Amministrazione di un sistema StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

Amministrazione di un sistema StorageGRID

Seguire queste istruzioni per configurare e amministrare un sistema StorageGRID.

Queste istruzioni descrivono come utilizzare Grid Manager per configurare gruppi e utenti, creare account tenant per consentire alle applicazioni client S3 e Swift di memorizzare e recuperare oggetti, configurare e gestire reti StorageGRID, configurare AutoSupport, gestire le impostazioni dei nodi e molto altro ancora.

> Le istruzioni per la gestione degli oggetti con le regole e le policy ILM (Information Lifecycle Management) sono state spostate in"Gestire gli oggetti con ILM".

Queste istruzioni sono destinate al personale tecnico che configurerà, amministrerà e supporterà un sistema StorageGRID dopo l'installazione.

Di cosa hai bisogno

- Hai una conoscenza generale del sistema StorageGRID.
- Hai una conoscenza abbastanza dettagliata delle shell dei comandi Linux, delle reti e della configurazione e configurazione dell'hardware del server.

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 a Grid Manager

Per accedere alla pagina di accesso di Grid Manager, immettere il nome di dominio completo (FQDN) o l'indirizzo IP di un nodo amministratore nella barra degli indirizzi di un browser Web supportato.

Di cosa hai bisogno

- È necessario disporre delle credenziali di accesso.

- È necessario disporre dell'URL per Grid Manager.
- È necessario utilizzare un browser Web supportato.
- I cookie devono essere attivati nel browser Web.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Ogni sistema StorageGRID include un nodo di amministrazione primario e un numero qualsiasi di nodi di amministrazione non primari. Per gestire il sistema StorageGRID, è possibile accedere a Grid Manager da qualsiasi nodo amministrativo. Tuttavia, i nodi Admin non sono esattamente gli stessi:

- Le conferme di allarme (sistema legacy) eseguite su un nodo di amministrazione non vengono copiate in altri nodi di amministrazione. Per questo motivo, le informazioni visualizzate per gli allarmi potrebbero non apparire identiche su ciascun nodo di amministrazione.
- Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

Se i nodi di amministrazione sono inclusi in un gruppo ad alta disponibilità (ha), la connessione viene eseguita utilizzando l'indirizzo IP virtuale del gruppo ha o un nome di dominio completo che viene mappato all'indirizzo IP virtuale. Il nodo di amministrazione primario deve essere selezionato come master preferito del gruppo, in modo che quando si accede a Grid Manager, si accede al nodo di amministrazione primario, a meno che il nodo di amministrazione primario non sia disponibile.

Fasi

1. Avviare un browser Web supportato.
2. Nella barra degli indirizzi del browser, immettere l'URL per Grid Manager:

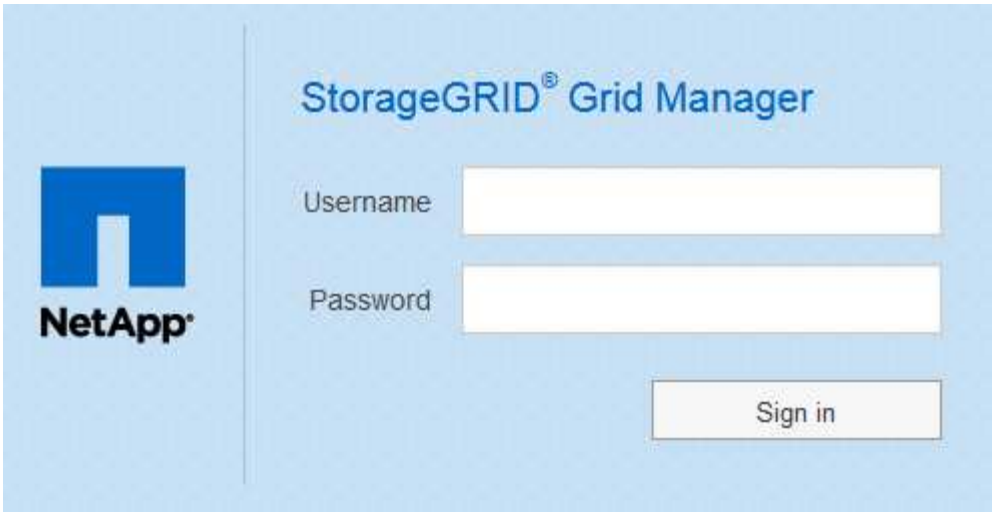
   `https://FQDN_or_Admin_Node_IP/`

   dove *`FQDN_or_Admin_Node_IP`* È un nome di dominio completo o l'indirizzo IP di un nodo di amministrazione o l'indirizzo IP virtuale di un gruppo ha di nodi di amministrazione.

   Se è necessario accedere a Grid Manager su una porta diversa da quella standard per HTTPS (443), immettere la seguente voce, dove *`FQDN_or_Admin_Node_IP`* È un nome di dominio completo o un indirizzo IP e porta è il numero di porta:

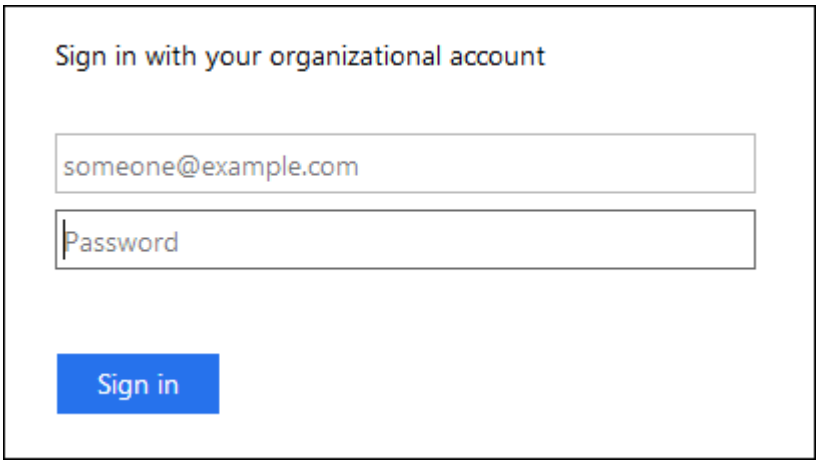
   `https://FQDN_or_Admin_Node_IP:port/`

3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser.
4. Accedi a Grid Manager:
   - Se il sistema StorageGRID non utilizza il Single Sign-on (SSO):
     i. Immettere il nome utente e la password per Grid Manager.
     ii. Fare clic su **Accedi**.



- Se SSO è attivato per il sistema StorageGRID ed è la prima volta che si accede all'URL dal browser:
  i. Fare clic su **Accedi**. È possibile lasciare vuoto il campo ID centro di costo.

  ii. Immettere le credenziali SSO standard nella pagina di accesso SSO dell'organizzazione. Ad esempio:

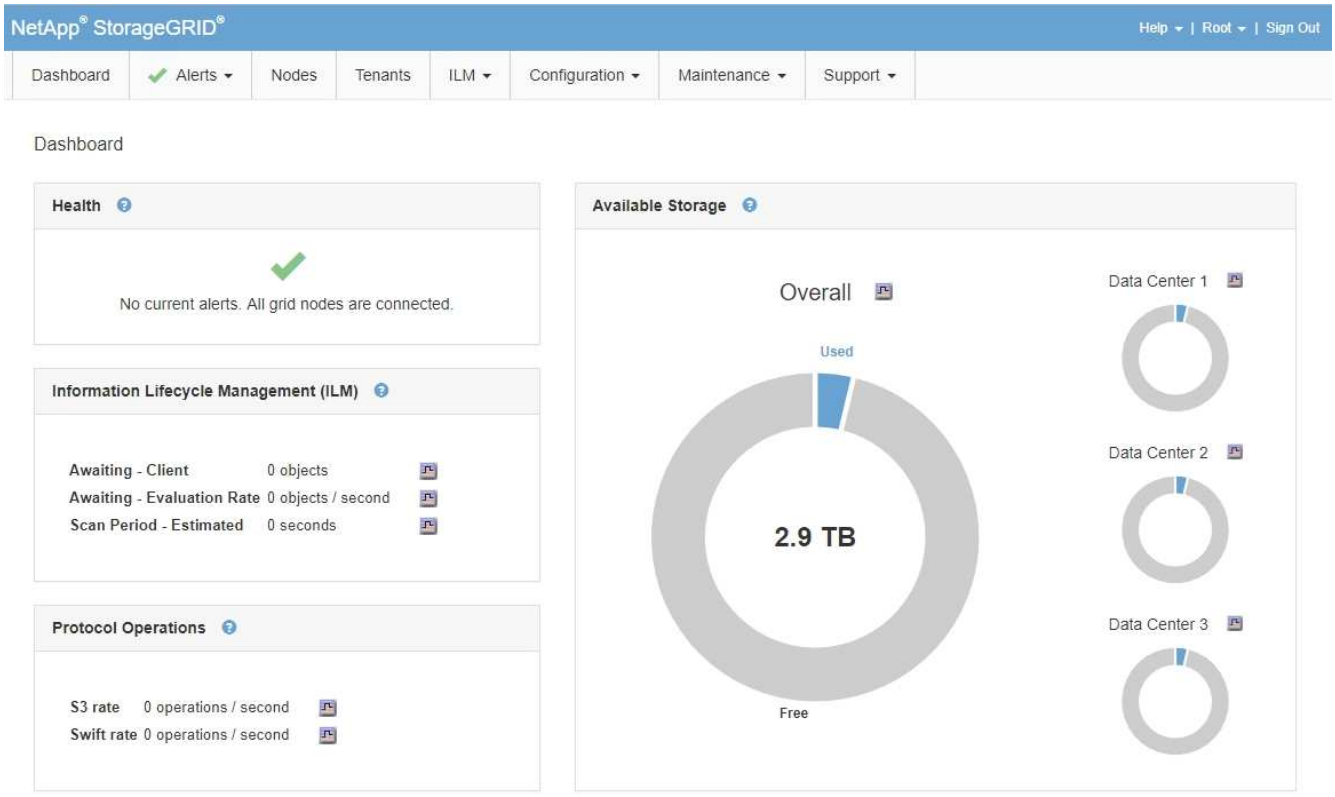


- Se SSO è abilitato per il sistema StorageGRID e si è precedentemente effettuato l'accesso a Grid Manager o a un account tenant:

i. Effettuare una delle seguenti operazioni:

- Immettere **0** (l'ID account per Grid Manager) e fare clic su **Sign in** (Accedi).
- Selezionare **Grid Manager** se compare nell'elenco degli account recenti e fare clic su **Sign in** (Accedi).

ii. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione. Una volta effettuato l'accesso, viene visualizzata la home page di Grid Manager, che include la dashboard. Per informazioni sulle informazioni fornite, consultare "visualizzazione della dashboard" nelle istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.



5. Se si desidera accedere a un altro nodo amministratore:

Opzione	Fasi
SSO non abilitato	a. Nella barra degli indirizzi del browser, inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Includere il numero di porta come richiesto. b. Immettere il nome utente e la password per Grid Manager. c. Fare clic su **Accedi**.
SSO attivato	Nella barra degli indirizzi del browser, inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Se si è effettuato l'accesso a un nodo di amministrazione, è possibile accedere ad altri nodi di amministrazione senza dover effettuare nuovamente l'accesso. Tuttavia, se la sessione SSO scade, vengono richieste nuovamente le credenziali. **Nota:** SSO non è disponibile sulla porta limitata di Grid Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

"Requisiti del browser Web"

"Controllo dell'accesso tramite firewall"

"Configurazione dei certificati del server"

"Configurazione del single sign-on"

"Gestione dei gruppi di amministratori"

"Gestione di gruppi ad alta disponibilità"

"Utilizzare un account tenant"

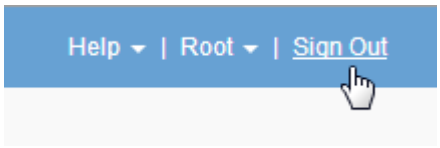
"Monitor risoluzione dei problemi"

Disconnessione da Grid Manager

Una volta terminato l'utilizzo di Grid 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 collegamento **Disconnetti** nell'angolo in alto a destra dell'interfaccia utente.



2. Fare clic su **Disconnetti**.

Opzione	Descrizione
SSO non in uso	Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso di Grid 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. **Grid Manager** è elencato come predefinito nell'elenco a discesa **Recent Accounts** (account recenti) e il campo **account ID** (ID account) mostra 0. **Nota:** se SSO è attivato e si è anche connessi al tenant Manager, è necessario disconnettersi dall'account tenant per disconnettersi da SSO.

Informazioni correlate

"Configurazione del single sign-on"

"Utilizzare un account tenant"

Modifica della password

Gli utenti locali di Grid Manager possono modificare la propria password.

Di cosa hai bisogno

È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

Se si effettua l'accesso a StorageGRID come utente federato o se è attivato il Single Sign-on (SSO), non è possibile modificare la password in Grid Manager. È invece necessario modificare la password nell'origine dell'identità esterna, ad esempio Active Directory o OpenLDAP.

Fasi

1. Dall'intestazione Grid Manager, selezionare **_nome_Modifica password**.

2. Inserire la password corrente.
3. Digitare una nuova password.

   La password deve contenere almeno 8 e non più di 32 caratteri. Le password distinguono tra maiuscole e minuscole.

4. Immettere nuovamente la nuova password.
5. Fare clic su **Save** (Salva).

Modifica della passphrase di provisioning

Utilizzare questa procedura per modificare la passphrase di provisioning StorageGRID. La passphrase è necessaria per le procedure di ripristino, espansione e manutenzione. La passphrase è necessaria anche per scaricare i backup del pacchetto di ripristino che includono le informazioni sulla topologia della griglia e le chiavi di crittografia per il sistema StorageGRID.

Di cosa hai bisogno

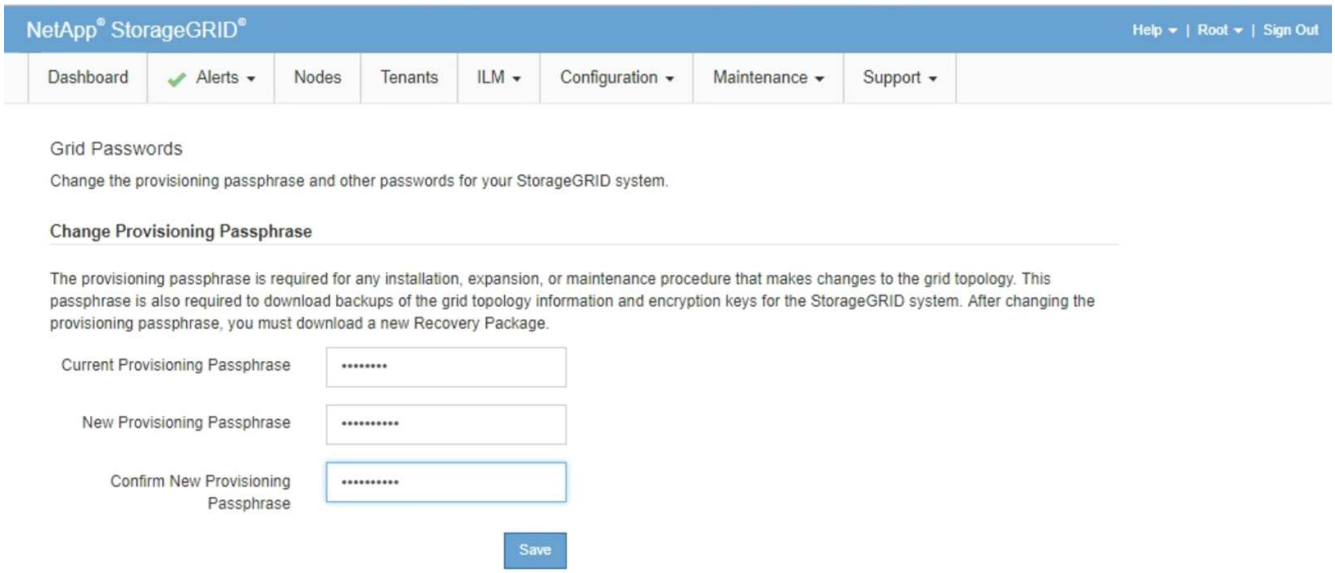
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre delle autorizzazioni di manutenzione o di accesso root.
- È necessario disporre della passphrase di provisioning corrente.

A proposito di questa attività

La passphrase di provisioning è necessaria per molte procedure di installazione e manutenzione e per scaricare il pacchetto di ripristino. La passphrase di provisioning non è elencata in `Passwords.txt` file. Assicurarsi di documentare la passphrase di provisioning e conservarla in una posizione sicura.

Fasi

1. Selezionare **Configurazione controllo accessi Password griglia**.



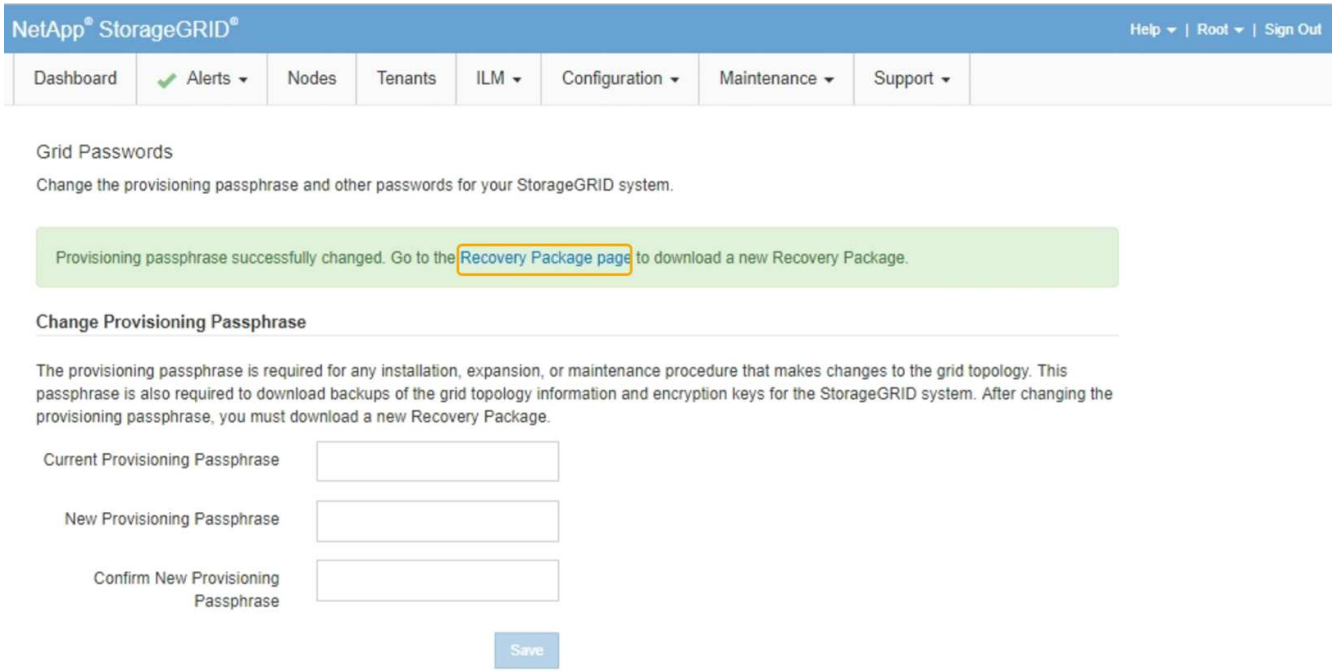
2. Inserire la passphrase di provisioning corrente.

3. Immettere la nuova passphrase.la passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili al maiuscolo/minuscolo.

> Memorizzare la nuova passphrase di provisioning in una posizione sicura. È necessario per le procedure di installazione, espansione e manutenzione.

4. Immettere nuovamente la nuova passphrase e fare clic su **Save** (Salva).

   Al termine della modifica della passphrase di provisioning, il sistema visualizza un banner verde di successo. La modifica dovrebbe richiedere meno di un minuto.



5. Selezionare il collegamento **Recovery Package page** all'interno del banner di successo.
6. Scarica il nuovo pacchetto di ripristino da Grid Manager. Selezionare **manutenzione pacchetto di ripristino** e inserire la nuova passphrase di provisioning.

> Dopo aver modificato la passphrase di provisioning, è necessario scaricare immediatamente un nuovo pacchetto di ripristino. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

Modifica del timeout della sessione del browser

È possibile controllare se gli utenti di Grid Manager e Tenant Manager vengono disconnessi se rimangono inattivi per più di un certo periodo di tempo.

Di cosa hai bisogno

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

A proposito di questa attività

Il valore predefinito del timeout di inattività della GUI è 900 secondi (15 minuti). Se la sessione del browser di

un utente non è attiva per questo periodo di tempo, la sessione viene chiusa.

Se necessario, è possibile aumentare o diminuire il periodo di timeout impostando l'opzione di visualizzazione Timeout inattività GUI.

Se è attivato il Single Sign-on (SSO) e la sessione del browser di un utente va in timeout, il sistema si comporta come se l'utente abbia fatto clic su **Disconnetti** manualmente. L'utente deve immettere nuovamente le proprie credenziali SSO per accedere nuovamente a StorageGRID.

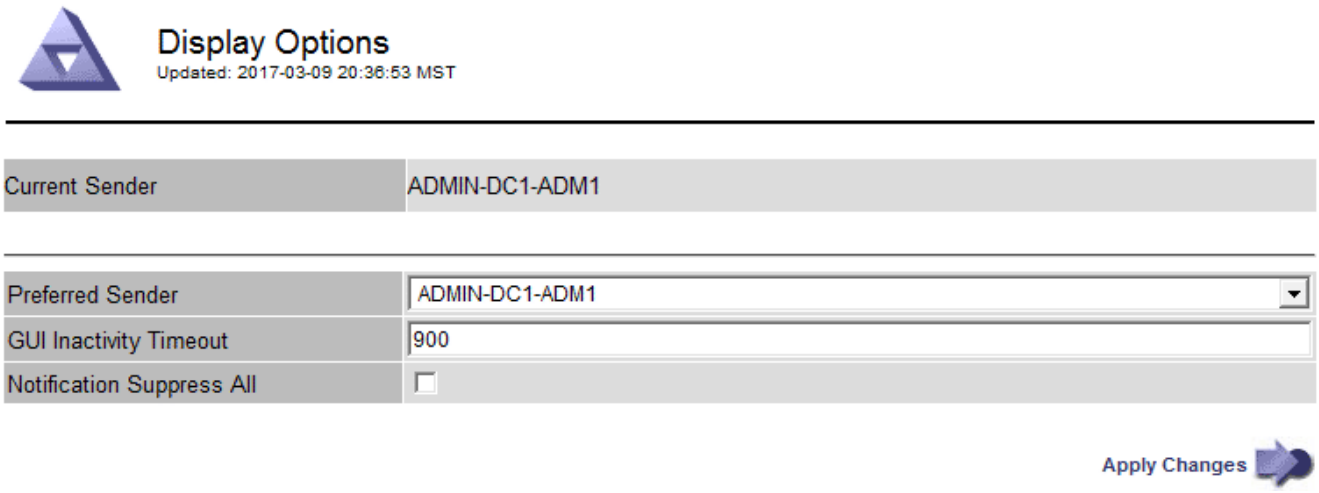
Il timeout della sessione utente può essere controllato anche da:

- Un timer StorageGRID separato, non configurabile, incluso per la sicurezza del sistema. Per impostazione predefinita, ogni token di autenticazione dell'utente scade 16 ore dopo l'accesso. Al termine dell'autenticazione, l'utente viene automaticamente disconnesso, anche se non viene raggiunto il valore per il timeout di inattività della GUI. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che SSO sia abilitato per StorageGRID.

Fasi

1. Selezionare **Configurazione** > **Impostazioni di sistema** > **Opzioni di visualizzazione**.
2. Per **GUI Inactivity Timeout** (Timeout inattività GUI), immettere un periodo di timeout di almeno 60 secondi.

   Impostare questo campo su 0 se non si desidera utilizzare questa funzionalità. Gli utenti vengono disconnessi 16 ore dopo l'accesso, quando scadono i token di autenticazione.



3. Fare clic su **Applica modifiche**.

   La nuova impostazione non influisce sugli utenti attualmente registrati. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser per rendere effettiva la nuova impostazione di timeout.

Informazioni correlate

"Come funziona il single sign-on"

"Utilizzare un account tenant"

Visualizzazione delle informazioni sulla licenza StorageGRID

Se necessario, è possibile visualizzare le informazioni sulla licenza del sistema StorageGRID, ad esempio la capacità di storage massima del grid.

Di cosa hai bisogno

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

A proposito di questa attività

In caso di problemi con la licenza software per questo sistema StorageGRID, il pannello Stato del dashboard include un'icona Stato licenza e un collegamento **licenza**. Il numero indica il numero di problemi relativi alla licenza.

Fase

Per visualizzare la licenza, effettuare una delle seguenti operazioni:

- Dal pannello Health (Stato) della dashboard, fare clic sull'icona License status (Stato licenza) o sul collegamento **License** (licenza). Questo collegamento viene visualizzato solo in caso di problemi con la licenza.
- Selezionare **manutenzione sistema licenza**.

Viene visualizzata la pagina License (licenza) che fornisce le seguenti informazioni di sola lettura sulla licenza corrente:

- ID sistema StorageGRID, che è il numero di identificazione univoco per l'installazione di StorageGRID
- Numero di serie della licenza
- Capacità di storage concessa in licenza del grid
- Data di fine della licenza software
- Data di fine del contratto di assistenza
- Contenuto del file di testo della licenza

Per le licenze rilasciate prima di StorageGRID 10.3, la capacità dello storage concesso in licenza non è inclusa nel file di licenza e viene visualizzato il messaggio "vedere il contratto di licenza" invece di un valore.

Aggiornamento delle informazioni sulla licenza StorageGRID

È necessario aggiornare le informazioni di licenza per il sistema StorageGRID in qualsiasi momento in cui i termini della licenza cambiano. Ad esempio, è necessario aggiornare le informazioni sulla licenza se si acquista ulteriore capacità di storage per il grid.

Di cosa hai bisogno

- È necessario disporre di un nuovo file di licenza per l'applicazione al sistema StorageGRID.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre della passphrase di provisioning.

Fasi

1. Selezionare **manutenzione sistema licenza**.
2. Inserire la passphrase di provisioning per il sistema StorageGRID nella casella di testo **Passphrase di provisioning**.
3. Fare clic su **Sfoglia**.
4. Nella finestra di dialogo Apri, individuare e selezionare il nuovo file di licenza (`.txt`), quindi fare clic su **Apri**.

   Il nuovo file di licenza viene validato e visualizzato.

5. Fare clic su **Save** (Salva).

Utilizzando l'API Grid Management

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

L'API Grid Management utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di eseguire operazioni in tempo reale in StorageGRID con l'API.

Risorse di alto livello

L'API Grid Management fornisce le seguenti risorse di primo livello:

- `/grid`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate.
- `/org`: L'accesso è limitato agli utenti che appartengono a un gruppo LDAP locale o federato per un account tenant. Per ulteriori informazioni, consulta le informazioni sull'utilizzo degli account tenant.

- `/private`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate. Queste API sono destinate esclusivamente all'uso interno e non sono documentate pubblicamente. Queste API sono inoltre soggette a modifiche senza preavviso.

Informazioni correlate

"Utilizzare un account tenant"

"Prometheus: Nozioni di base sulle query"

Operazioni API di Grid Management

L'API Grid Management organizza le operazioni API disponibili nelle seguenti sezioni.

- **Account** — operazioni per gestire gli account del tenant di storage, inclusa la creazione di nuovi account e il recupero dell'utilizzo dello storage per un determinato account.
- **Alarms** — operazioni per elencare gli allarmi correnti (sistema legacy) e restituire informazioni sullo stato della griglia, inclusi gli avvisi correnti e un riepilogo degli stati di connessione del nodo.
- **Alert-history** — operazioni sugli avvisi risolti.
- **Ricevitori di avvisi** — operazioni sui destinatari di notifiche di avvisi (e-mail).
- **Alert-rules** — operazioni sulle regole di allerta.
- **Silenzi di allerta** — operazioni su silenzi di allerta.
- **Alerts** — operazioni sugli avvisi.
- **Audit** — operazioni per elencare e aggiornare la configurazione dell'audit.
- **Auth** — operazioni per eseguire l'autenticazione della sessione utente.

  L'API Grid Management supporta lo schema di autenticazione del token del bearer. Per effettuare l'accesso, inserisci un nome utente e una password 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 ("Authorization: Bearer *token*").

  > Se per il sistema StorageGRID è attivato il single sign-on, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "autenticare l'API se è attivato il Single Sign-on".

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

- **Certificati-client** — operazioni per configurare i certificati client in modo che sia possibile accedere in modo sicuro a StorageGRID utilizzando strumenti di monitoraggio esterni.
- **Config** — operazioni relative alla release del prodotto e alle versioni dell'API Grid Management. È possibile elencare la versione del prodotto e le principali versioni dell'API Grid Management supportate da tale release ed è possibile disattivare le versioni obsolete dell'API.
- **Disattivato-funzioni** — operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **dns-servers** — operazioni per elencare e modificare i server DNS esterni configurati.
- **Nomi-dominio-endpoint** — operazioni per elencare e modificare i nomi di dominio degli endpoint.
- **Erasure-coding** — operazioni sui profili di codifica Erasure.
- **Espansione** — operazioni di espansione (a livello di procedura).

- **Expansion-node** — operazioni di espansione (a livello di nodo).
- **Expansion-sites** — operazioni di espansione (a livello di sito).
- **Grid-networks** — operazioni per elencare e modificare l'elenco Grid Network.
- **Grid-password** — operazioni per la gestione delle password grid.
- **Gruppi** — operazioni per gestire i gruppi di amministratori di griglia locali e recuperare i gruppi di amministratori di griglia federati da un server LDAP esterno.
- **Identity-source** — operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm** — operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **Licenza** — operazioni per recuperare e aggiornare la licenza StorageGRID.
- **Logs** — operazioni per la raccolta e il download dei file di log.
- **Metriche** — operazioni su metriche StorageGRID, incluse query metriche istantanee in un singolo punto nel tempo e query metriche di intervallo in un intervallo di tempo. L'API Grid Management utilizza lo strumento di monitoraggio dei sistemi Prometheus come origine dei dati back-end. Per informazioni sulla creazione di query Prometheus, visitare il sito Web Prometheus.

> Metriche che includono `private` i loro nomi sono destinati esclusivamente all'uso interno. Queste metriche sono soggette a modifiche senza preavviso tra le versioni di StorageGRID.

- **Node-Health** — operazioni sullo stato di salute del nodo.
- **ntp-servers** — operazioni per elencare o aggiornare server NTP (Network Time Protocol) esterni.
- **Objects** — operazioni su oggetti e metadati di oggetti.
- **Recovery** — operazioni per la procedura di recovery.
- **Recovery-package** — operazioni per scaricare il pacchetto di ripristino.
- **Regioni** — operazioni per visualizzare e creare regioni.
- **s3-Object-lock** — operazioni sulle impostazioni generali di blocco oggetti S3.
- **Certificato-server** — operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp** — operazioni sulla configurazione SNMP corrente.
- **Classi di traffico** — operazioni per le policy di classificazione del traffico.
- **Untrusted-client-network** — operazioni sulla configurazione Untrusted Client Network.
- **Utenti** — operazioni per visualizzare e gestire gli utenti di Grid Manager.

Invio di richieste API

L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.

Di cosa hai bisogno

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

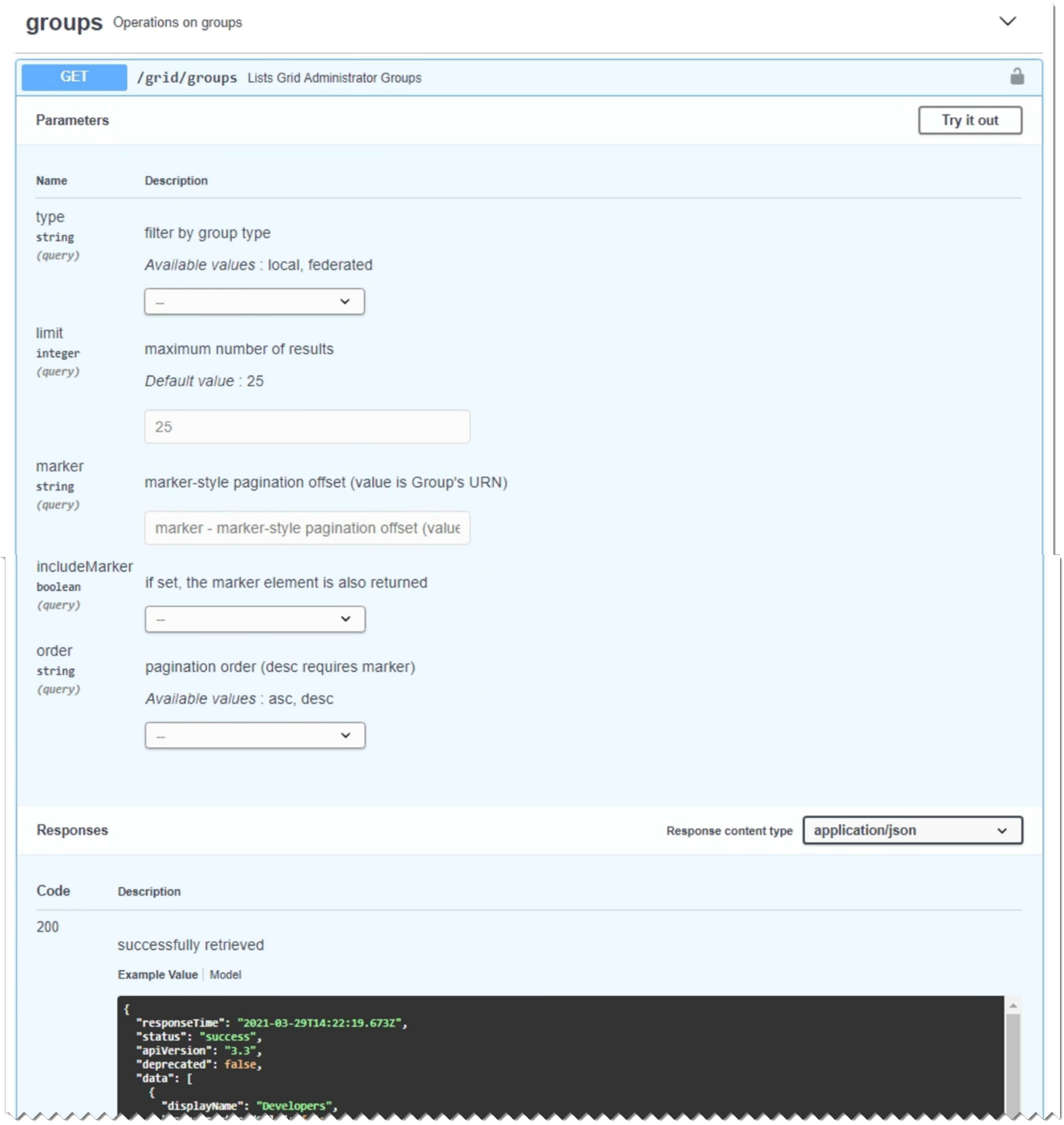
> Tutte le operazioni API eseguite utilizzando la pagina web API Docs sono operazioni live. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Fasi

1. Selezionare **Help API Documentation** dall'intestazione Grid Manager.
2. Selezionare l'operazione desiderata.

   Quando si espande un'operazione API, è possibile visualizzare le azioni HTTP disponibili, ad esempio GET, PUT, UPDATE ed DELETE.

3. Selezionare un'azione HTTP per visualizzare i dettagli della richiesta, tra cui l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.



4. 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.

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

Versione dell'API Grid Management

L'API Grid Management 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 si installa il software StorageGRID per la prima volta, viene attivata solo la versione più recente dell'API di gestione griglia. Tuttavia, quando si esegue l'aggiornamento a una nuova release di funzionalità di StorageGRID, si continua ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.

> È possibile utilizzare l'API Grid Management per configurare le versioni supportate. Per ulteriori informazioni, consultare la sezione "config" della documentazione dell'API Swagger. Disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API Grid Management per utilizzare la versione più recente.

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
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

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.

Utilizzo dell'API se è attivato il single sign-on

Se per il sistema StorageGRID è stato attivato il Single Sign-on (SSO), non è possibile utilizzare le richieste API autenticate standard per accedere e disconnettersi dall'API di gestione griglia o dall'API di gestione tenant.

Accesso all'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per ottenere un token di autenticazione da ad FS valido per l'API Grid Management o l'API Tenant Management.

Di cosa hai bisogno

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- Il `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione di StorageGRID (`./rpms` Per Red Hat Enterprise Linux o CentOS, `./debs` Per Ubuntu o Debian, e. `./vsphere` Per VMware).

- Un esempio di workflow di richieste di curl.

  Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: Impossibile trovare una SubjectConfirmation valida in questa risposta.

  L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: Versione SAML non supportata.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
   - Utilizzare `storagegrid-ssoauth.py` Script Python. Passare alla fase 2.
   - USA richieste di curl. Passare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` Passare lo script all'interprete Python ed eseguirlo.

   Quando richiesto, inserire i valori per i seguenti argomenti:

   - Il nome utente SSO
   - Il dominio in cui è installato StorageGRID
   - L'indirizzo per StorageGRID
   - Se si desidera accedere all'API di gestione tenant, inserire l'ID account tenant.

   +
   ```
   python3 /tmp/storagegrid-ssoauth.py
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.

   a. Dichiarare le variabili necessarie per l'accesso.

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export SAMLDOMAIN='my-domain'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   export AD_FS_ADDRESS='adfs.example.com'
   ```

Per accedere all'API Grid Management, utilizzare 0 AS `TENANTACCOUNTID`.

b. Per ricevere un URL di autenticazione firmato, inviare una richiesta DI POST a. `/api/v3/authorize-saml`E rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per `TENANTACCOUNTID`. I risultati verranno passati a python -m json.tool per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salvare `SAMLRequest` dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Ottenere un URL completo che includa l'ID della richiesta del client da ad FS.

Un'opzione consiste nel richiedere il modulo di accesso utilizzando l'URL della risposta precedente.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

La risposta include l'ID della richiesta del client:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salvare l'ID della richiesta del client dalla risposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Inviare le credenziali all'azione del modulo della risposta precedente.

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMLPASSWORD&AuthMethod=For
msAuthentication" --include
```

AD FS restituisce un reindirizzamento 302, con informazioni aggiuntive nelle intestazioni.

> Se l'autenticazione a più fattori (MFA) è attivata per il sistema SSO, il post del modulo conterrà anche la seconda password o altre credenziali.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salvare `MSISAuth` cookie dalla risposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Inviare una richiesta GET alla posizione specificata con i cookie del POST di autenticazione.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --cookie "MSISAuth=$MSISAuth" --include
```

Le intestazioni delle risposte conterranno le informazioni della sessione di ad FS per un utilizzo successivo della disconnessione e il corpo della risposta conterrà la risposta SAMLin un campo di forma nascosto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Salvare `SAMLResponse` dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato `SAMLResponse`, Creare un StorageGRID`/api/saml-response` Richiesta di generazione di un token di autenticazione StorageGRID.

Per `RelayState`, Utilizzare l'ID account tenant o utilizzare 0 se si desidera accedere all'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La risposta include il token di autenticazione.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salvare il token di autenticazione nella risposta con nome `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi utilizzare `MYTOKEN` Per le altre richieste, in modo simile a come si utilizza l'API se SSO non viene utilizzato.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management.

A proposito di questa attività

Se necessario, puoi disconnetterti dall'API StorageGRID semplicemente disconnettendoti dalla singola pagina di disconnessione della tua organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da StorageGRID, che richiede un token bearer StorageGRID valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true"` All'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Salvare l'URL di disconnessione.

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEI
RfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true"` Non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

R `204 No Content` la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

Utilizzo dei certificati di sicurezza StorageGRID

I certificati di sicurezza sono piccoli file di dati utilizzati per creare connessioni sicure e affidabili tra i componenti di StorageGRID e tra i componenti di StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

- **I certificati server** sono richiesti quando si utilizzano connessioni HTTPS. I certificati del server vengono utilizzati per stabilire connessioni sicure tra client e server, autenticando l'identità di un server nei suoi client e fornendo un percorso di comunicazione sicuro per i dati. Il server e il client dispongono di una copia del certificato.
- **Certificati client** autenticano un'identità del client o dell'utente sul server, fornendo un'autenticazione più sicura rispetto alle sole password. I certificati client non crittografano i dati.

Quando un client si connette al server utilizzando HTTPS, il server risponde con il certificato del server, che contiene una chiave pubblica. Il client verifica questo certificato confrontando la firma del server con la firma sulla copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server utilizzando la stessa chiave pubblica.

StorageGRID funziona come server per alcune connessioni (come l'endpoint del bilanciamento del carico) o come client per altre connessioni (come il servizio di replica di CloudMirror).

Un'autorità di certificazione esterna (CA) può emettere certificati personalizzati pienamente conformi ai criteri di sicurezza delle informazioni dell'organizzazione. StorageGRID include anche un'autorità di certificazione (CA) incorporata che genera certificati CA interni durante l'installazione del sistema. Questi certificati CA interni vengono utilizzati, per impostazione predefinita, per proteggere il traffico StorageGRID interno. Sebbene sia possibile utilizzare i certificati CA interni per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Sono supportate anche le connessioni non protette senza certificato, ma non sono consigliate.

- I certificati CA personalizzati non rimuovono i certificati interni; tuttavia, i certificati personalizzati devono essere quelli specificati per la verifica delle connessioni al server.
- Tutti i certificati personalizzati devono soddisfare le linee guida per la protezione avanzata del sistema per i certificati server.

  "Protezione avanzata del sistema"

- StorageGRID supporta il raggruppamento di certificati da una CA in un singolo file (noto come bundle di certificati CA).

> StorageGRID include anche certificati CA del sistema operativo che sono gli stessi su tutte le griglie. Negli ambienti di produzione, assicurarsi di specificare un certificato personalizzato firmato da un'autorità di certificazione esterna al posto del certificato CA del sistema operativo.

Le varianti dei tipi di certificato server e client vengono implementate in diversi modi. Prima di configurare il sistema, è necessario disporre di tutti i certificati necessari per la configurazione specifica di StorageGRID.

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Certificato del client di amministratore	Client	Installato su ciascun client, consentendo a StorageGRID di autenticare l'accesso client esterno. • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID utilizzando strumenti esterni.	**Configurazione controllo accessi certificati client**	"Configurazione dei certificati client dell'amministratore"
Certificato di federazione delle identità	Server	Autentica la connessione tra StorageGRID e un server di directory esterno, OpenLDAP o Oracle. Utilizzato per la federazione delle identità, che consente la gestione di gruppi di amministratori e utenti da parte di un sistema esterno.	**Configurazione controllo accessi Federazione identità**	"Utilizzo della federazione delle identità"
Certificato SSO (Single Sign-on)	Server	Autentica la connessione tra servizi di federazione Active Directory (ad FS) e StorageGRID utilizzata per le richieste SSO (Single Sign-on).	**Configurazione controllo accessi Single Sign-on**	"Configurazione del single sign-on"

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Certificato del Key Management Server (KMS)	Server e client	Autentica la connessione tra StorageGRID e un KMS (Key Management Server) esterno, che fornisce chiavi di crittografia ai nodi appliance StorageGRID.	**Configurazione Impostazioni di sistema Server di gestione delle chiavi**	"Aggiunta di un server di gestione delle chiavi (KMS)"
Certificato di notifica degli avvisi via email	Server e client	Autentica la connessione tra un server e-mail SMTP e StorageGRID utilizzato per le notifiche degli avvisi. • Se le comunicazioni con il server SMTP richiedono TLS (Transport Layer Security), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta SMTP richiede certificati client per l'autenticazione.	**Avvisi Configurazione e-mail**	"Monitor risoluzione dei problemi"

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Certificato endpoint per il bilanciamento del carico	Server	Autentica la connessione tra i client S3 o Swift e il servizio bilanciamento del carico StorageGRID sui nodi gateway o sui nodi di amministrazione. Quando si configura un endpoint di bilanciamento del carico, si carica o genera un certificato di bilanciamento del carico.le applicazioni client utilizzano il certificato di bilanciamento del carico quando si effettua la connessione a StorageGRID per salvare e recuperare i dati degli oggetti. **Nota:** il certificato di bilanciamento del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID.	**Configurazione Impostazioni di rete endpoint del bilanciamento del carico**	• "Configurazione degli endpoint del bilanciamento del carico" • Creazione di un endpoint di bilanciamento del carico per FabricPool "Configurare StorageGRID per FabricPool"

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Certificato del server dell'interfaccia di gestione	Server	Autentica la connessione tra i browser Web client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza. Questo certificato autentica anche le connessioni API Grid Management e API Tenant Management. È possibile utilizzare il certificato CA interno o caricare un certificato personalizzato.	**Configurazione Impostazioni di rete certificati server**	• "Configurazione dei certificati del server" • "Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"
Certificato endpoint Cloud Storage Pool	Server	Autentica la connessione dal pool di storage cloud di StorageGRID a una posizione di storage esterna (ad esempio, lo storage S3 Glacier o Microsoft Azure Blob). Per ogni tipo di cloud provider è necessario un certificato diverso.	**ILM Storage Pools**	"Gestire gli oggetti con ILM"
Certificato endpoint dei servizi di piattaforma	Server	Autentica la connessione dal servizio della piattaforma StorageGRID a una risorsa di storage S3.	**Tenant Manager STORAGE (S3) endpoint dei servizi della piattaforma**	"Utilizzare un account tenant"

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Object Storage API Service Endpoint Server Certificate	Server	Autentica le connessioni client protette S3 o Swift al servizio LDR (Local Distribution Router) su un nodo di storage o al servizio CLB (Connection Load Balancer) obsoleto su un nodo gateway.	**Configurazione Impostazioni di rete endpoint del bilanciamento del carico**	"Configurazione di un certificato server personalizzato per le connessioni al nodo di storage o al servizio CLB"

Esempio 1: Servizio di bilanciamento del carico

In questo esempio, StorageGRID agisce come server.

1. È possibile configurare un endpoint di bilanciamento del carico e caricare o generare un certificato server in StorageGRID.
2. È possibile configurare una connessione client S3 o Swift all'endpoint del bilanciamento del carico e caricare lo stesso certificato nel client.
3. Quando il client desidera salvare o recuperare i dati, si connette all'endpoint del bilanciamento del carico utilizzando HTTPS.
4. StorageGRID risponde con il certificato del server, che contiene una chiave pubblica, e con una firma basata sulla chiave privata.
5. Il client verifica questo certificato confrontando la firma del server con la firma sulla copia del certificato. Se le firme corrispondono, il client avvia una sessione utilizzando la stessa chiave pubblica.
6. Il client invia i dati dell'oggetto a StorageGRID.

Esempio 2: Server KMS (Key Management Server) esterno

In questo esempio, StorageGRID agisce come client.

1. Utilizzando il software del server di gestione delle chiavi esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server con firma CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, è possibile configurare un server KMS e caricare i certificati server e client e la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, effettua una richiesta al server KMS che include i dati del certificato e una firma basata sulla chiave privata.
4. Il server KMS convalida la firma del certificato e decide che può fidarsi di StorageGRID.
5. Il server KMS risponde utilizzando la connessione validata.

Informazioni sul copyright

Informazioni sul marchio commerciale