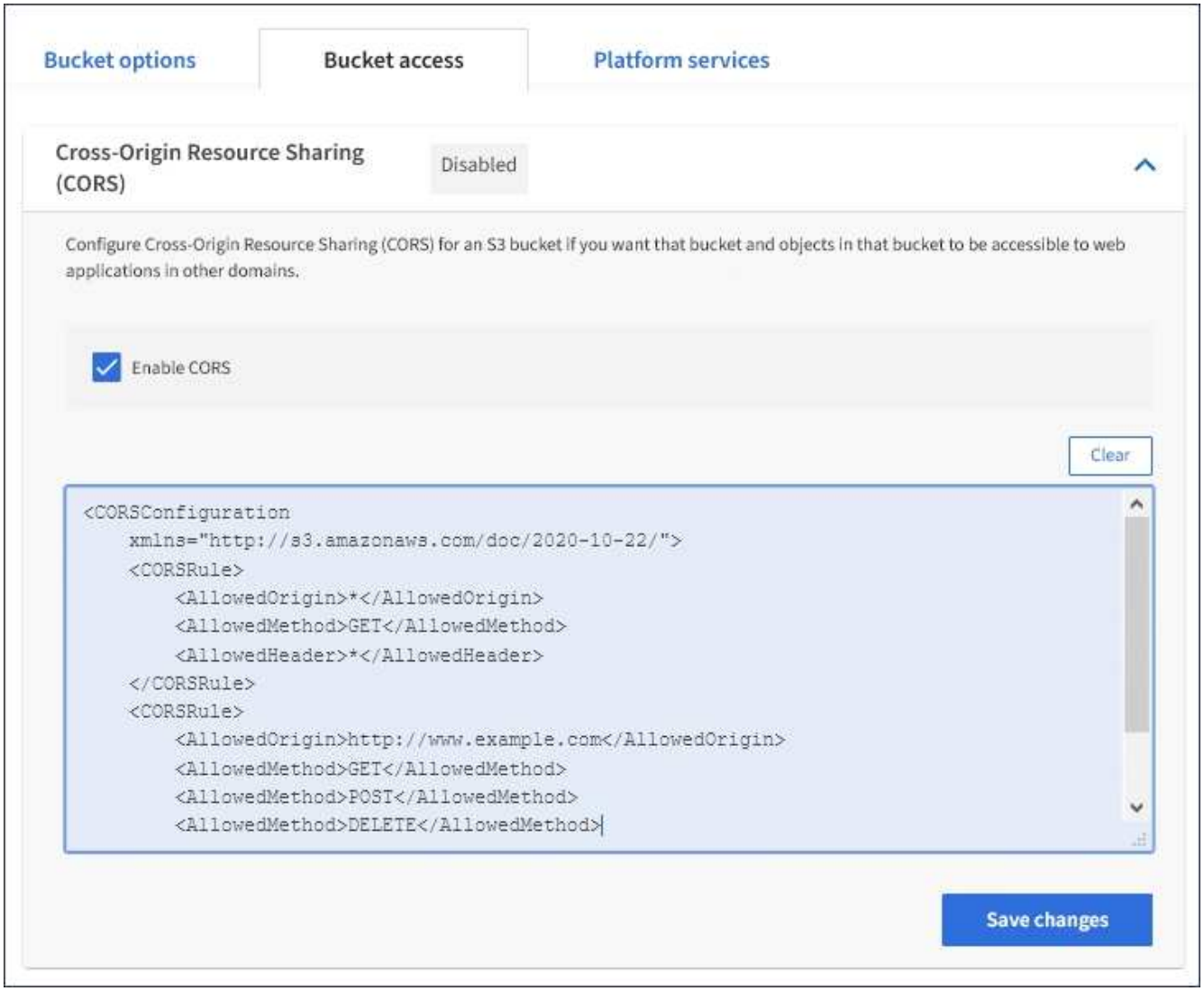
```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>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

Elimina bucket S3

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

Di cosa hai bisogno

- È necessario accedere al tenant manager utilizzando un browser web 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. Vedere Permessi di gestione del tenant.
- I bucket che si desidera eliminare sono vuoti.

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 o versioni di oggetti non correnti. Per informazioni sull'eliminazione degli oggetti con versione S3, vedere istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

Fasi

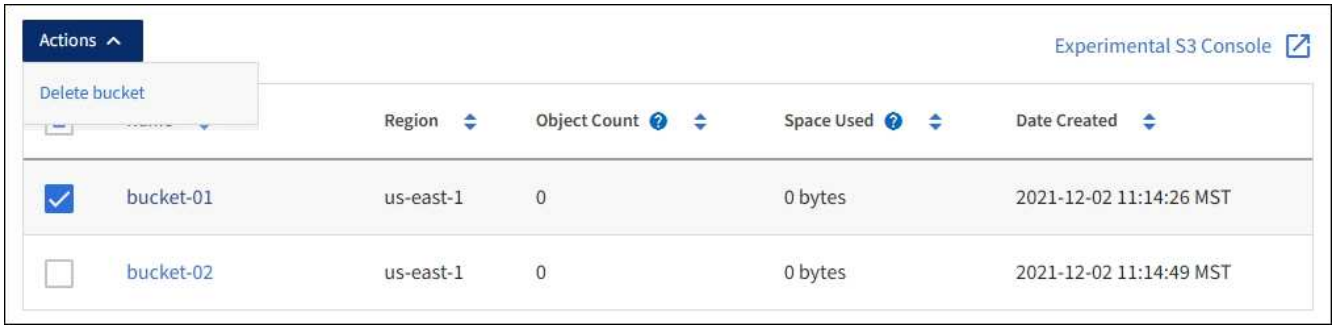
1. Selezionare **STORAGE (S3)** > **Bucket**.

   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. È possibile selezionare più bucket alla volta.

   Il menu Actions (azioni) è attivato.

3. Dal menu Actions (azioni), selezionare **Delete bucket** (Elimina bucket) (oppure **Delete bucket** (Elimina bucket) se sono stati selezionati più bucket).



4. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Sì** per eliminare tutti i bucket scelti.

   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 prima di poter eliminare un bucket.

Utilizzare la console S3 sperimentale

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

È inoltre possibile utilizzare la console S3 per effettuare le seguenti operazioni:

- Aggiungere ed eliminare oggetti, versioni di oggetti e cartelle
- Rinominare gli oggetti
- Spostare e copiare oggetti tra bucket e cartelle
- Gestire tag di oggetti
- Visualizzare i metadati degli oggetti
- Scarica oggetti

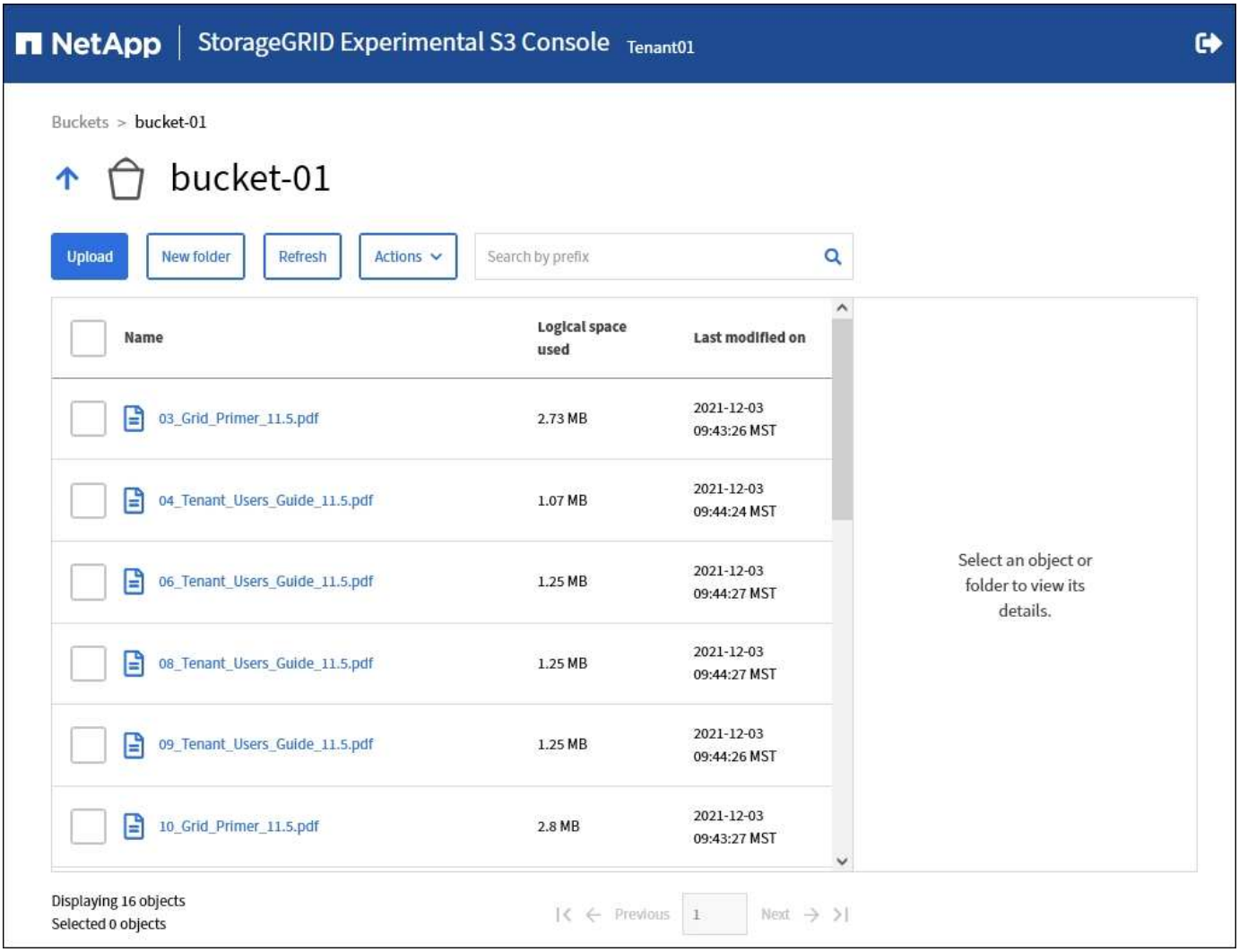
> S3 Console non è stato completamente testato ed è contrassegnato come "sperimentale". Non è destinato alla gestione in blocco di oggetti o all'utilizzo in un ambiente di produzione. I tenant devono utilizzare la console S3 solo quando eseguono funzioni per un numero limitato di oggetti, ad esempio durante il caricamento di oggetti per simulare una nuova policy ILM, la risoluzione dei problemi di acquisizione o l'utilizzo di griglie proof-of-concept o non di produzione.

Di cosa hai bisogno

- Hai effettuato l'accesso al tenant manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Gestisci credenziali S3.
- Hai creato un bucket.
- 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 **Bucket**.
2. Selezionare Experimental S3 Console . Puoi anche accedere a questo link dalla pagina dei dettagli del bucket.
3. Nella pagina di accesso alla console S3 sperimentale, 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. Gestire gli oggetti in base alle esigenze.


NetApp
StorageGRID Experimental S3 Console
Tenant01
Buckets > bucket-01
bucket-01
Upload
New folder
Refresh
Actions
Search by prefix
Name
Logical space used
Last modified on
03_Grid_Primer_11.5.pdf
2.73 MB
2021-12-03 09:43:26 MST
04_Tenant_Users_Guide_11.5.pdf
1.07 MB
2021-12-03 09:44:24 MST
06_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:27 MST
08_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:27 MST
09_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:26 MST
10_Grid_Primer_11.5.pdf
2.8 MB
2021-12-03 09:43:27 MST
Select an object or folder to view its details.
Displaying 16 objects
Selected 0 objects
Previous
1
Next