Utilizzo di Tenant Manager

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

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

Browser Web	Versione minima supportata
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.

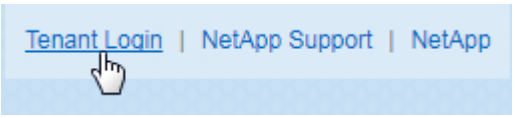
- Se l'URL non include l'ID account a 20 cifre del tenant, è necessario disporre di questo ID account.
- È necessario utilizzare un browser Web supportato.
- I cookie devono essere attivati nel browser Web.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

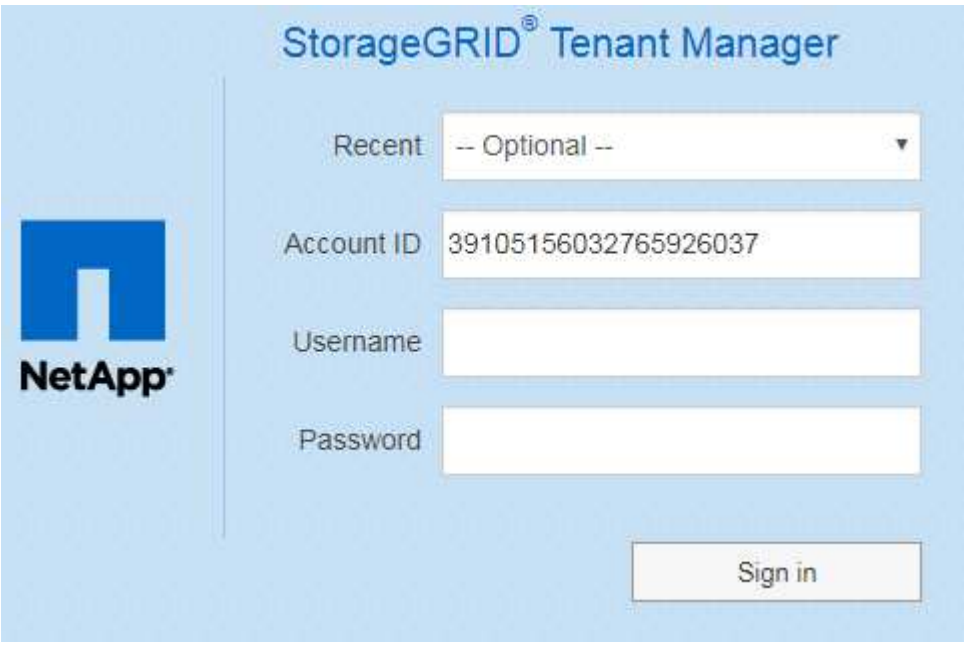
1. Avviare un browser Web supportato.
2. Nella barra degli indirizzi del browser, immettere l'URL per accedere a Tenant Manager.
3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser.
4. Accedi al tenant manager.

   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.

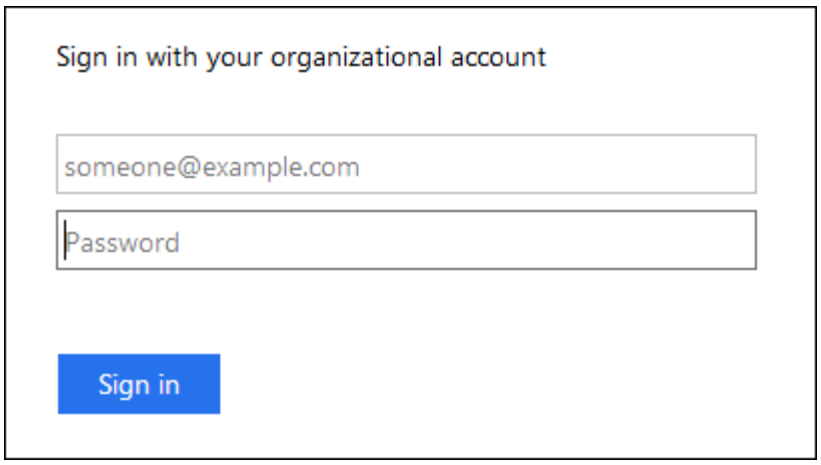
     i. Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.

     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:



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

- La pagina di accesso SSO di Tenant Manager.

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. Fare clic su **Accedi**.

iii. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Viene visualizzata la dashboard di Tenant Manager.

5. 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"

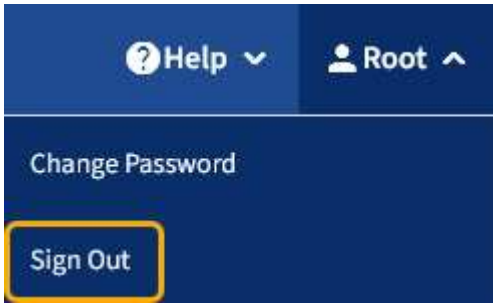
"Requisiti del browser Web"

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**.

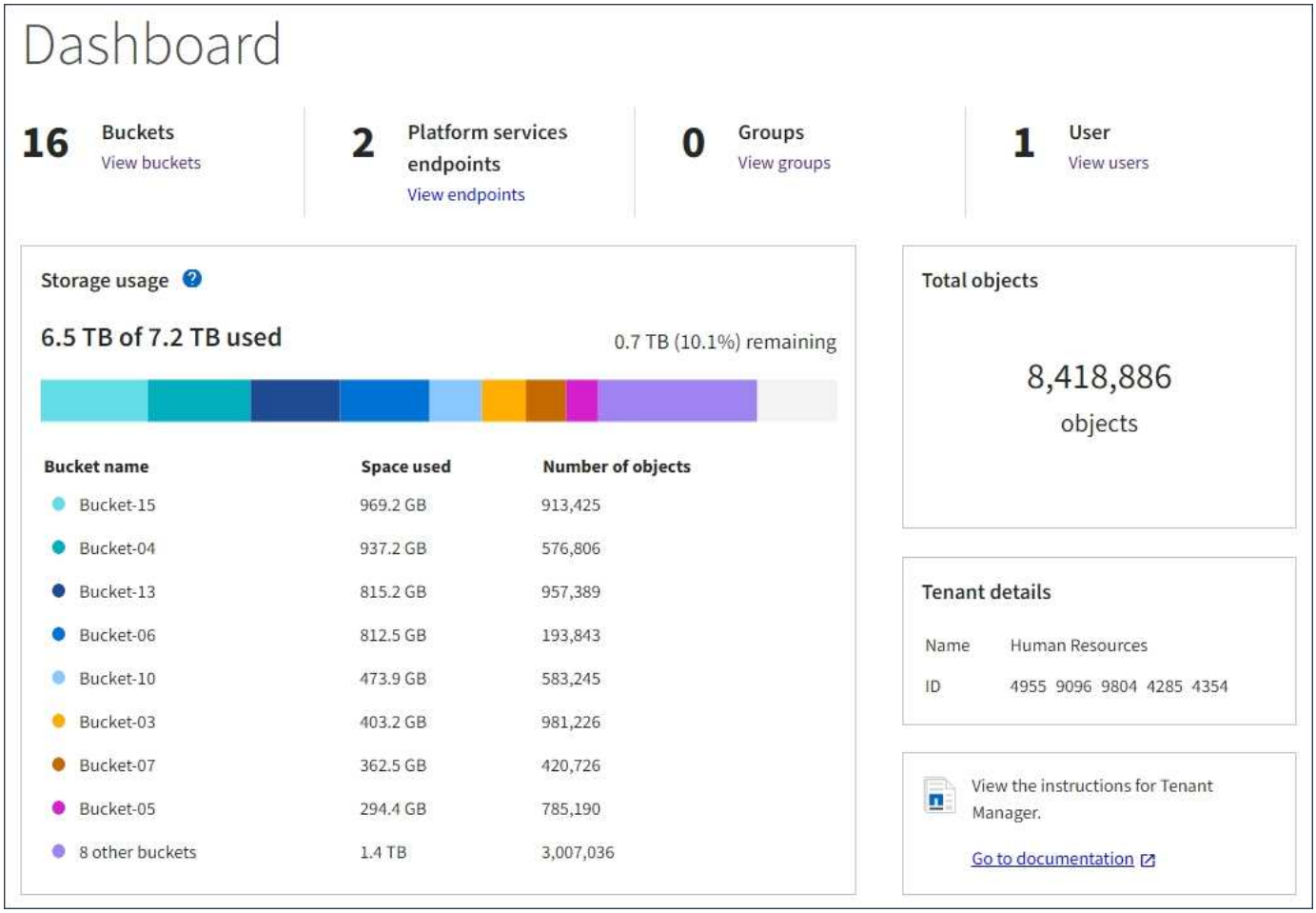
Opzione	Descrizione
SSO non in uso	Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso del tenant manager. **Nota:** se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.
SSO attivato	Si è disconnessi da tutti i nodi di amministrazione 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. **Nota:** se SSO è attivato e si è anche connessi a Grid Manager, è necessario disconnettersi da Grid Manager per disconnettersi da SSO.

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.

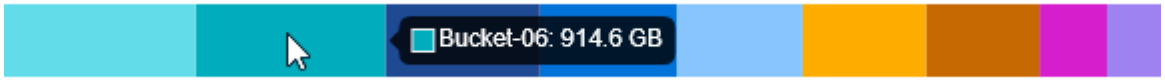
  > Questo valore indica la quantità totale di dati dell'oggetto caricati e non rappresenta lo spazio utilizzato per memorizzare le copie di tali oggetti e dei relativi metadati.

- 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.

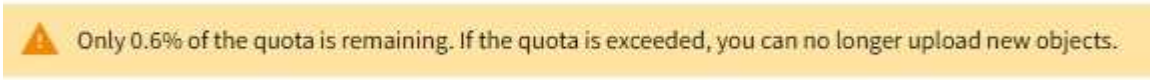
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

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.

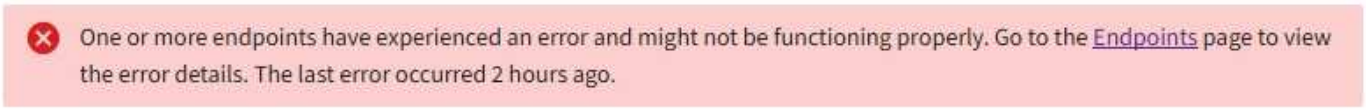


Se si supera la quota, non è possibile caricare nuovi oggetti.

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.



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:

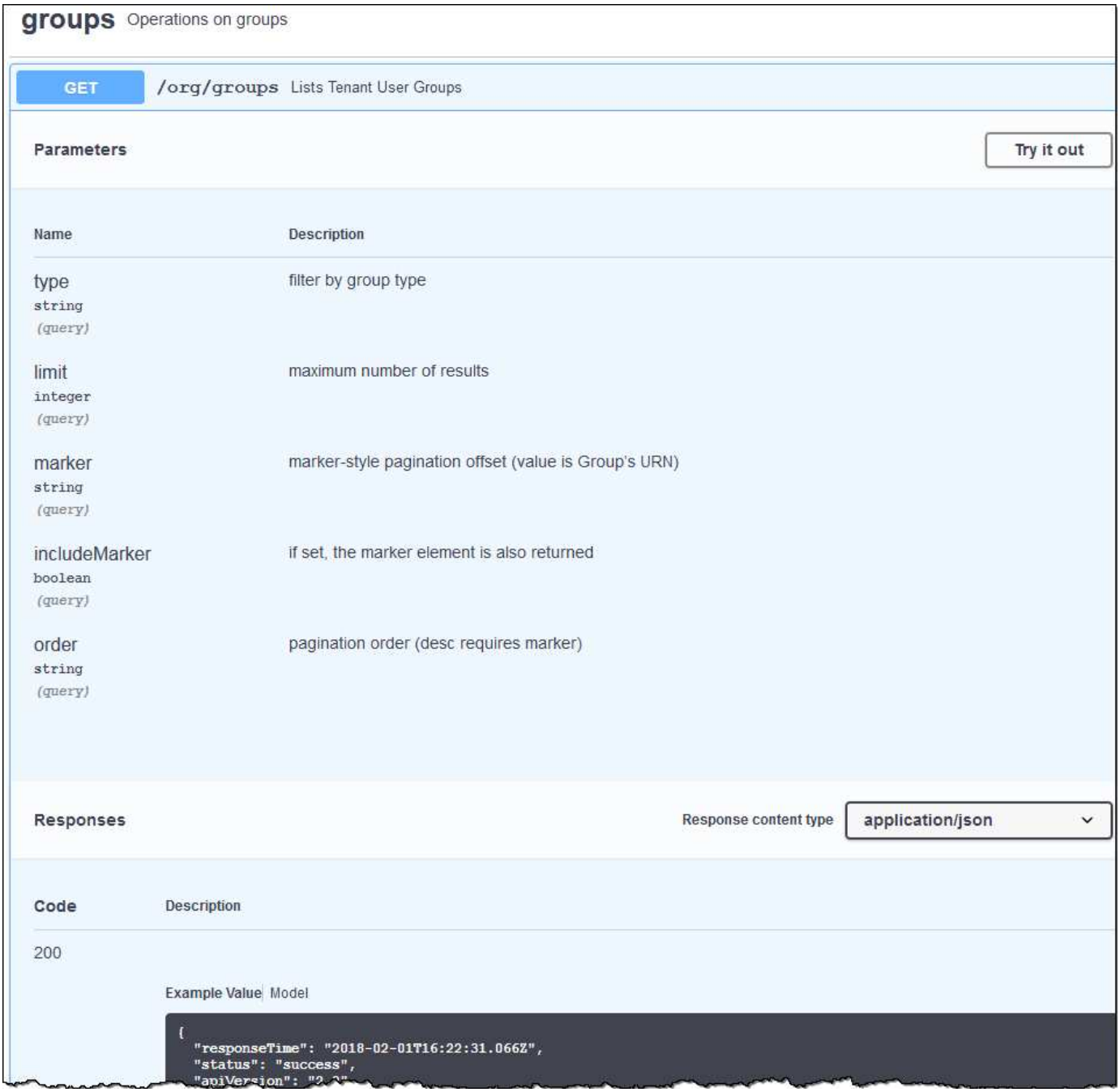
Protocollo	Permesso consentito
S3	• Creazione di bucket conformi e non conformi • Modifica delle impostazioni di compliance legacy • Impostazione del controllo di coerenza per le operazioni eseguite sugli oggetti • Creazione, aggiornamento ed eliminazione della configurazione CORS di un bucket • Attivazione 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

Protocollo	Permesso consentito
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.



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.