



Utilizzare un account tenant

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

- Utilizzare un account tenant 1
 - Utilizzo di Tenant Manager 1
 - Gestione dell'accesso al sistema per gli utenti tenant 15
 - Gestione degli account tenant S3 37
 - Gestione dei servizi della piattaforma S3 66

Utilizzare un account tenant

Scopri come utilizzare un account tenant StorageGRID.

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

Utilizzo di Tenant Manager

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

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

Utilizzando un account tenant StorageGRID

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

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

Facoltativamente, gli account tenant possono essere utilizzati per separare gli oggetti memorizzati da diverse entità. Ad esempio, è possibile utilizzare più account tenant per uno dei seguenti casi di utilizzo:

- **Caso d'utilizzo aziendale:** se il sistema StorageGRID viene utilizzato all'interno di un'azienda, lo storage a oggetti del grid potrebbe essere separato dai diversi reparti dell'organizzazione. Ad esempio, potrebbero essere presenti account tenant per il reparto Marketing, il reparto Assistenza clienti, il reparto risorse umane e così via.



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

- **Caso d'utilizzo del provider di servizi:** se il sistema StorageGRID viene utilizzato da un provider di servizi, lo storage a oggetti della griglia potrebbe essere separato dalle diverse entità che affittano lo storage. Ad esempio, potrebbero essere presenti account tenant per la società A, la società B, la società C e così via.

Creazione di account tenant

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

- Nome visualizzato per il tenant (l'ID account del tenant viene assegnato automaticamente e non può essere modificato).
- Se l'account tenant utilizzerà S3 o Swift.
- Per gli account tenant S3: Se l'account tenant è autorizzato a utilizzare i servizi della piattaforma. Se è

consentito l'utilizzo dei servizi della piattaforma, la griglia deve essere configurata per supportarne l'utilizzo.

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

Inoltre, gli amministratori della griglia possono attivare l'impostazione blocco oggetti S3 per il sistema StorageGRID se gli account tenant S3 devono soddisfare i requisiti normativi. Quando S3 Object Lock è attivato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

Configurazione dei tenant S3

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

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



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

Configurazione dei tenant Swift

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

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



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

Informazioni correlate

["Amministrare StorageGRID"](#)

["Utilizzare S3"](#)

["USA Swift"](#)

Requisiti del browser Web

È necessario utilizzare un browser Web supportato.

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

Impostare la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024
Ottimale	1280

Accesso al tenant manager

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

Di cosa hai bisogno

- È necessario disporre delle credenziali di accesso.
- Per accedere a tenant Manager, è necessario disporre di un URL fornito dall'amministratore della griglia. L'URL sarà simile a uno dei seguenti esempi:

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

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

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

L'URL contiene sempre il nome di dominio completo (FQDN) o l'indirizzo IP utilizzato per accedere a un nodo di amministrazione e può includere facoltativamente anche un numero di porta, l'ID dell'account tenant a 20 cifre o entrambi.

- Se l'URL non include l'ID account a 20 cifre del tenant, è necessario disporre di questo ID account.

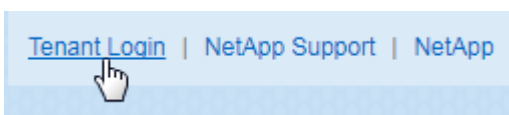
- È necessario utilizzare un browser Web supportato.
- I cookie devono essere attivati nel browser Web.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Avviare un browser Web supportato.
2. Nella barra degli indirizzi del browser, immettere l'URL per accedere a Tenant Manager.
3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser.
4. Accedi al tenant manager.

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

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



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

- i. Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.
- ii. Immettere il nome utente e la password.
- iii. Fare clic su **Accedi**.

Viene visualizzata la dashboard di Tenant Manager.

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

Sign in with your organizational account

someone@example.com

Password

Sign in

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

- La pagina di accesso SSO di Tenant Manager.

- Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.
- Fare clic su **Accedi**.
- Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Viene visualizzata la dashboard di Tenant Manager.

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



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

Informazioni correlate

["Amministrare StorageGRID"](#)

["Requisiti del browser Web"](#)

Disconnessione dal tenant manager

Una volta terminata la collaborazione con il tenant manager, è necessario disconnettersi per garantire che gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnettersi dal sistema, in base alle impostazioni dei cookie del browser.

Fasi

1. Individuare il menu a discesa Username (Nome utente) nell'angolo in alto a destra dell'interfaccia utente.



2. Selezionare il nome utente, quindi selezionare **Disconnetti**.

Opzione	Descrizione
SSO non in uso	<p>Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso del tenant manager.</p> <p>Nota: se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.</p>
SSO attivato	<p>Si è disconnessi da tutti i nodi di amministrazione ai quali si stava accedendo. Viene visualizzata la pagina di accesso a StorageGRID. Il nome dell'account tenant a cui hai appena effettuato l'accesso viene elencato come predefinito nell'elenco a discesa account recenti e viene visualizzato l'ID account* del tenant.</p> <p>Nota: se SSO è attivato e si è anche connessi a Grid Manager, è necessario disconnettersi da Grid Manager per disconnettersi da SSO.</p>

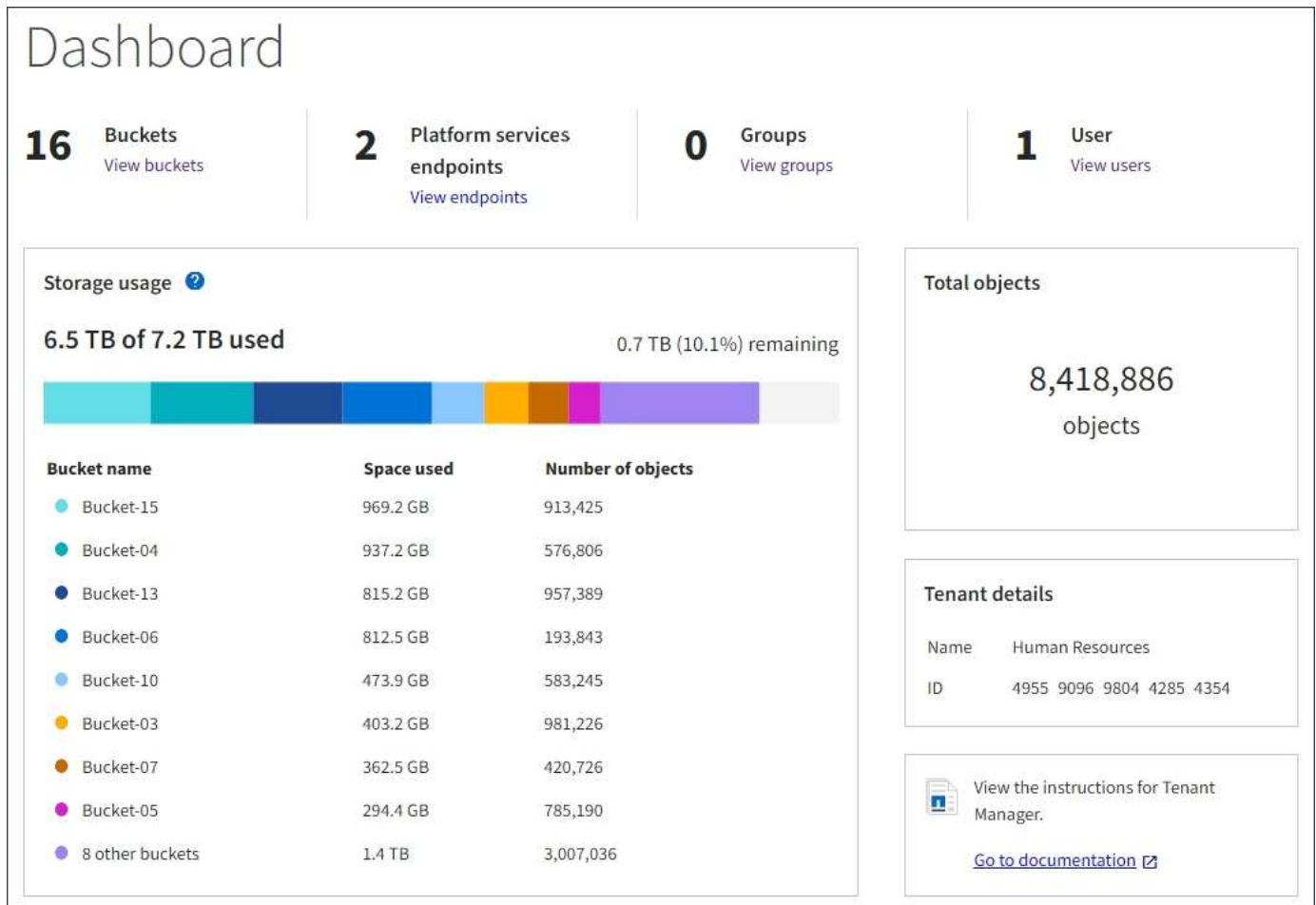
Informazioni sulla dashboard di Tenant Manager

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



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

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



Riepilogo account tenant

La parte superiore della dashboard contiene le seguenti informazioni:

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

È possibile selezionare i collegamenti per visualizzare i dettagli.

Il lato destro della dashboard contiene le seguenti informazioni:

- Il numero totale di oggetti per il tenant.

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

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

Utilizzo dello storage e delle quote

Il pannello Storage Use (utilizzo storage) contiene le seguenti informazioni:

- La quantità di dati oggetto per il tenant.



Questo valore indica la quantità totale di dati dell'oggetto caricati e non rappresenta lo spazio utilizzato per memorizzare le copie di tali oggetti e dei relativi metadati.

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



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

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

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



- Per corrispondere al grafico a barre, un elenco dei bucket o container più grandi, inclusa la quantità totale di dati oggetto e il numero di oggetti per ciascun bucket o container.

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

Se il tenant ha più di nove bucket o container, tutti gli altri bucket o container vengono combinati in una singola voce in fondo all'elenco.


Avvisi sull'utilizzo delle quote

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

Se è stato utilizzato il 90% o più della quota di un tenant, viene attivato l'avviso **quota di utilizzo elevata del tenant**. Per ulteriori informazioni, consultare il riferimento agli avvisi nelle istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

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

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


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



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

Errori degli endpoint

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

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Per visualizzare i dettagli relativi a un errore di endpoint, selezionare gli endpoint per visualizzare la pagina degli endpoint.

Informazioni correlate

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

["Monitor risoluzione dei problemi"](#)

Informazioni sull'API di gestione del tenant

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

L'API di gestione tenant utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di interagire con l'API. L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.

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

Fasi

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

Operazioni API

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

- **Account** — operazioni sull'account tenant corrente, incluso il recupero delle informazioni sull'utilizzo dello storage.
- **Auth** — operazioni per eseguire l'autenticazione della sessione utente.

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

Per informazioni su come migliorare la sicurezza dell'autenticazione, consultare "Protecting Against Cross-Site Request Fjery".



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

- **Config** — operazioni relative alla release del prodotto e alle versioni dell'API di gestione tenant. È possibile elencare la versione di release del prodotto e le principali versioni dell'API supportate da tale release.
- **Containers** — operazioni su bucket S3 o container Swift, come segue:

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

- **Disattivato-funzioni** — operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **Endpoint** — operazioni per gestire un endpoint. Gli endpoint consentono a un bucket S3 di utilizzare un

servizio esterno per la replica, le notifiche o l'integrazione della ricerca di StorageGRID CloudMirror.

- **Groups** — operazioni per gestire gruppi di tenant locali e recuperare gruppi di tenant federati da un'origine di identità esterna.
- **Identity-source** — operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **Regioni** — operazioni per determinare quali regioni sono state configurate per il sistema StorageGRID.
- **s3** — operazioni per gestire le chiavi di accesso S3 per gli utenti del tenant.
- **s3-Object-lock** — operazioni per determinare la modalità di configurazione del blocco oggetti S3 globale (compliance) per il sistema StorageGRID.
- **Utenti** — operazioni per visualizzare e gestire gli utenti del tenant.

Dettagli dell'operazione

Quando si espandono le operazioni API, è possibile visualizzare l'azione HTTP, l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.

groups Operations on groups

GET

/org/groups Lists Tenant User Groups

Parameters

Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses

Response content type

application/json

Code Description

200

Example Value Model

```
{
  "responseTime": "2018-02-01T16:22:31.066Z",
  "status": "success",
  "apiVersion": "2.1"
}
```

Invio di richieste API



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

Fasi

1. Fare clic sull'azione HTTP per visualizzare i dettagli della richiesta.
2. Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.
3. Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, fare clic su **Model** per conoscere i requisiti di ciascun campo.

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

Informazioni correlate

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

["Amministrare StorageGRID"](#)

Versione dell'API di gestione tenant

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

Ad esempio, questo URL di richiesta specifica la versione 3 dell'API.

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

La versione principale dell'API di gestione tenant viene bloccata quando vengono apportate modifiche **non compatibili** con le versioni precedenti. La versione minore dell'API di gestione tenant viene ridotta quando vengono apportate modifiche che **sono compatibili** con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o di nuove proprietà. Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2.1	2.2
Non compatibile con versioni precedenti	2.1	3.0

Quando il software StorageGRID viene installato per la prima volta, viene attivata solo la versione più recente dell'API di gestione del tenant. Tuttavia, quando StorageGRID viene aggiornato a una nuova release di funzionalità, si continua ad avere accesso alla versione API precedente per almeno una release di funzionalità StorageGRID.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero

Determinazione delle versioni API supportate nella release corrente

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

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

Specifica di una versione API per una richiesta

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

```
curl https://[IP-Address]/api/v3/grid/accounts
curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Protezione contro la contraffazione delle richieste (CSRF)

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

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

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


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

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

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

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



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

Gestione dell'accesso al sistema per gli utenti tenant

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

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

Utilizzo della federazione delle identità

L'utilizzo della federazione delle identità rende più rapida la configurazione di gruppi e utenti tenant e consente agli utenti tenant di accedere all'account tenant utilizzando credenziali familiari.

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

Configurazione di un'origine di identità federata

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


Di cosa hai bisogno

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

- È necessario utilizzare Active Directory, OpenLDAP o Oracle Directory Server come provider di identità. Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare il supporto tecnico.
- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3.

A proposito di questa attività

La possibilità di configurare un servizio di federazione delle identità per il tenant dipende dalla configurazione dell'account tenant. Il tenant potrebbe condividere il servizio di federazione delle identità configurato per Grid Manager. Se viene visualizzato questo messaggio quando si accede alla pagina Identity Federation, non è possibile configurare un'origine di identità federata separata per questo tenant.

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

Fasi

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

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

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

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP.
 - **User Unique Name** (Nome univoco utente): Il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` Per Active Directory e `uid` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
 - **UUID utente**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` Per Active Directory e `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Ogni valore dell'utente per l'attributo specificato deve essere un numero esadecimale a 32 cifre in formato a 16 byte o stringa, dove i trattini vengono ignorati.
 - **Group unique name** (Nome univoco gruppo): Il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a `sAMAccountName` Per Active Directory e `cn` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
 - **UUID gruppo**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` Per Active Directory e `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale a 32 cifre nel formato a 16 byte o stringa, dove i trattini vengono ignorati.
5. Nella sezione Configure LDAP server (Configura server LDAP), immettere le informazioni richieste per il server LDAP e la connessione di rete.
 - **Nome host**: Nome host del server o indirizzo IP del server LDAP.
 - **Port** (porta): Porta utilizzata per la connessione al server LDAP. La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

- **Username:** Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP. Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome principale dell'utente.

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

- sAMAccountName oppure uid
- objectGUID, entryUUID, o. nsuniqueid
- cn
- memberOf oppure isMemberOf

- **Password:** La password associata al nome utente.
- **DN base gruppo:** Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), tutti i gruppi il cui nome distinto è relativo al DN di base (DC=storagegrid,DC=example,DC=com) possono essere utilizzati come gruppi federati.

I valori **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

- **User base DN:** Il percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.

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

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

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

Questa opzione non è supportata se il server Active Directory applica la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.

- **Usa certificato CA del sistema operativo:** Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere le connessioni.
- **Usa certificato CA personalizzato:** Utilizza un certificato di protezione personalizzato.

Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

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

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

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

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

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory OpenLDAP Other

Configure LDAP server (All fields are required)

Hostname **Port**

Username

Password

Group Base DN

User Base DN

Informazioni correlate

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

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

Linee guida per la configurazione di un server OpenLDAP

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

MemberOf e refint overlay

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

Indicizzazione

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

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

Inoltre, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

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

Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

Di cosa hai bisogno

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

Fasi

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

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



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

2. Selezionare **Server di sincronizzazione**.

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

Informazioni correlate

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

Disattivazione della federazione delle identità

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

Di cosa hai bisogno

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

A proposito di questa attività

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

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso all'account tenant fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non viene eseguita.

Fasi

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

Informazioni correlate

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

Gestione dei gruppi

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



Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti locali non potranno accedere a Gestione tenant, anche se possono accedere alle risorse S3 e Swift, in base alle autorizzazioni di gruppo.

Permessi di gestione del tenant

Prima di creare un gruppo tenant, prendere in considerazione le autorizzazioni che si desidera assegnare a tale gruppo. Le autorizzazioni di gestione del tenant determinano le attività che gli utenti possono eseguire utilizzando il tenant Manager o l'API di gestione del tenant. Un utente può appartenere a uno o più gruppi. Le autorizzazioni sono cumulative se un utente appartiene a più gruppi.

Per accedere a tenant Manager o utilizzare l'API di gestione tenant, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono accedere possono eseguire le seguenti operazioni:

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

Per tutte le autorizzazioni, l'impostazione della modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità.



Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

È possibile assegnare a un gruppo le seguenti autorizzazioni. Tenere presente che i tenant S3 e Swift dispongono di permessi di gruppo diversi. Le modifiche potrebbero richiedere fino a 15 minuti per essere effettive a causa del caching.

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

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

Informazioni correlate

["Utilizzare S3"](#)

["USA Swift"](#)

Creazione di gruppi per un tenant S3

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

Di cosa hai bisogno

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

Fasi

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

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

2. Selezionare **Crea gruppo**.
3. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda

Federated group (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

4. Inserire il nome del gruppo.

- **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.
- **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

5. Selezionare **continua**.

6. Selezionare una modalità di accesso. Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

- **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
- **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API di gestione del tenant Manager o del tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

7. Selezionare le autorizzazioni di gruppo per questo gruppo.

Consultare le informazioni sulle autorizzazioni di gestione del tenant.

8. Selezionare **continua**.

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

- **Nessun accesso S3**: Impostazione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
- **Accesso di sola lettura**: Gli utenti di questo gruppo hanno accesso di sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
- **Accesso completo**: Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
- **Personalizzato**: Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo. Consultare le istruzioni per l'implementazione di un'applicazione client S3 per informazioni dettagliate sui criteri di gruppo, tra cui la sintassi del linguaggio e gli esempi.

10. Se si seleziona **Custom**, inserire il criterio di gruppo. Ogni policy di gruppo ha un limite di dimensione di 5,120 byte. Immettere una stringa valida formattata con JSON.

In questo esempio, i membri del gruppo possono solo elencare e accedere a una cartella corrispondente al proprio nome utente (prefisso della chiave) nel bucket specificato. Tenere presente che le autorizzazioni di accesso da altre policy di gruppo e la policy del bucket devono essere prese in considerazione quando si determina la privacy di queste cartelle.

No S3 Access

Read Only Access

Full Access

Custom
(Must be a valid JSON formatted string.)

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

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

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

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

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

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

13. Selezionare **fine**.

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

Informazioni correlate

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

["Utilizzare S3"](#)

Creazione di gruppi per un tenant Swift

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

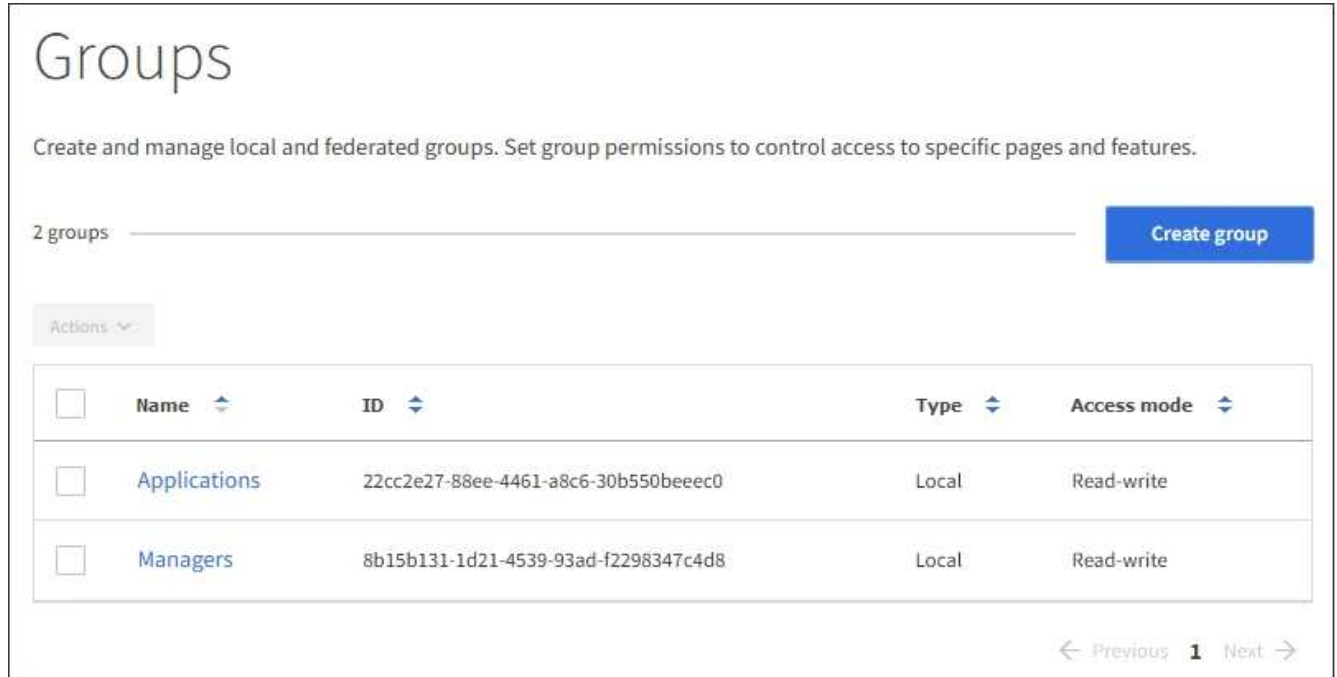
dell'autorizzazione Swift Administrator, necessaria per gestire i container e gli oggetti per un account tenant Swift.

Di cosa hai bisogno

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

Fasi

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



2. Selezionare **Crea gruppo**.
3. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda **Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

4. Inserire il nome del gruppo.
 - **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.
 - **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.
5. Selezionare **continua**.
6. Selezionare una modalità di accesso. Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

- **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
- **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API di gestione del tenant Manager o del tenant. Gli utenti locali di sola lettura possono modificare le proprie password.

7. Impostare l'autorizzazione di gruppo.

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

8. Selezionare **continua**.

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

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

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

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

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

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

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

12. Selezionare **fine**.

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

Informazioni correlate

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

["USA Swift"](#)

Visualizzazione e modifica dei dettagli del gruppo

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

Di cosa hai bisogno

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

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

Fasi

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

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

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

Overview

Display name:	Applications 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

Group permissions

S3 group policy

Users

Manage group permissions

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

Access mode

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

Read-write Read-only

Group permissions

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

Root Access

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

Manage All Buckets

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

Manage Endpoints

Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials


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

Save changes

3. Apportare le modifiche necessarie alle impostazioni del gruppo.



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

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

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

- b. Facoltativamente, aggiornare le autorizzazioni.

- c. Per i criteri di gruppo, apportare le modifiche appropriate al tenant S3 o Swift.

- Se si modifica un gruppo per un tenant S3, selezionare un criterio di gruppo S3 diverso. Se si seleziona un criterio S3 personalizzato, aggiornare la stringa JSON come richiesto.
- Se si modifica un gruppo per un tenant Swift, selezionare o deselezionare la casella di controllo **Swift Administrator**.

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

- d. Facoltativamente, aggiungere o rimuovere utenti.

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

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

Informazioni correlate

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

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

Aggiunta di utenti a un gruppo locale

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

Di cosa hai bisogno

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

Fasi

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

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

Viene visualizzata la pagina dei dettagli del gruppo.

Overview

Display name:	Applications 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

Group permissions

S3 group policy

Users

Manage group permissions

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

Access mode

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

Read-write Read-only

Group permissions

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

Root Access

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

Manage All Buckets

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

Manage Endpoints

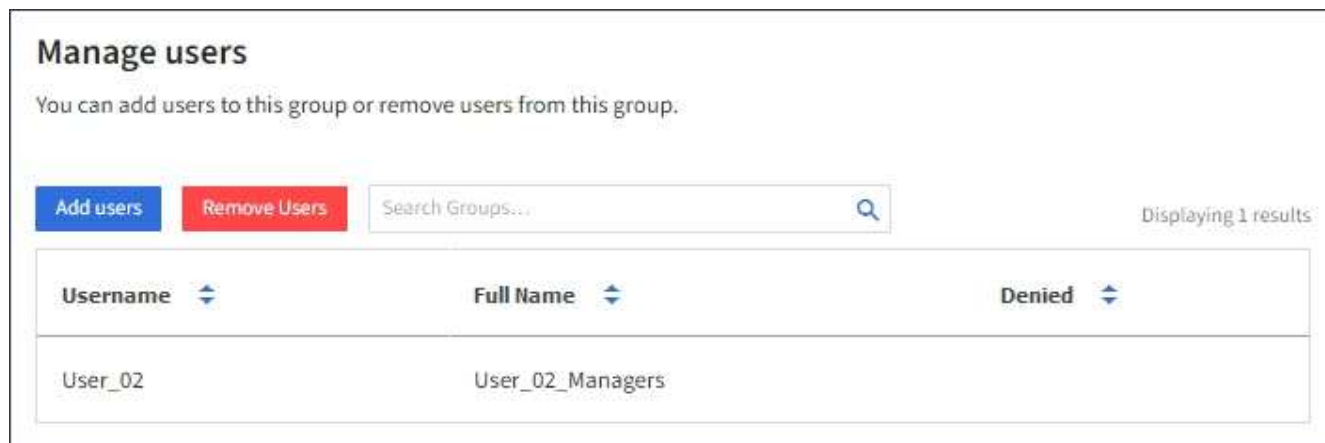
Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

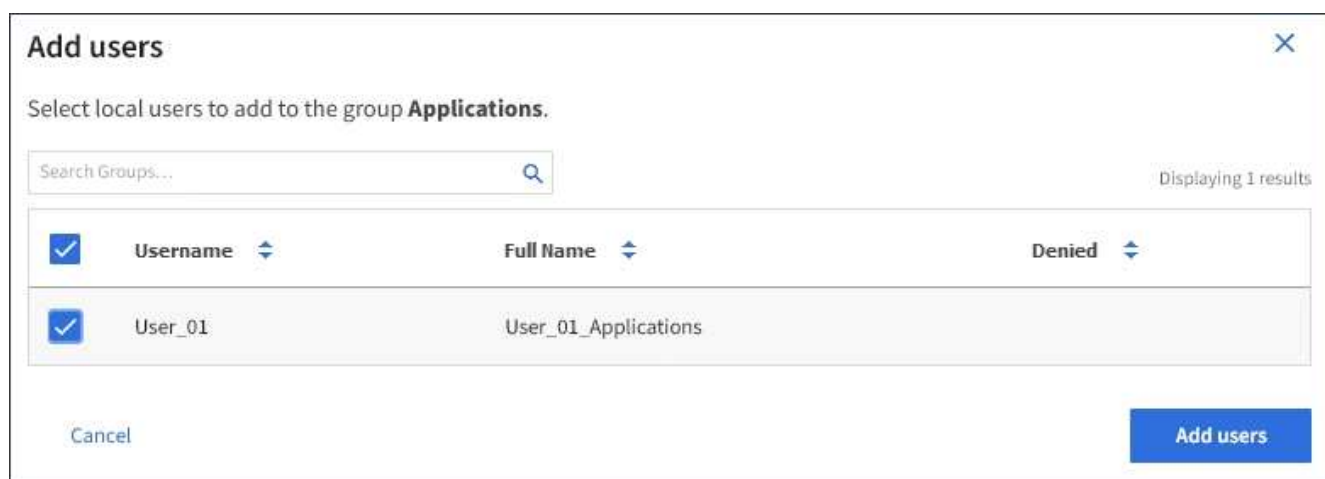
Allows users to create and delete their own S3 access keys.

Save changes

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



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



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

Modifica del nome di un gruppo

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

Di cosa hai bisogno

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

Fasi

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

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

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

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

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

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

Informazioni correlate

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

Duplicazione di un gruppo

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

Di cosa hai bisogno

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

Fasi

1. Selezionare **GESTIONE ACCESSI > gruppi**.
2. Selezionare la casella di controllo relativa al gruppo che si desidera duplicare.
3. Selezionare **Duplica gruppo**. Per ulteriori dettagli sulla creazione di un gruppo, consulta le istruzioni per la creazione di gruppi per un tenant S3 o Swift.
4. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda **Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

5. Inserire il nome del gruppo.

- **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.
- **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato a `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato a `uid` attributo.

6. Selezionare **continua**.

7. Se necessario, modificare le autorizzazioni per questo gruppo.

8. Selezionare **continua**.

9. Se si desidera duplicare un gruppo per un tenant S3, selezionare un criterio diverso dai pulsanti di opzione **Add S3 policy** (Aggiungi criterio S3). Se è stato selezionato un criterio personalizzato, aggiornare la stringa JSON come richiesto.

10. Selezionare **Crea gruppo**.

Informazioni correlate

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

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

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

Eliminazione di un gruppo

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

Di cosa hai bisogno

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

Fasi

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

Groups

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

2 groups Create group

Actions ▼

<input type="checkbox"/>	Name ↕	ID ↕	Type ↕	Access mode ↕
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beee0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous **1** Next →

2. Selezionare le caselle di controllo dei gruppi che si desidera eliminare.
3. Selezionare **azioni > Elimina gruppo**.

Viene visualizzato un messaggio di conferma.

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

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

Informazioni correlate

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

Gestione degli utenti locali

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

Di cosa hai bisogno

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



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

Accesso alla pagina utenti

Selezionare **ACCESS MANAGEMENT > Users**.

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

Creazione di utenti locali

È possibile creare utenti locali e assegnarli a uno o più gruppi locali per controllarne le autorizzazioni di accesso.

Gli utenti S3 che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o criteri di gruppo S3 applicati. Questi utenti potrebbero avere accesso al bucket S3 concesso tramite una policy bucket.

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

Fasi

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

ancora appartenere a uno o più gruppi.

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

3. Selezionare **continua**.
4. Assegnare l'utente a uno o più gruppi locali.

Gli utenti che non appartengono a nessun gruppo non disporranno di autorizzazioni di gestione. Le autorizzazioni sono cumulative. Gli utenti disporranno di tutte le autorizzazioni per tutti i gruppi a cui appartengono.

5. Selezionare **Crea utente**.

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


Modifica dei dettagli dell'utente

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

Fasi

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

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

2. Apportare le modifiche necessarie alle impostazioni utente.
 - a. Modificare il nome completo dell'utente in base alle necessità selezionando il nome completo o l'icona di modifica  Nella sezione Panoramica.

Non è possibile modificare il nome utente.
 - b. Nella scheda **Password**, modificare la password dell'utente in base alle necessità.
 - c. Nella scheda **Access**, consentire all'utente di accedere (selezionare **No**) o impedire all'utente di accedere (selezionare **Si**) in base alle necessità.
 - d. Nella scheda **gruppi**, aggiungere l'utente ai gruppi o rimuoverlo dai gruppi in base alle necessità.
 - e. In base alle esigenze di ciascuna sezione, selezionare **Save Changes** (Salva modifiche).

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

Duplicazione degli utenti locali

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

Fasi

1. Nell'elenco Users (utenti), selezionare l'utente che si desidera duplicare.
2. Selezionare **Duplica utente**.
3. Modificare i seguenti campi per il nuovo utente.

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

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

4. Selezionare **continua**.
5. Selezionare uno o più gruppi locali.

Gli utenti che non appartengono a nessun gruppo non disporranno di autorizzazioni di gestione. Le autorizzazioni sono cumulative. Gli utenti disporranno di tutte le autorizzazioni per tutti i gruppi a cui appartengono.

6. Selezionare **Crea utente**.

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

Eliminazione degli utenti locali

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

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

Fasi

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

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

Informazioni correlate

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

Gestione degli account tenant S3

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

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

- ["Gestione dei bucket S3"](#)

Gestione delle chiavi di accesso S3

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

A proposito di questa attività

Le chiavi di accesso S3 possono essere gestite come segue:

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

StorageGRID supporta l'autenticazione Firma versione 2 e Firma versione 4. L'accesso multiaccount non è consentito a meno che non sia esplicitamente abilitato da una policy bucket.

Creazione di chiavi di accesso S3 personalizzate

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

Di cosa hai bisogno

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

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 che consentono di creare e gestire i bucket per l'account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quelle necessarie ed eliminare le chiavi non utilizzate. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

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

- Impostare una scadenza per le chiavi in modo da limitare l'accesso a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre il rischio in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio di protezione nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare una scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.



È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

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

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

2. Selezionare **Crea chiave**.

3. Effettuare una delle seguenti operazioni:

- Selezionare **non impostare una scadenza** per creare una chiave che non scadrà. (Impostazione predefinita)
- Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.

1 Choose expiration time ————— 2 Download access key

Choose expiration time

Do not set an expiration time
This access key will never expire.

Set an expiration time

MM/DD/YYYY HH : MM AM

Cancel **Create access key**

4. Selezionare **Crea chiave di accesso**.

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

5. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.



Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni.

Create access key

Choose expiration time ————— 2 Download access key

Download access key

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

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

Access key ID

SHTBQKDRVHQ34YKKUAWX

Secret access key

UGu9+XeACtnOWQYFdbzmgmgVXXDvCkSOzT10sz9K

Download .csv Finish

6. Selezionare **fine**.

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

Informazioni correlate

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

Visualizzazione delle chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile visualizzare un elenco delle chiavi di accesso S3. È possibile ordinare l'elenco in base alla data di scadenza, in modo da determinare quali chiavi scadranno a breve. In base alle esigenze, è possibile creare nuove chiavi o eliminare chiavi che non vengono più utilizzate.

Di cosa hai bisogno

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



È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

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

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

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

2. Ordinare le chiavi in base a **scadenza** o **ID chiave di accesso**.
3. Se necessario, creare nuove chiavi ed eliminarle manualmente che non si stanno più utilizzando.

Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, è possibile iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

"Creazione di chiavi di accesso S3 personalizzate"

"Eliminazione delle proprie chiavi di accesso S3"

Eliminazione delle proprie chiavi di accesso S3

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le proprie chiavi di accesso S3. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Di cosa hai bisogno

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



È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

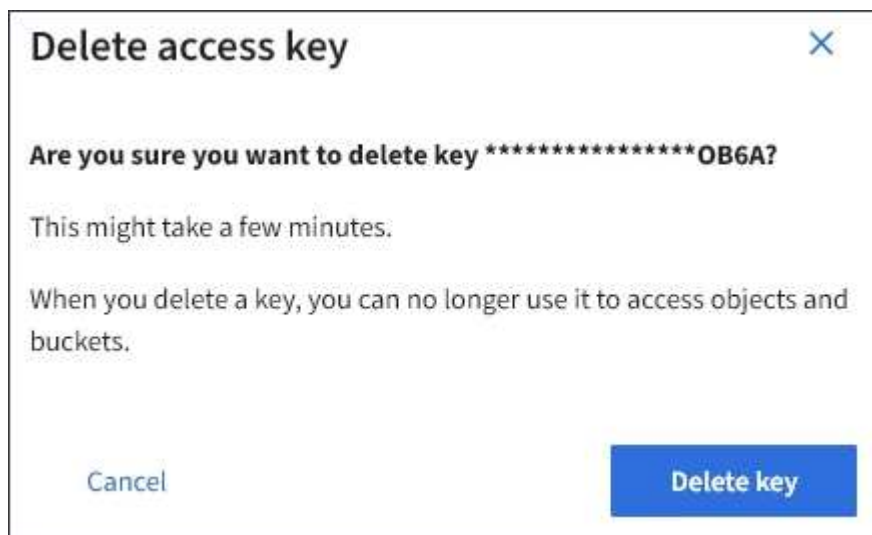
Fasi

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

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

2. Selezionare la casella di controllo per ogni chiave di accesso che si desidera rimuovere.
3. Selezionare **Delete key** (Elimina chiave).

Viene visualizzata una finestra di dialogo di conferma.



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

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

Informazioni correlate

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

Creazione delle chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare chiavi di accesso S3 per altri utenti, ad esempio applicazioni che richiedono l'accesso a bucket e oggetti.

Di cosa hai bisogno

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

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 per altri utenti in modo che possano creare e gestire i bucket per il proprio account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quelle richieste dall'utente ed eliminare le chiavi non utilizzate. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

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

- Impostare una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre i rischi in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio di protezione nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare una scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.



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

Fasi

1. Selezionare **ACCESS MANAGEMENT > Users**.
2. Selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

Viene visualizzata la pagina User Detail (Dettagli utente).

3. Selezionare **Access keys**, quindi selezionare **Create key**.
4. Effettuare una delle seguenti operazioni:
 - Selezionare **non impostare una scadenza** per creare una chiave che non scade. (Impostazione predefinita)
 - Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.


Create access key

1 Choose expiration time ————— 2 Download access key

Choose expiration time

Do not set an expiration time
This access key will never expire.

Set an expiration time

MM/DD/YYYY  HH : MM AM

Cancel **Create access key**

5. Selezionare **Crea chiave di accesso**.

Viene visualizzata la finestra di dialogo Download access key (Scarica chiave di accesso), che elenca l'ID della chiave di accesso e la chiave di accesso segreta.

6. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.



Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni.

Create access key


Choose expiration time ————— 2 Download access key

Download access key


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



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

Access key ID

SHTBQKDRVHQ34YKKUAWX 

Secret access key

UGu9+XeACtnOWQYFdbzmgmgVXXDvCkSOzT1Osz9K 

7. Selezionare **fine**.

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

Informazioni correlate

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

Visualizzazione delle chiavi di accesso S3 di un altro utente

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

Di cosa hai bisogno

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



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

Fasi

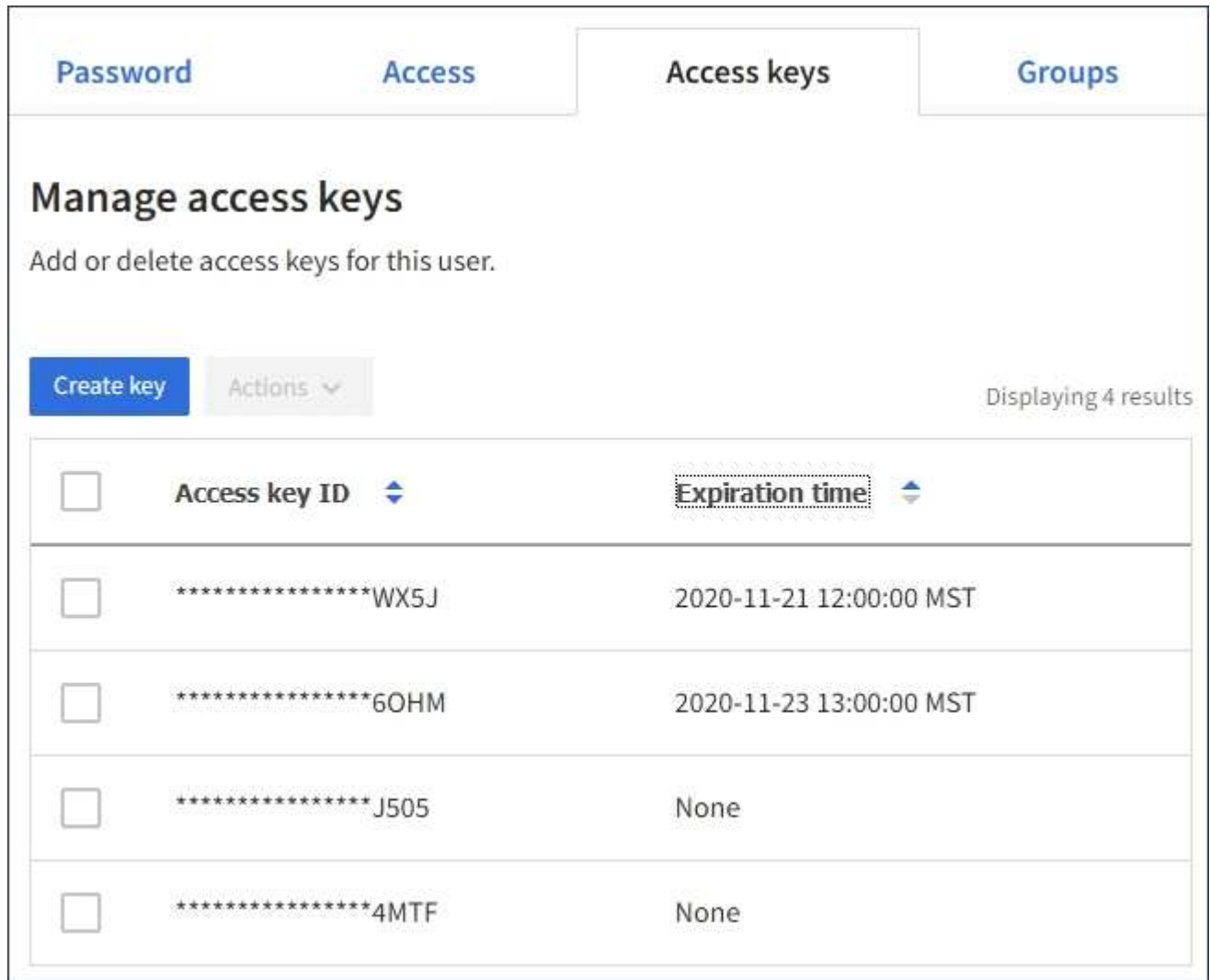
1. Selezionare **ACCESS MANAGEMENT > Users**.

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

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

Viene visualizzata la pagina User Details (Dettagli utente).

3. Selezionare **Access keys**.



The screenshot shows the 'Manage access keys' page in the AWS IAM console. The page has a navigation bar with tabs for 'Password', 'Access', 'Access keys', and 'Groups'. The 'Access keys' tab is selected. Below the navigation bar, the page title is 'Manage access keys' and the subtitle is 'Add or delete access keys for this user.' There is a 'Create key' button and an 'Actions' dropdown menu. The page indicates 'Displaying 4 results'. The table below shows the following data:

<input type="checkbox"/>	Access key ID	Expiration time
<input type="checkbox"/>	*****WX5J	2020-11-21 12:00:00 MST
<input type="checkbox"/>	*****6OHM	2020-11-23 13:00:00 MST
<input type="checkbox"/>	*****J505	None
<input type="checkbox"/>	*****4MTF	None

4. Ordinare le chiavi in base a **scadenza** o **ID chiave di accesso**.
5. Se necessario, creare nuove chiavi ed eliminare manualmente le chiavi che non sono più in uso.

Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, l'utente può iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

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

Eliminazione delle chiavi di accesso S3 di un altro utente

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le chiavi di accesso S3 di un altro utente. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Di cosa hai bisogno

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



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

Fasi

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

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

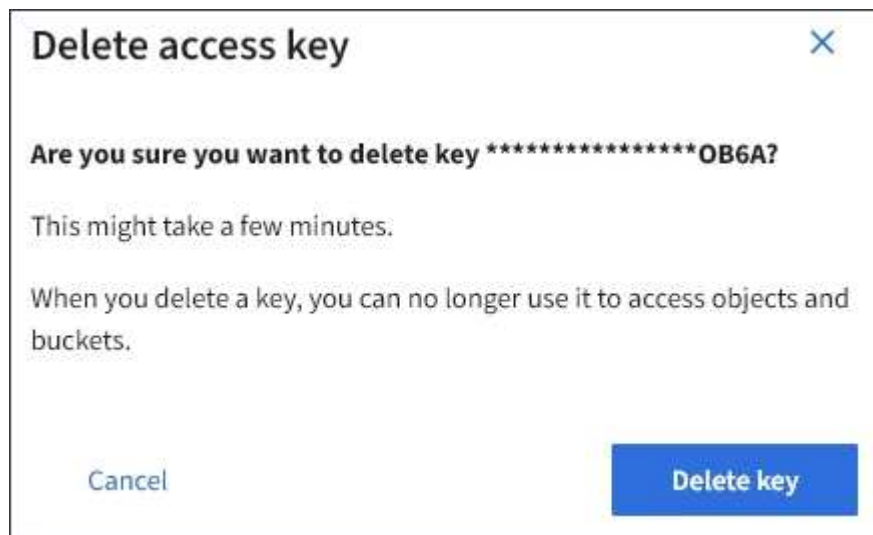
2. Selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

Viene visualizzata la pagina User Details (Dettagli utente).

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

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

Viene visualizzata una finestra di dialogo di conferma.



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

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

Informazioni correlate

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

Gestione dei bucket S3

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

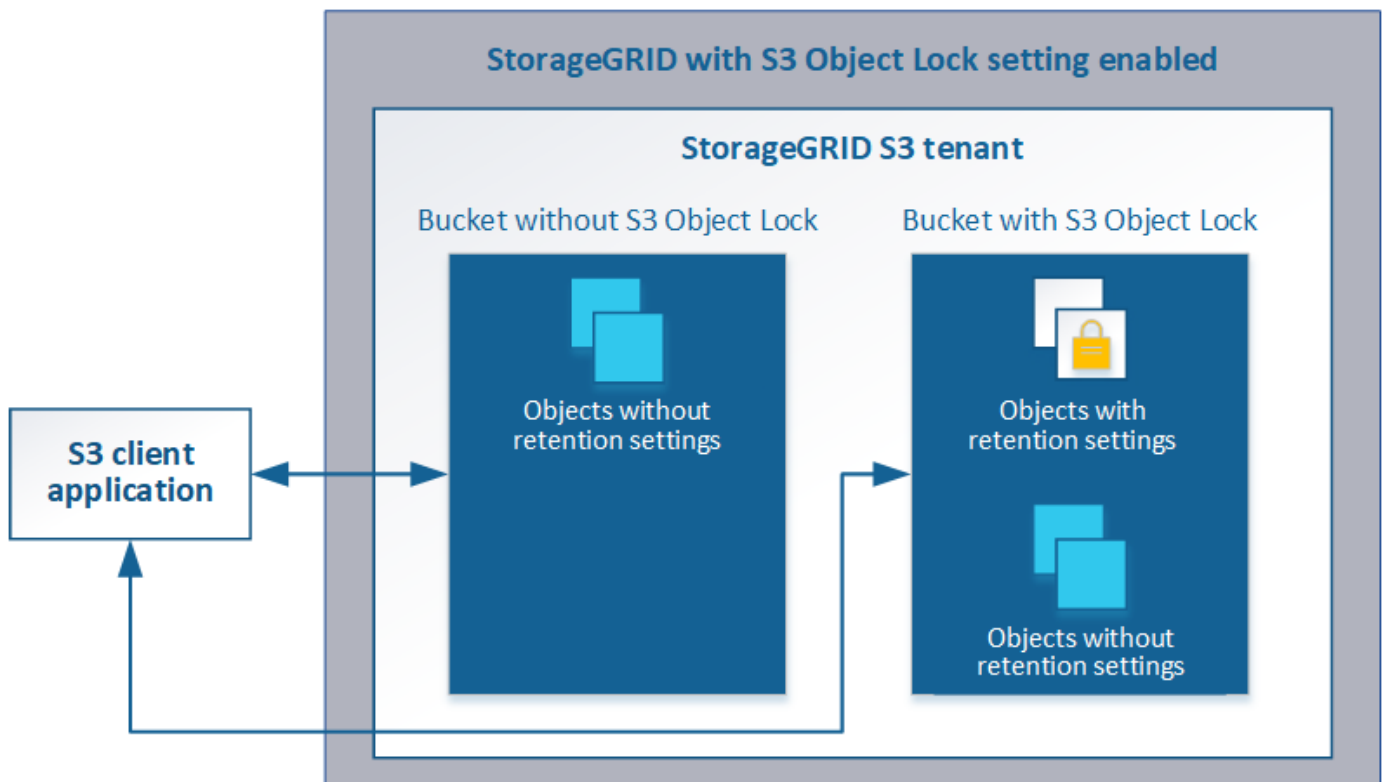
Utilizzo di S3 Object Lock

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

Che cos'è il blocco oggetti S3?

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

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



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

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

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

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

Gestione dei bucket conformi alle versioni precedenti

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

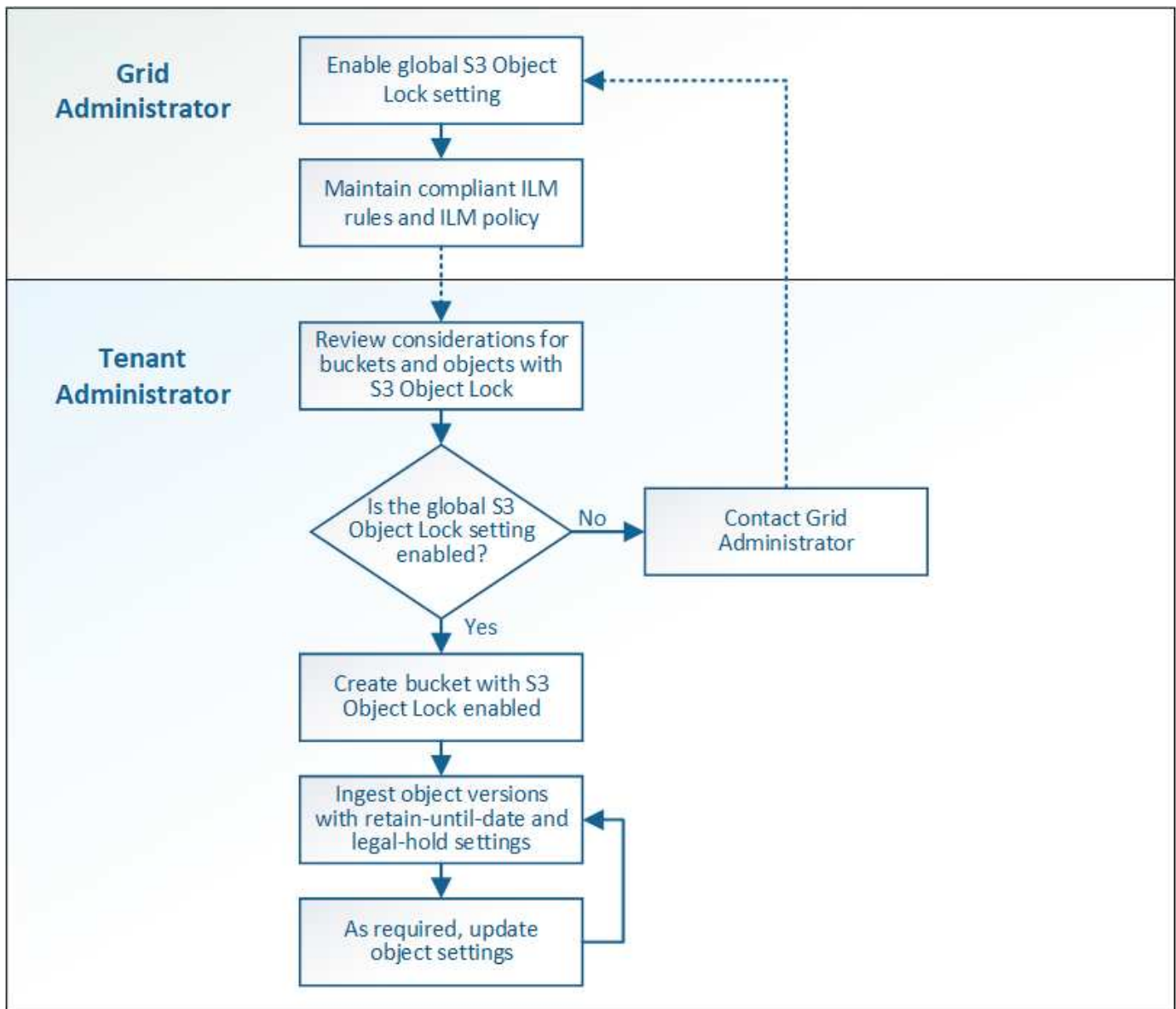
["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Workflow di blocco oggetti S3

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

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

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



Informazioni correlate

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

Requisiti per il blocco oggetti S3

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

Requisiti per i bucket con S3 Object Lock attivato

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

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

Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock  ▾	Region ▾	Object Count  ▾	Space Used  ▾	Date Created ▾
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

- 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

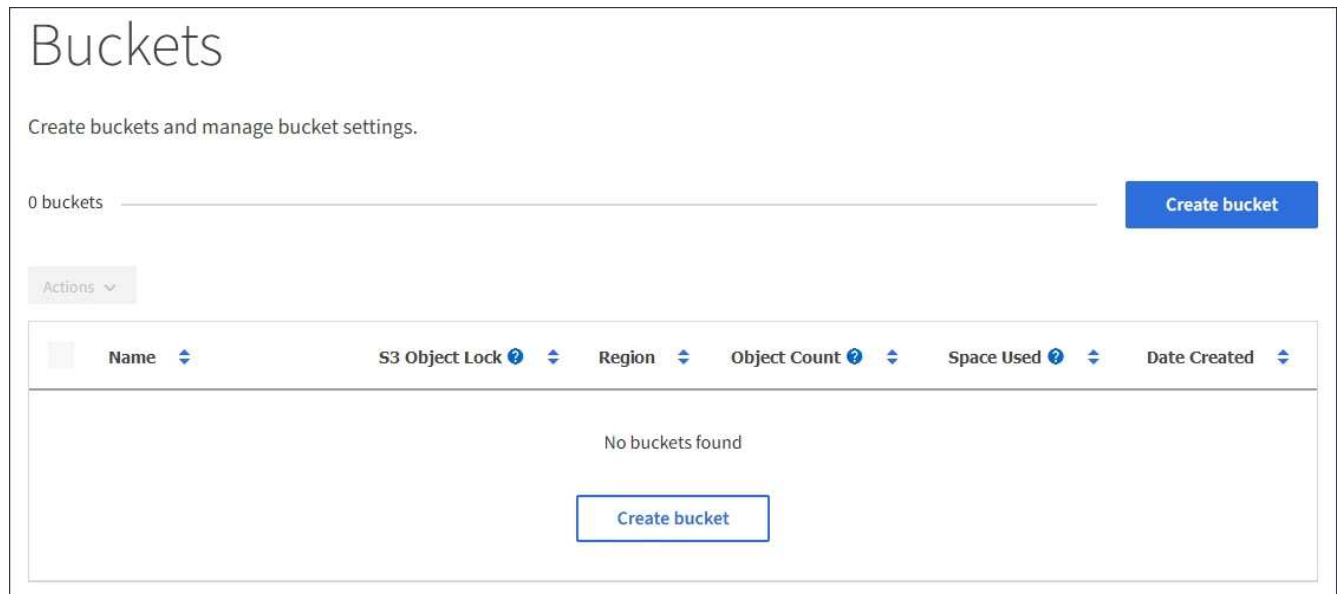
- È necessario accedere a tenant Manager utilizzando un browser supportato.
- È necessario appartenere a un gruppo di utenti che disponga dell'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni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

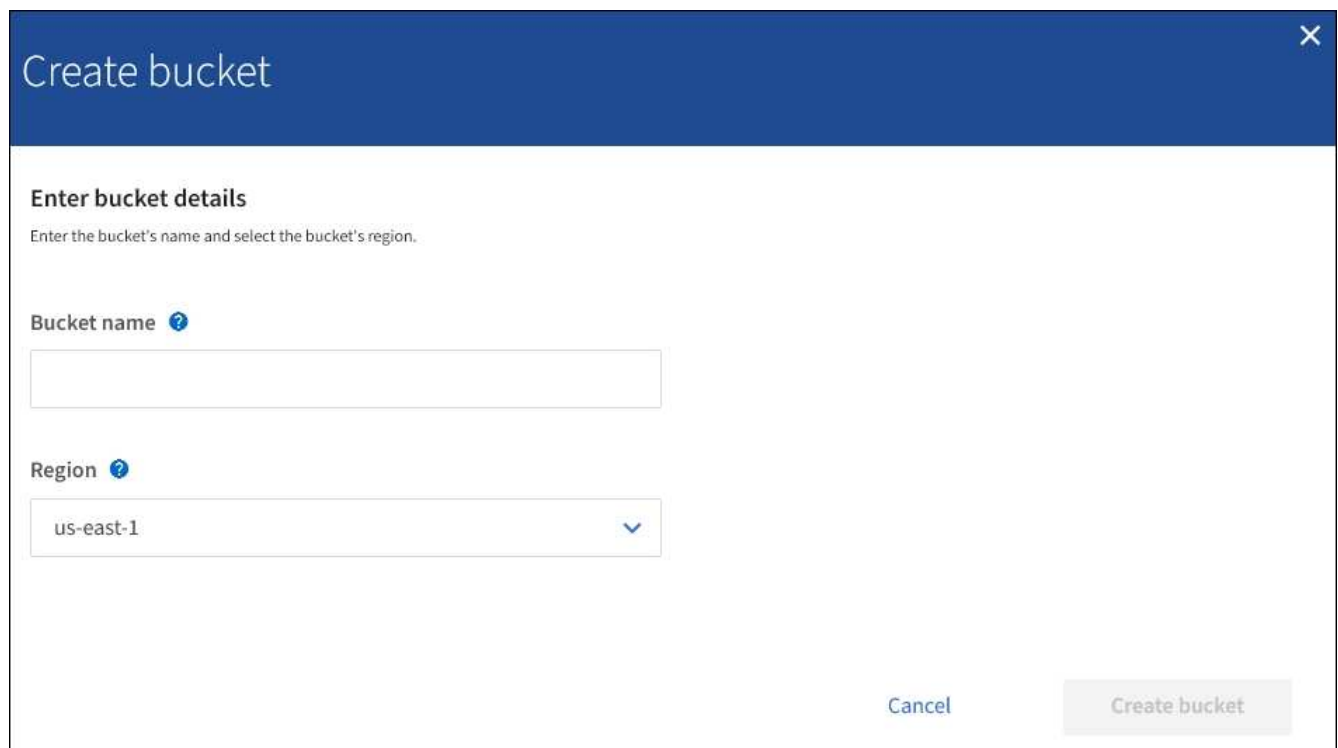
1. Selezionare **STORAGE (S3) > Bucket**.

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).

Create bucket

Enter details ———— 2 Manage S3 Object Lock
Optional

Manage S3 Object Lock (This step is optional)

S3 Object Lock allows you to specify retention and legal hold settings for the objects ingested into a bucket. If you want to use S3 Object Lock, you must enable this setting when you create the bucket. You cannot add or disable S3 Object Lock after a bucket is created.

If S3 Object Lock is enabled, bucket versioning is required and will be enabled automatically.

Enable S3 Object Lock

Previous **Create bucket**

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.

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

2. Esaminare le informazioni relative a ciascun bucket.

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

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

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

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



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

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

Viene visualizzata la pagina dei dettagli del bucket.

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

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

Buckets > bucket-02

Overview

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

Bucket options Bucket access Platform services

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

Informazioni correlate

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

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

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

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

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

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

Modifica del livello di coerenza

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

Di cosa hai bisogno

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

A proposito di questa attività

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

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



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

Fasi

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

Viene visualizzata la pagina dei dettagli del bucket.

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

Bucket options
Bucket access
Platform services

Consistency level
Read-after-new-write (default)
⤴

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

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

- All
Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.
- Strong-global
Guarantees read-after-write consistency for all client requests across all sites.
- Strong-site
Guarantees read-after-write consistency for all client requests within a site.
- Read-after-new-write (default)**
Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

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

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

Save changes

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

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

Livello di coerenza	Descrizione
Sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
Read-after-new-write (valore predefinito)	<p>Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Corrisponde alle garanzie di coerenza di Amazon S3.</p> <p>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.</p>
Disponibile (eventuale coerenza per le operazioni TESTA)	Si comporta come il livello di coerenza Read-after-new-write , ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a Read-after-new-write se i nodi storage non sono disponibili. Differisce dalle garanzie di coerenza di Amazon S3 solo per le operazioni HEAD.

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	<ul style="list-style-type: none"> No, per la copia di origine Sì, per la copia di destinazione 	<ul style="list-style-type: none"> No, per la copia di origine Sì, per la copia di destinazione 	<ul style="list-style-type: none"> Sì, per la copia di origine Sì, per la copia di destinazione 	<ul style="list-style-type: none"> 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.

The screenshot shows the 'Bucket options' tab in the AWS S3 console. It features three sub-tabs: 'Bucket options', 'Bucket access', and 'Platform services'. Under 'Bucket options', there are two main sections: 'Consistency level' (set to 'Read-after-new-write') and 'Last access time updates' (set to 'Disabled'). Below the 'Last access time updates' section, there is explanatory text and a list of behaviors when updates are disabled. A yellow warning box highlights that updating the last access time can reduce performance. At the bottom, there are two radio buttons: 'Enable last access time updates when retrieving an object' (unselected) and 'Disable last access time updates when retrieving an object' (selected). A 'Save changes' button is located at the bottom right of the panel.

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

Informazioni correlate

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

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).

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

Cross-Origin Resource Sharing (CORS) Disabled

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

Enable CORS

Clear

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

Save changes

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

8. Per disattivare il CORS per il bucket, deselegionare 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.

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

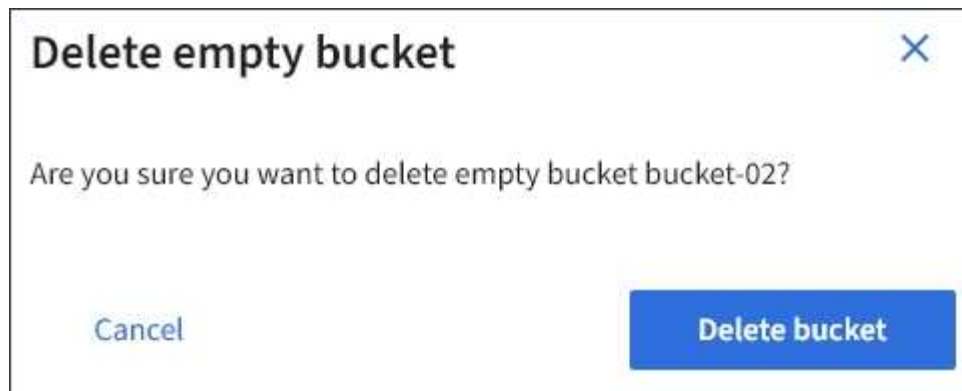
2. Selezionare la casella di controllo per il bucket vuoto che si desidera eliminare.

Il menu Actions (azioni) è attivato.

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

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

Viene visualizzato un messaggio di conferma.



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

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

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



Informazioni correlate

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

Gestione dei servizi della piattaforma S3

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

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

Quali sono i servizi della piattaforma

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

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

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

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



La replica di CloudMirror non è supportata se il bucket di origine ha attivato il blocco oggetti S3.

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

Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.



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

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

Ad esempio, è possibile configurare i bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. È quindi possibile utilizzare Elasticsearch per eseguire ricerche tra bucket ed eseguire analisi sofisticate dei modelli presenti nei metadati degli oggetti.



Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock attivato, i metadati S3 Object Lock (inclusi Retain until Date e Legal Hold status) degli oggetti non saranno inclusi nei messaggi di notifica.

Poiché la posizione di destinazione dei servizi della piattaforma è generalmente esterna all'implementazione di StorageGRID, i servizi della piattaforma offrono la potenza e la flessibilità derivanti dall'utilizzo di risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi per i dati.

È possibile configurare qualsiasi combinazione di servizi di piattaforma per un singolo bucket S3. Ad esempio, è possibile configurare il servizio CloudMirror e le notifiche su un bucket StorageGRID S3 in modo da eseguire il mirroring di oggetti specifici al servizio di storage semplice Amazon, inviando una notifica relativa a ciascun oggetto a un'applicazione di monitoraggio di terze parti per tenere traccia delle spese AWS.



L'utilizzo dei servizi della piattaforma deve essere abilitato per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione del grid.

Modalità di configurazione dei servizi della piattaforma

I servizi della piattaforma comunicano con gli endpoint esterni configurati utilizzando Tenant Manager o l'API di gestione tenant. Ogni endpoint rappresenta una destinazione esterna, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento SNS (Simple Notification Service) o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

Dopo aver creato un endpoint, è possibile attivare un servizio di piattaforma per un bucket aggiungendo la

configurazione XML al bucket. La configurazione XML identifica gli oggetti su cui il bucket deve agire, l'azione che il bucket deve intraprendere e l'endpoint che il bucket deve utilizzare per il servizio.

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

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

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

Servizio di piattaforma	API REST S3
Replica di CloudMirror	<ul style="list-style-type: none">• OTTIENI la replica bucket• METTI la replica del bucket
Notifiche	<ul style="list-style-type: none">• OTTIENI notifica bucket• NOTIFICA DEL bucket
Integrazione della ricerca	<ul style="list-style-type: none">• OTTIENI la configurazione della notifica dei metadati del bucket• INSERIRE la configurazione della notifica dei metadati del bucket <p>Queste operazioni sono personalizzate per StorageGRID.</p>

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

Informazioni correlate

["Utilizzare S3"](#)

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

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

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

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

Informazioni sul servizio di replica CloudMirror

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

La replica di CloudMirror funziona indipendentemente dal criterio ILM attivo del grid. Il servizio CloudMirror

replica gli oggetti memorizzati nel bucket di origine e li consegna al bucket di destinazione il prima possibile. La consegna degli oggetti replicati viene attivata quando l'acquisizione degli oggetti ha esito positivo.

Se si attiva la replica CloudMirror per un bucket esistente, vengono replicati solo i nuovi oggetti aggiunti a tale bucket. Gli oggetti esistenti nel bucket non vengono replicati. Per forzare la replica degli oggetti esistenti, è possibile aggiornare i metadati dell'oggetto esistente eseguendo una copia dell'oggetto.



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

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

Inoltre, è possibile configurare la replica di CloudMirror su bucket con versione o senza versione e specificare un bucket con versione o senza versione come destinazione. È possibile utilizzare qualsiasi combinazione di bucket con versione e senza versione. Ad esempio, è possibile specificare un bucket con versione come destinazione per un bucket di origine senza versione o viceversa. È inoltre possibile eseguire la replica tra bucket senza versione.

Il comportamento di eliminazione per il servizio di replica CloudMirror è lo stesso del comportamento di eliminazione del servizio CRR (Cross Region Replication) fornito da Amazon S3: L'eliminazione di un oggetto in un bucket di origine non elimina mai un oggetto replicato nella destinazione. Se sia il bucket di origine che quello di destinazione sono entrambi con versione, il marker di eliminazione viene replicato. Se il bucket di destinazione non è dotato di versione, l'eliminazione di un oggetto nel bucket di origine non replica il marker di eliminazione nel bucket di destinazione né elimina l'oggetto di destinazione.

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



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

L'unicità e l'ordinamento degli eventi nel bucket di destinazione non sono garantiti. Più di una copia identica di un oggetto di origine potrebbe essere consegnata alla destinazione in seguito alle operazioni eseguite per garantire il successo della consegna. In rari casi, quando lo stesso oggetto viene aggiornato simultaneamente da due o più siti StorageGRID diversi, l'ordine delle operazioni sul bucket di destinazione potrebbe non corrispondere all'ordine degli eventi sul bucket di origine.

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

Informazioni correlate

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

Informazioni sulle notifiche per i bucket

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

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

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

L'unicità e l'ordine delle notifiche non sono garantiti. È possibile che più di una notifica di un evento venga inviata alla destinazione a seguito delle operazioni eseguite per garantire il successo della consegna. Inoltre, poiché la consegna è asincrona, non è garantito che l'ordine temporale delle notifiche alla destinazione corrisponda all'ordine degli eventi nel bucket di origine, in particolare per le operazioni provenienti da diversi siti StorageGRID. È possibile utilizzare `sequencer` Digitare il messaggio dell'evento per determinare l'ordine degli eventi per un particolare oggetto, come descritto nella documentazione di Amazon S3.

Notifiche e messaggi supportati

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

- Non è possibile configurare una notifica per i seguenti tipi di eventi. Questi tipi di evento sono **non** supportati.
 - `s3:ReducedRedundancyLostObject`
 - `s3:ObjectRestore:Completed`
- Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ad eccezione del fatto che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nella tabella:

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

Informazioni correlate

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

Informazioni sul servizio di integrazione della ricerca

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

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

È possibile attivare il servizio di integrazione della ricerca per qualsiasi bucket con versione o senza versione. L'integrazione della ricerca viene configurata associando XML di configurazione della notifica dei metadati al bucket che specifica gli oggetti su cui agire e la destinazione dei metadati dell'oggetto.

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



Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

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

- Viene creato un oggetto.
- Un oggetto viene eliminato, anche quando gli oggetti vengono eliminati in seguito all'operazione della policy ILM della griglia.
- I tag o i metadati degli oggetti vengono aggiunti, aggiornati o cancellati. L'insieme completo di metadati e tag viene sempre inviato in seguito all'aggiornamento, non solo i valori modificati.

Dopo aver aggiunto XML per la configurazione delle notifiche dei metadati a un bucket, vengono inviate notifiche per i nuovi oggetti creati e per gli oggetti modificati aggiornando i dati, i metadati dell'utente o i tag. Tuttavia, non vengono inviate notifiche per oggetti già presenti nel bucket. Per garantire che i metadati degli oggetti per tutti gli oggetti nel bucket vengano inviati alla destinazione, eseguire una delle seguenti operazioni:

- Configurare il servizio di integrazione della ricerca subito dopo la creazione del bucket e prima di aggiungere oggetti.
- Eseguire un'azione su tutti gli oggetti già presenti nel bucket che attiverà l'invio di un messaggio di notifica dei metadati alla destinazione.

Il servizio di integrazione della ricerca di StorageGRID supporta un cluster Elasticsearch come destinazione. Come per gli altri servizi della piattaforma, la destinazione viene specificata nell'endpoint il cui URN viene utilizzato nel XML di configurazione per il servizio. Utilizzare il *Interoperability Matrix Tool* per determinare le versioni supportate di Elasticsearch.

Informazioni correlate

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

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

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

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

Considerazioni sull'utilizzo dei servizi della piattaforma

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

Considerazioni sull'utilizzo dei servizi della piattaforma

Considerazione	Dettagli
Monitoraggio degli endpoint di destinazione	<p>È necessario monitorare la disponibilità di ciascun endpoint di destinazione. Se la connettività all'endpoint di destinazione viene persa per un periodo di tempo prolungato ed esiste un grande backlog di richieste, le richieste client aggiuntive (come LE richieste PUT) a StorageGRID non avranno esito positivo. È necessario riprovare queste richieste non riuscite quando l'endpoint diventa raggiungibile.</p>
Rallentamento dell'endpoint di destinazione	<p>Il software StorageGRID potrebbe ridurre le richieste S3 in entrata per un bucket se la velocità con cui le richieste vengono inviate supera la velocità con cui l'endpoint di destinazione può ricevere le richieste. La limitazione si verifica solo quando è presente un backlog di richieste in attesa di essere inviate all'endpoint di destinazione.</p> <p>L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, le operazioni del client S3 (come LE richieste PUT) finiranno per fallire.</p> <p>È più probabile che le richieste CloudMirror siano influenzate dalle performance dell'endpoint di destinazione, perché queste richieste comportano in genere un maggior numero di trasferimenti di dati rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.</p>
Garanzie di ordinazione	<p>StorageGRID garantisce l'ordine delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni relative a un oggetto si trovano all'interno dello stesso sito, lo stato finale dell'oggetto (per la replica) sarà sempre uguale allo stato in StorageGRID.</p> <p>StorageGRID tenta al meglio di ordinare le richieste quando le operazioni vengono eseguite nei siti StorageGRID. Ad esempio, se si scrive inizialmente un oggetto nel sito A e successivamente si sovrascrive lo stesso oggetto nel sito B, l'oggetto finale replicato da CloudMirror nel bucket di destinazione non è garantito come l'oggetto più recente.</p>

Considerazione	Dettagli
Eliminazioni di oggetti basate su ILM	<p>Per far corrispondere il comportamento di eliminazione dei servizi CRR e SNS di AWS, CloudMirror e le richieste di notifica degli eventi non vengono inviate quando un oggetto nel bucket di origine viene cancellato a causa delle regole ILM di StorageGRID. Ad esempio, se una regola ILM elimina un oggetto dopo 14 giorni, non viene inviata alcuna richiesta di notifica di CloudMirror o di evento.</p> <p>Al contrario, le richieste di integrazione della ricerca vengono inviate quando gli oggetti vengono eliminati a causa di ILM.</p>

Considerazioni sull'utilizzo del servizio di replica CloudMirror

Considerazione	Dettagli
Stato della replica	StorageGRID non supporta <code>x-amz-replication-status</code> intestazione.
Dimensione dell'oggetto	La dimensione massima per gli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è di 5 TB, che corrisponde alla dimensione massima degli oggetti supportata da StorageGRID.
Versioni e ID della versione del bucket	<p>Se il bucket S3 di origine in StorageGRID ha attivato la versione, è necessario attivare anche la versione per il bucket di destinazione.</p> <p>Quando si utilizza la versione, tenere presente che l'ordinamento delle versioni degli oggetti nel bucket di destinazione è il massimo sforzo e non garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3.</p> <p>Nota: Gli ID della versione per il bucket di origine in StorageGRID non sono correlati agli ID della versione per il bucket di destinazione.</p>

<p>Tagging per le versioni degli oggetti</p>	<p>Il servizio CloudMirror non replica alcuna richiesta DI tag DEGLI oggetti PUT o DELETE che fornisca un ID di versione, a causa delle limitazioni del protocollo S3. Poiché gli ID di versione per l'origine e la destinazione non sono correlati, non esiste alcun modo per garantire che venga replicato un tag aggiornato a un ID di versione specifico.</p> <p>Al contrario, il servizio CloudMirror replica le richieste DI tagging DEGLI oggetti PUT o ELIMINA le richieste di tagging degli oggetti che non specificano un ID di versione. Queste richieste aggiornano i tag per la chiave più recente (o la versione più recente se il bucket è in versione). Vengono replicati anche i normali ingest con tag (senza tagging degli aggiornamenti).</p>
<p>Caricamenti multiparte e. ETag valori</p>	<p>Quando si esegue il mirroring degli oggetti caricati utilizzando un caricamento multiparte, il servizio CloudMirror non conserva le parti. Di conseguenza, il ETag il valore dell'oggetto mirrorato sarà diverso da ETag valore dell'oggetto originale.</p>
<p>Oggetti crittografati con SSE-C (crittografia lato server con chiavi fornite dal cliente)</p>	<p>Il servizio CloudMirror non supporta gli oggetti crittografati con SSE-C. Se si tenta di acquisire un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione non riesce.</p>
<p>Bucket con blocco oggetti S3 attivato</p>	<p>Se il bucket S3 di destinazione per la replica CloudMirror ha attivato il blocco oggetti S3, l'operazione di replica non riesce e viene visualizzato un errore AccessDenied.</p>

Informazioni correlate

["Utilizzare S3"](#)

Configurazione degli endpoint dei servizi di piattaforma

Prima di poter configurare un servizio di piattaforma per un bucket, è necessario configurare almeno un endpoint in modo che sia la destinazione del servizio di piattaforma.

L'accesso ai servizi della piattaforma viene attivato per tenant da un amministratore di StorageGRID. Per creare o utilizzare un endpoint di servizi di piattaforma, è necessario essere un utente tenant con autorizzazione Manage Endpoints (Gestisci endpoint) o Root Access (accesso root), in una griglia la cui rete è stata configurata per consentire ai nodi di storage di accedere alle risorse esterne degli endpoint. Per ulteriori informazioni, contattare l'amministratore di StorageGRID.

Che cos'è un endpoint di servizi di piattaforma

Quando si crea un endpoint di servizi di piattaforma, si specificano le informazioni necessarie a StorageGRID per accedere alla destinazione esterna.

Ad esempio, se si desidera replicare gli oggetti da un bucket StorageGRID a un bucket S3, si crea un endpoint dei servizi della piattaforma che include le informazioni e le credenziali necessarie a StorageGRID per accedere al bucket di destinazione su AWS.

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

È possibile utilizzare lo stesso endpoint della destinazione per più bucket di origine. Ad esempio, è possibile configurare diversi bucket di origine per inviare metadati di oggetto allo stesso endpoint di integrazione della ricerca, in modo da poter eseguire ricerche in più bucket. È inoltre possibile configurare un bucket di origine in modo che utilizzi più di un endpoint come destinazione, consentendo di eseguire operazioni come l'invio di notifiche sulla creazione di oggetti a un singolo argomento SNS e le notifiche sull'eliminazione di oggetti a un secondo argomento SNS.

Endpoint per la replica di CloudMirror

StorageGRID supporta endpoint di replica che rappresentano i bucket S3. Questi bucket potrebbero essere ospitati su Amazon Web Services, sullo stesso o in un'implementazione remota di StorageGRID o su un altro servizio.

Endpoint per le notifiche

StorageGRID supporta endpoint SNS (Simple Notification Service). Gli endpoint SQS (Simple Queue Service) o AWS Lambda non sono supportati.

Endpoint per il servizio di integrazione della ricerca

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

L'endpoint di integrazione della ricerca si riferisce a un tipo e un indice Elasticsearch specifici. È necessario creare l'indice in Elasticsearch prima di creare l'endpoint in StorageGRID, altrimenti la creazione dell'endpoint non avrà esito positivo. Non è necessario creare il tipo prima di creare l'endpoint. StorageGRID crea il tipo, se necessario, quando invia i metadati dell'oggetto all'endpoint.

Informazioni correlate

["Amministrare StorageGRID"](#)

Specifica dell'URN per un endpoint di servizi di piattaforma

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

StorageGRID convalida gli endpoint dei servizi della piattaforma durante la loro creazione. Prima di creare un endpoint di servizi di piattaforma, verificare che la risorsa specificata nell'endpoint esista e che sia possibile

raggiungerla.

Elementi DI URNA

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

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

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

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

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

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

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

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

Urns per i servizi ospitati su AWS

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

- Replica di CloudMirror:

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

- Notifiche:

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

- Integrazione della ricerca:

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



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

Urns per servizi in hosting locale

Quando si utilizzano servizi ospitati in locale invece di servizi cloud, è possibile specificare l'URN in qualsiasi modo che crei un URN valido e univoco, purché l'URN includa gli elementi richiesti nella terza e ultima posizione. È possibile lasciare vuoti gli elementi indicati da opzionale oppure specificarli in qualsiasi modo che consenta di identificare la risorsa e rendere l'URN unico. Ad esempio:

- Replica di CloudMirror:

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

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

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

- Notifiche:

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

- Integrazione della ricerca:

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



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

Creazione di un endpoint di servizi di piattaforma

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

Di cosa hai bisogno

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



Se si prevede di utilizzare un bucket ospitato su un sistema StorageGRID come endpoint per la replica di CloudMirror, contattare l'amministratore del grid per determinare i valori da inserire.

- Nome risorsa univoco (URN)

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

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

Fasi

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

Viene visualizzata la pagina Platform Services Endpoint.

Platform services endpoints

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

0 endpoints

Create endpoint

Delete endpoint

	Display name ?	Last error ?	Type ?	URI ?	URN ?
No endpoints found					
<p>Create endpoint</p>					

2. Selezionare **Crea endpoint**.

Create endpoint

1 Enter details — 2 Select authentication type Optional — 3 Verify server Optional

Enter endpoint details

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

Display name ?

URI ?

URN ?

Cancel Continue

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

Il tipo di servizio della piattaforma supportato dall'endpoint viene visualizzato accanto al nome dell'endpoint quando viene elencato nella pagina degli endpoint, quindi non è necessario includere tali informazioni nel nome.

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

Utilizzare uno dei seguenti formati:

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

Se non si specifica una porta, la porta 443 viene utilizzata per gli URI HTTPS e la porta 80 per gli URI HTTP.

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

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

In questo esempio, `s3.example.com` Rappresenta la voce DNS per l'IP virtuale (VIP) del gruppo ha

(StorageGRID High Availability), e. 10443 rappresenta la porta definita nell'endpoint del bilanciamento del carico.



Quando possibile, è necessario connettersi a un gruppo ha di nodi per il bilanciamento del carico per evitare un singolo punto di errore.

Analogamente, l'URI per un bucket ospitato su AWS potrebbe essere:

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



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

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



Non è possibile modificare l'URN di un endpoint dopo la creazione dell'endpoint.

6. Selezionare **continua**.

7. Selezionare un valore per **Authentication type** (tipo di autenticazione), quindi immettere le credenziali richieste.

The screenshot shows a 'Create endpoint' wizard with three steps: 1. Enter details, 2. Select authentication type (Optional), and 3. Verify server (Optional). Step 2 is active. The 'Authentication type' dropdown menu is open, showing three options: 'Anonymous' (selected), 'Access Key', and 'Basic HTTP'. At the bottom right, there are 'Previous' and 'Continue' buttons.

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

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	<ul style="list-style-type: none">• ID chiave di accesso• Chiave di accesso segreta
HTTP di base	Utilizza un nome utente e una password per autenticare le connessioni alla destinazione.	<ul style="list-style-type: none">• Nome utente• Password

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

Create endpoint

Enter details — Select authentication type (Optional) — **3 Verify server (Optional)**

Verify server

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

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abcdefghijklmnopkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklmnopklABCD
-----END CERTIFICATE-----
```

Previous Test and create endpoint

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

10. Selezionare **Test e creare endpoint**.

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



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

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

Informazioni correlate

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

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

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

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

Verifica della connessione per un endpoint di servizi di piattaforma

Se la connessione a un servizio della piattaforma è stata modificata, è possibile verificare la connessione per l'endpoint per verificare l'esistenza della risorsa di destinazione e che sia possibile raggiungerla utilizzando le credenziali specificate.

Di cosa hai bisogno

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

A proposito di questa attività

StorageGRID non convalida che le credenziali dispongano delle autorizzazioni corrette.

Fasi

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

Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.

Platform services endpoints

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

4 endpoints [Create endpoint](#)

[Delete endpoint](#)

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

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

Viene visualizzata la pagina dei dettagli dell'endpoint.

Overview ^

Display name:	my-endpoint-1 ✎
Type:	S3 Bucket
URI:	http://10.96.104.167:10443
URN:	urn:sgws:s3:::bucket1

Connection Configuration

Verify connection ?

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

Test connection

3. Selezionare **Test di connessione**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene convalidata da un nodo in ogni sito.
- Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Se è necessario modificare l'endpoint per correggere l'errore, selezionare **Configuration** (Configurazione) e aggiornare le informazioni. Quindi, selezionare **Test e salvare le modifiche**.

Modifica di un endpoint di servizi di piattaforma

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

Di cosa hai bisogno

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

Fasi

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

Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.







Platform services endpoints

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

4 endpoints

Create endpoint

Delete endpoint

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

2. Selezionare l'endpoint che si desidera modificare.

Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Configurazione**.

Overview

Display name: **my-endpoint-3** 

Type: **Notifications**

URI: **http://10.96.104.202:8080/**

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

Connection

Configuration

Edit configuration

Endpoint details

URI 

http://10.96.104.202:8080/

URN 

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

Authentication type 

Basic HTTP 

Username 

testme

Password 

••••••••

Edit password

Verify server 

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


```
-----BEGIN CERTIFICATE-----  
abcdefghijklmnop1234567890ABCDEFGHIJKL  
123456/7890ABCDEFabcdefghijklmnop123456  
-----END CERTIFICATE-----
```

Test and save changes

4. Se necessario, modificare la configurazione dell'endpoint.



Non è possibile modificare l'URN di un endpoint dopo la creazione dell'endpoint.

- a. Per modificare il nome visualizzato per l'endpoint, selezionare l'icona di modifica .
- b. Se necessario, modificare l'URI.
- c. Se necessario, modificare il tipo di autenticazione.
 - Per l'autenticazione HTTP di base, modificare il nome utente in base alle necessità. Modificare la password in base alle necessità selezionando **Modifica password** e immettendo la nuova password. Per annullare le modifiche, selezionare **Ripristina modifica password**.
 - Per l'autenticazione della chiave di accesso, modificare la chiave in base alle necessità selezionando **Modifica chiave S3** e incollando un nuovo ID della chiave di accesso e una chiave di accesso segreta. Se si desidera annullare le modifiche, selezionare **Ripristina modifica tasto S3**.
- d. Se necessario, modificare il metodo di verifica del server.

5. Selezionare **Test e salvare le modifiche**.

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

Informazioni correlate

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

Eliminazione di un endpoint dei servizi della piattaforma

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

Di cosa hai bisogno

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

Fasi

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

Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.







Platform services endpoints

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

4 endpoints

Create endpoint

Delete endpoint

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

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



Se elimini un endpoint di servizi di piattaforma in uso, il servizio di piattaforma associato verrà disattivato per tutti i bucket che utilizzano l'endpoint. Tutte le richieste non ancora completate verranno interrotte. Le nuove richieste continueranno a essere generate fino a quando non si modifica la configurazione del bucket per non fare più riferimento all'URN cancellato. StorageGRID segnalerà queste richieste come errori irrecuperabili.

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

Viene visualizzato un messaggio di conferma.

Delete endpoint

Are you sure you want to delete endpoint my-endpoint-10?

This might take a few minutes.

When you delete an endpoint, you can no longer use it to access external resources.

[Cancel](#) [Delete endpoint](#)


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

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

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi della piattaforma, viene visualizzato un messaggio nella dashboard. Nella pagina Platform Services Endpoint, la colonna Last error (ultimo errore) indica per quanto tempo si è verificato l'errore. Se le autorizzazioni associate alle credenziali di un endpoint non sono corrette, non viene visualizzato alcun errore.


Determinare se si è verificato un errore

Se si sono verificati errori degli endpoint dei servizi della piattaforma negli ultimi 7 giorni, il pannello di controllo di Tenant Manager visualizza un messaggio di avviso. Per ulteriori informazioni sull'errore, visitare la pagina relativa agli endpoint dei servizi della piattaforma.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Lo stesso errore visualizzato nella dashboard viene visualizzato anche nella parte superiore della pagina Platform Services Endpoint. Per visualizzare un messaggio di errore più dettagliato:

Fasi

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

Overview ^

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

Connection

Configuration

Verify connection

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

Test connection

Last error details

2 hours ago

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

Verifica della presenza di un errore

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

Fasi

1. Selezionare l'endpoint.

Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Selezionare **connessione** > **verifica connessione**.

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

Risoluzione degli errori degli endpoint

È possibile utilizzare il messaggio **Last error** (ultimo errore) nella pagina dei dettagli dell'endpoint per determinare la causa dell'errore. Alcuni errori potrebbero richiedere la modifica dell'endpoint per risolvere il problema. Ad esempio, se StorageGRID non riesce ad accedere al bucket S3 di destinazione perché non

91

dispone delle autorizzazioni di accesso corrette o la chiave di accesso è scaduta, può verificarsi un errore di CloudMirroring. Il messaggio è “è necessario aggiornare le credenziali dell’endpoint o l’accesso alla destinazione,” e i dettagli sono “AccessDenied” o “InvalidAccessKeyId”.

Se è necessario modificare l’endpoint per risolvere un errore: Selezionando **verifica e salva modifiche**, StorageGRID convalida l’endpoint aggiornato e conferma che è possibile raggiungerlo con le credenziali correnti. La connessione all’endpoint viene convalidata da un nodo in ogni sito.

Fasi

1. Selezionare l’endpoint.
2. Nella pagina dei dettagli dell’endpoint, selezionare **Configurazione**.
3. Modificare la configurazione dell’endpoint in base alle necessità.
4. Selezionare **connessione > verifica connessione**.

Credenziali endpoint con autorizzazioni insufficienti

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

Troubleshooting di servizi di piattaforma aggiuntivi

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

["Amministrare StorageGRID"](#)

Informazioni correlate

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

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

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

Configurazione della replica di CloudMirror

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

Di cosa hai bisogno

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

gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

La replica di CloudMirror copia gli oggetti da un bucket di origine a un bucket di destinazione specificato in un endpoint. Per attivare la replica CloudMirror per un bucket, è necessario creare e applicare un XML di configurazione valido per la replica del bucket. L'XML di configurazione della replica deve utilizzare l'URN di un endpoint del bucket S3 per ciascuna destinazione.



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

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

Se si attiva la replica di CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket vengono replicati, ma gli oggetti esistenti nel bucket non lo sono. È necessario aggiornare gli oggetti esistenti per attivare la replica.

Se si specifica una classe di storage nell'XML di configurazione della replica, StorageGRID utilizza tale classe quando esegue operazioni sull'endpoint S3 di destinazione. L'endpoint di destinazione deve supportare anche la classe di storage specificata. Assicurarsi di seguire le raccomandazioni fornite dal vendor del sistema di destinazione.

Fasi

1. Abilita la replica per il bucket di origine:

Utilizzare un editor di testo per creare l'XML di configurazione della replica richiesto per attivare la replica, come specificato nell'API di replica S3. Durante la configurazione dell'XML:

- Tenere presente che StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo di `Filter` Per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, consultare la documentazione di Amazon sulla configurazione della replica.
- Utilizzare l'URN di un endpoint del bucket S3 come destinazione.
- Se si desidera, aggiungere `<StorageClass>` e specificare una delle seguenti opzioni:
 - `STANDARD`: La classe di storage predefinita. Se non si specifica una classe di storage quando si carica un oggetto, il `STANDARD` viene utilizzata la classe di storage.
 - `STANDARD_IA`: (Standard - accesso non frequente). Utilizzare questa classe di storage per i dati a cui si accede meno frequentemente, ma che richiedono comunque un accesso rapido quando necessario.
 - `REDUCED_REDUNDANCY`: Utilizzare questa classe di storage per i dati non critici e riproducibili che possono essere memorizzati con una ridondanza inferiore rispetto a. `STANDARD` classe di storage.
- Se si specifica un `Role` Nel file XML di configurazione, verrà ignorato. Questo valore non viene utilizzato da StorageGRID.

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

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

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Replication**.

5. Selezionare la casella di controllo **Enable Replication** (attiva replica).

6. Incollare il file XML di configurazione della replica nella casella di testo e selezionare **Save changes** (Salva modifiche).

Bucket options
Bucket access
Platform services

Replication
Disabled
^

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

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

Enable replication

Clear

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

Save changes



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

7. Verificare che la replica sia configurata correttamente:

- a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per la replica come specificato nella configurazione della replica.

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

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

Per gli oggetti di piccole dimensioni, la replica avviene rapidamente.

Informazioni correlate

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

["Utilizzare S3"](#)

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

Configurazione delle notifiche degli eventi

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

Di cosa hai bisogno

- I servizi della piattaforma devono essere abilitati per l'account tenant da un amministratore di StorageGRID.
- È necessario aver già creato un bucket per fungere da origine delle notifiche.
- L'endpoint che si intende utilizzare come destinazione per le notifiche degli eventi deve già esistere ed è necessario disporre dell'URN.
- È necessario appartenere a un gruppo di utenti con l'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root), che consente di gestire le impostazioni di tutti i bucket S3 nell'account tenant. Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

Dopo aver configurato le notifiche degli eventi, ogni volta che si verifica un evento specifico per un oggetto nel bucket di origine, viene generata una notifica e inviata all'argomento Simple Notification Service (SNS) utilizzato come endpoint di destinazione. Per attivare le notifiche per un bucket, è necessario creare e applicare un XML di configurazione delle notifiche valido. L'XML di configurazione delle notifiche deve utilizzare l'URN di un endpoint delle notifiche degli eventi per ciascuna destinazione.

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

Se si abilitano le notifiche degli eventi per un bucket che contiene oggetti, le notifiche vengono inviate solo per le azioni eseguite dopo il salvataggio della configurazione della notifica.

Fasi

1. Abilita le notifiche per il bucket di origine:
 - Utilizzare un editor di testo per creare l'XML di configurazione delle notifiche richiesto per attivare le notifiche degli eventi, come specificato nell'API di notifica S3.
 - Quando si configura l'XML, utilizzare l'URN di un endpoint di notifica degli eventi come argomento di destinazione.

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

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

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Event Notifications**.

5. Selezionare la casella di controllo **Enable event notifications** (attiva notifiche eventi).

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

Bucket options
Bucket access
Platform services

Replication
Disabled
▼

Event notifications
Disabled
▲

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

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

Enable event notifications

Clear

```

<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
      
```

Save changes



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

7. Verificare che le notifiche degli eventi siano configurate correttamente:

- a. Eseguire un'azione su un oggetto nel bucket di origine che soddisfi i requisiti per l'attivazione di una notifica come configurato nel XML di configurazione.

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

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

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

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

Se la notifica viene ricevuta nell'argomento di destinazione, il bucket di origine è stato configurato

correttamente per le notifiche StorageGRID.

Informazioni correlate

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

["Utilizzare S3"](#)

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

Utilizzando il servizio di integrazione della ricerca

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

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



Poiché il servizio di integrazione della ricerca fa sì che i metadati degli oggetti vengano inviati a una destinazione, il relativo XML di configurazione viene definito *metadata notification Configuration XML*. Questo XML di configurazione è diverso dal *XML di configurazione delle notifiche* utilizzato per attivare le notifiche degli eventi.

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

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

Informazioni correlate

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

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

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

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

["Utilizzare S3"](#)

XML di configurazione per l'integrazione della ricerca

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

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, è possibile inviare metadati per oggetti con il prefisso `/images` a una destinazione e metadati per gli oggetti con il prefisso `/videos` a un altro. Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, una configurazione che include una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2` non è consentita.

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

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

La tabella descrive gli elementi contenuti nel file XML di configurazione per la notifica dei metadati.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No

Nome	Descrizione	Obbligatorio
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì
Urna	URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: <ul style="list-style-type: none"> • es deve essere il terzo elemento. • L'URN deve terminare con l'indice e il tipo in cui sono memorizzati i metadati, nel form <code>domain-name/myindex/mytype</code>. <p>Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404.</p> <p>L'urn è incluso nell'elemento Destination.</p>	Sì

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

Configurazione della notifica dei metadati applicabile a tutti gli oggetti

In questo esempio, i metadati degli oggetti per tutti gli oggetti vengono inviati alla stessa destinazione.


```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:mys:es::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Configurazione della notifica dei metadati con due regole

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

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Informazioni correlate

["Utilizzare S3"](#)

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

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

Configurazione del servizio di integrazione della ricerca

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

Di cosa hai bisogno

- I servizi della piattaforma devono essere abilitati per l'account tenant da un amministratore di StorageGRID.
- È necessario aver già creato un bucket S3 di cui si desidera indicizzare il contenuto.
- L'endpoint che si intende utilizzare come destinazione per il servizio di integrazione della ricerca deve già esistere ed è necessario disporre del relativo URN.
- È necessario appartenere a un gruppo di utenti con l'autorizzazione Manage All Bucket (Gestisci tutti i bucket) o Root Access (accesso root), che consente di gestire le impostazioni di tutti i bucket S3 nell'account tenant. Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

Dopo aver configurato il servizio di integrazione della ricerca per un bucket di origine, la creazione di un oggetto o l'aggiornamento dei metadati o dei tag di un oggetto attiva l'invio dei metadati dell'oggetto all'endpoint di destinazione. Se si attiva il servizio di integrazione della ricerca per un bucket che contiene già oggetti, le notifiche dei metadati non vengono inviate automaticamente per gli oggetti esistenti. È necessario aggiornare questi oggetti esistenti per assicurarsi che i relativi metadati vengano aggiunti all'indice di ricerca della destinazione.

Fasi

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

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:11111111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

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

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Search Integration**
5. Selezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).
6. Incollare la configurazione di notifica dei metadati nella casella di testo e selezionare **Salva modifiche**.

The screenshot shows the 'Platform services' configuration page. Under the 'Search integration' section, the status is 'Disabled'. A checkbox labeled 'Enable search integration' is checked. Below this, there is a text area containing the following XML configuration:

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

A 'Clear' button is located to the right of the text area, and a 'Save changes' button is at the bottom right of the configuration panel.



I servizi della piattaforma devono essere attivati per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che il servizio di integrazione della ricerca sia configurato correttamente:
 - a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per l'attivazione di una notifica dei

metadati come specificato nel file XML di configurazione.

Nell'esempio illustrato in precedenza, tutti gli oggetti aggiunti al bucket attivano una notifica dei metadati.

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

Al termine

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

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

Informazioni correlate

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

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

["Utilizzare S3"](#)

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

JSON generato dal servizio di integrazione della ricerca

Quando si attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. Il `test` bucket non è configurato, quindi il `versionId` tag vuoto.

```

{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}

```

Metadati degli oggetti inclusi nelle notifiche dei metadati

La tabella elenca tutti i campi inclusi nel documento JSON che viene inviato all'endpoint di destinazione quando è attivata l'integrazione della ricerca.

Il nome del documento include il nome del bucket, il nome dell'oggetto e l'ID della versione, se presente.

Tipo	Nome e descrizione dell'elemento
Informazioni su bucket e oggetti	bucket: Nome del bucket
key: Nome chiave oggetto	versionID: Versione oggetto, per gli oggetti nei bucket con versione
region: Area bucket, ad esempio us-east-1	Metadati di sistema
size: Dimensione dell'oggetto (in byte) come visibile a un client HTTP	md5: Hash di oggetto
Metadati dell'utente	metadata: Tutti i metadati dell'utente per l'oggetto, come coppie chiave-valore key:value
Tag	tags: Tutti i tag di oggetto definiti per l'oggetto, come coppie chiave-valore key:value



Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

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

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

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

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

Informazioni sul marchio commerciale

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