Inizia con Grid Manager

StorageGRID software

NetApp
December 03, 2025

Sommario

Inizia con Grid Manager

Requisiti del browser web

È necessario utilizzare un browser web supportato.

browser web	Versione minima supportata
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Dovresti impostare la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024
Ottimale	1280

Sign in a Grid Manager

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

Ogni sistema StorageGRID include un nodo amministrativo primario e un numero qualsiasi di nodi amministrativi non primari. È possibile accedere a Grid Manager su qualsiasi nodo di amministrazione per gestire il sistema StorageGRID . Tuttavia, alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

Connettiti al gruppo HA

Se i nodi amministrativi sono inclusi in un gruppo ad alta disponibilità (HA), la connessione avviene tramite l'indirizzo IP virtuale del gruppo HA o un nome di dominio completo mappato all'indirizzo IP virtuale. Il nodo di amministrazione primario dovrebbe essere selezionato come interfaccia primaria del gruppo, in modo che quando si accede a Grid Manager, si acceda al nodo di amministrazione primario, a meno che il nodo di amministrazione primario non sia disponibile. Vedere "Gestire gruppi ad alta disponibilità" .

Utilizzare SSO

I passaggi di accesso sono leggermente diversi se"è stato configurato l'accesso singolo (SSO)" .

Sign in a Grid Manager sul primo nodo di amministrazione

Prima di iniziare

- Hai le tue credenziali di accesso.
- Stai utilizzando un"browser web supportato" .
- I cookie sono abilitati nel tuo browser web.
- Appartieni a un gruppo di utenti che ha almeno un'autorizzazione.
- Hai l'URL per Grid Manager:

  `https://FQDN_or_Admin_Node_IP/`

  È possibile utilizzare il nome di dominio completo, l'indirizzo IP di un nodo di amministrazione o l'indirizzo IP virtuale di un gruppo HA di nodi di amministrazione.

  Per accedere a Grid Manager su una porta diversa da quella predefinita per HTTPS (443), includere il numero di porta nell'URL:

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO non è disponibile sulla porta riservata di Grid Manager. È necessario utilizzare la porta 443.

Passi

1. Avviare un browser web supportato.
2. Nella barra degli indirizzi del browser, inserisci l'URL di Grid Manager.
3. Se viene visualizzato un avviso di sicurezza, installare il certificato utilizzando la procedura guidata di installazione del browser. Vedere "Gestire i certificati di sicurezza" .
4. Sign in a Grid Manager.

   La schermata di accesso visualizzata dipende dalla configurazione dell'accesso singolo (SSO) per StorageGRID.

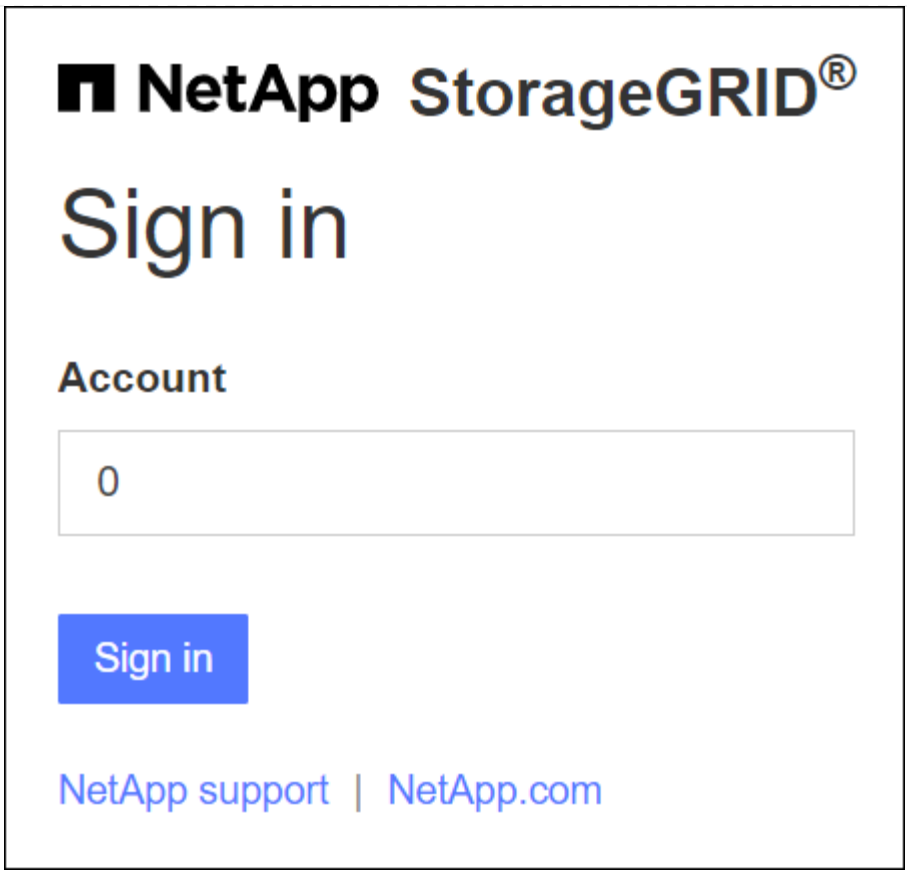
Non si utilizza SSO

a. Inserisci il tuo nome utente e la password per Grid Manager.

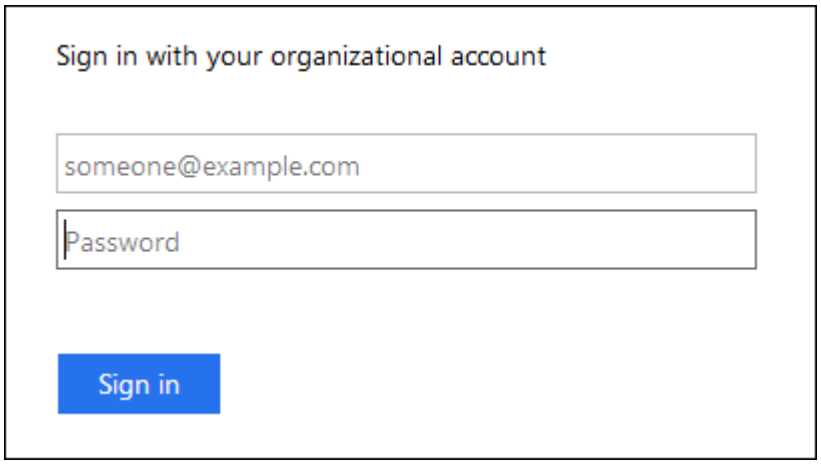
b. Seleziona **Accedi**.

Utilizzo di SSO

- Se StorageGRID utilizza SSO e questa è la prima volta che accedi all'URL su questo browser:
  i. Seleziona * Sign in*. Puoi lasciare lo 0 nel campo Account.



ii. Inserisci le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione. Per esempio:



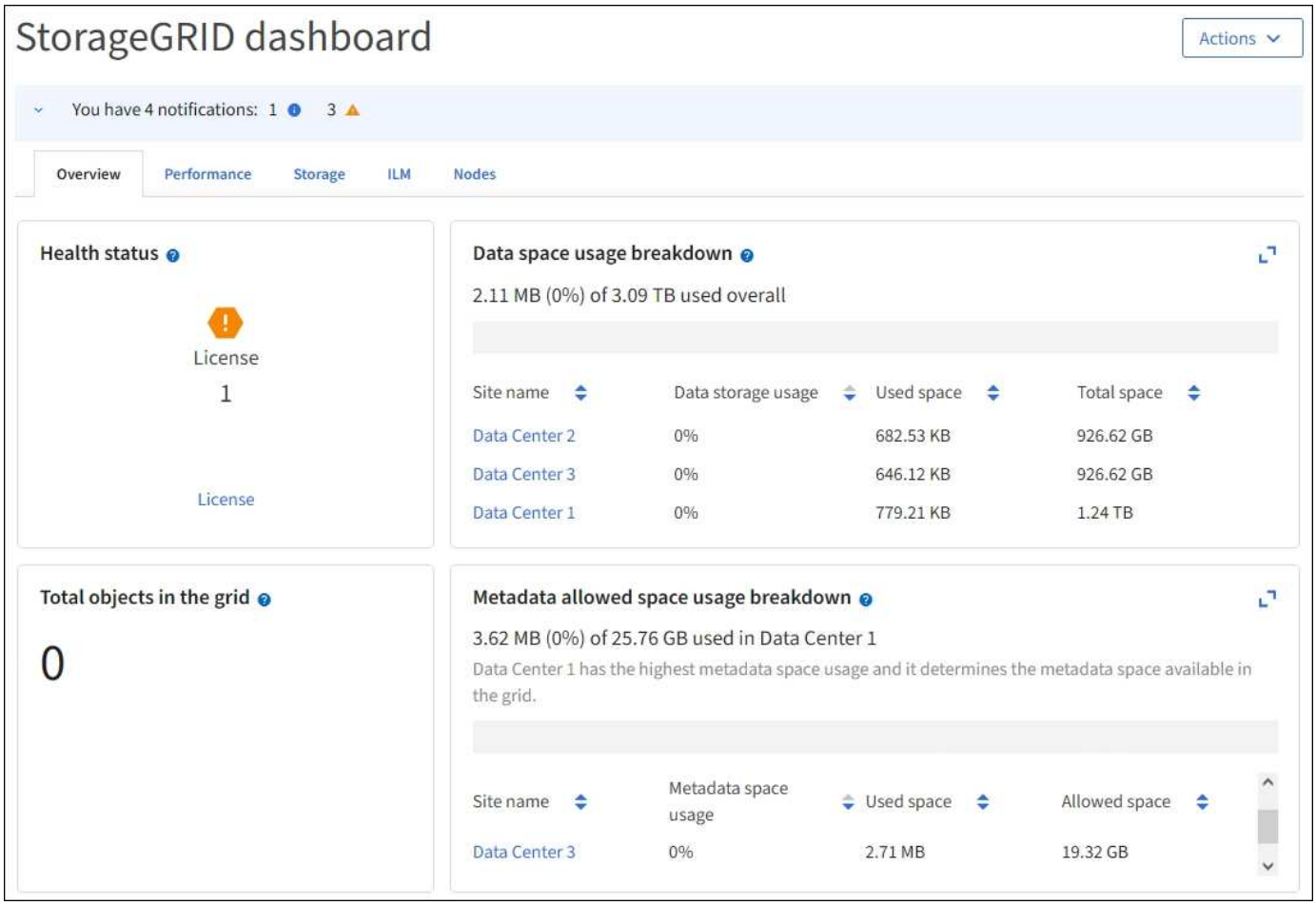
- Se StorageGRID utilizza SSO e in precedenza hai effettuato l'accesso a Grid Manager o a un account tenant:

  i. Inserisci **0** (ID account per Grid Manager) oppure seleziona **Grid Manager** se compare nell'elenco degli account recenti.

ii. Seleziona * Sign in*.

iii. Sign in con le tue credenziali SSO standard alla pagina di accesso SSO della tua organizzazione.

Dopo aver effettuato l'accesso, viene visualizzata la home page di Grid Manager, che include la dashboard. Per sapere quali informazioni sono fornite, vedere"Visualizza e gestisci la dashboard" .



Accedi a un altro nodo di amministrazione

Per accedere a un altro nodo di amministrazione, seguire questi passaggi.

Non si utilizza SSO

Passi

1. Nella barra degli indirizzi del browser, inserisci il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Includere il numero di porta, se necessario.
2. Inserisci il tuo nome utente e la password per Grid Manager.
3. Seleziona **Accedi**.

Utilizzo di SSO

Se StorageGRID utilizza SSO e hai effettuato l'accesso a un nodo amministrativo, puoi accedere ad altri nodi amministrativi senza dover effettuare nuovamente l'accesso.

Passi

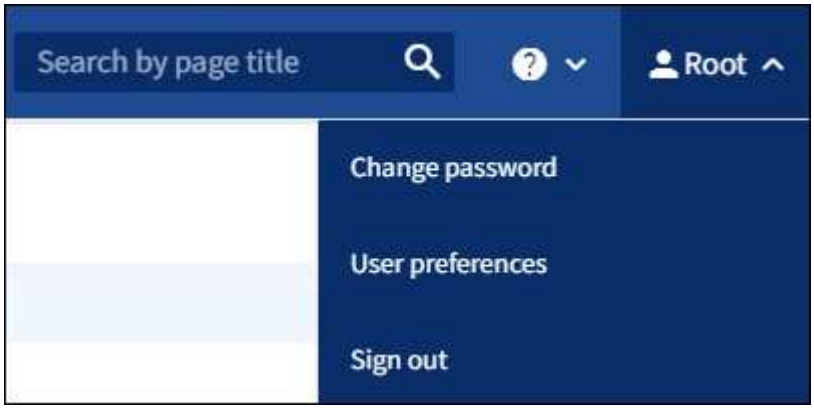
1. Inserisci il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione nella barra degli indirizzi del browser.
2. Se la sessione SSO è scaduta, inserisci nuovamente le tue credenziali.

Esci da Grid Manager

Una volta terminato di lavorare con Grid Manager, è necessario disconnettersi per impedire agli utenti non autorizzati di accedere al sistema StorageGRID . In base alle impostazioni dei cookie del browser, la chiusura del browser potrebbe non comportare la disconnessione dal sistema.

Passi

1. Seleziona il tuo nome utente nell'angolo in alto a destra.



2. Seleziona **Esci**.

Opzione	Descrizione
SSO non in uso	Hai effettuato la disconnessione dal nodo di amministrazione. Viene visualizzata la pagina di accesso di Grid Manager. **Nota:** se hai effettuato l'accesso a più di un nodo di amministrazione, devi disconnetterti da ciascun nodo.
SSO abilitato	Hai effettuato l'uscita da tutti i nodi amministrativi a cui stavi accedendo. Viene visualizzata la pagina di accesso a StorageGRID . **Grid Manager** è elencato come predefinito nel menu a discesa **Account recenti** e il campo **ID account** mostra 0. **Nota:** se l'SSO è abilitato e hai effettuato l'accesso anche a Tenant Manager, devi anche"uscire dall'account dell'inquilino" A"uscire da SSO" .

Cambia la tua password

Se sei un utente locale di Grid Manager, puoi modificare la tua password.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .

Informazioni su questo compito

Se accedi a StorageGRID come utente federato o se è abilitato l'accesso singolo (SSO), non puoi modificare la password in Grid Manager. In alternativa, è necessario modificare la password nella fonte di identità esterna, ad esempio Active Directory o OpenLDAP.

Passi

1. Dall'intestazione Grid Manager, seleziona ***il tuo nome*** > **Cambia password**.
2. Inserisci la tua password attuale.
3. Digita una nuova password.

   La password deve contenere almeno 8 e non più di 32 caratteri. Le password sono sensibili alle maiuscole e alle minuscole.
4. Reinserisci la nuova password.
5. Seleziona **Salva**.

Visualizza le informazioni sulla licenza StorageGRID

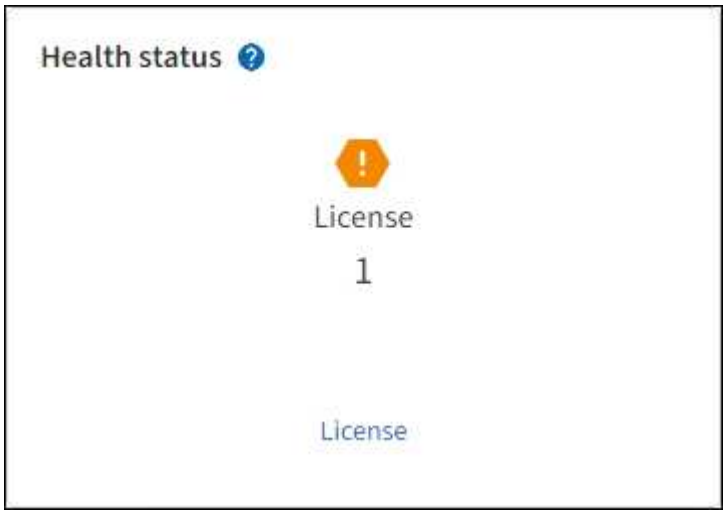
Ogni volta che è necessario, è possibile visualizzare le informazioni sulla licenza del sistema StorageGRID , ad esempio la capacità di archiviazione massima della griglia.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .

Informazioni su questo compito

Se si verifica un problema con la licenza software per questo sistema StorageGRID , la scheda Stato di integrità nella dashboard include un'icona Stato licenza e un collegamento **Licenza**. Il numero indica il numero di problemi relativi alla licenza.



Passi

1. Accedi alla pagina Licenza eseguendo una delle seguenti operazioni:
   - Selezionare **MANUTENZIONE** > **Sistema** > **Licenza**.
   - Dalla scheda Stato di integrità nella dashboard, seleziona l'icona Stato licenza o il collegamento **Licenza**.

     Questo collegamento appare solo se c'è un problema con la licenza.

2. Visualizza i dettagli di sola lettura per la licenza corrente:
    - ID di sistema StorageGRID , ovvero il numero di identificazione univoco per questa installazione StorageGRID
    - Numero di serie della licenza
    - Tipo di licenza, **Perpetua** o **Abbonamento**
    - Capacità di stoccaggio autorizzata della rete
    - Capacità di archiviazione supportata
    - Data di scadenza della licenza. **N/D** appare per una licenza perpetua.
    - Data di fine del supporto

      Questa data viene letta dal file di licenza corrente e potrebbe non essere aggiornata se hai esteso o rinnovato il contratto di assistenza dopo aver ottenuto il file di licenza. Per aggiornare questo valore, vedere"Aggiorna le informazioni sulla licenza StorageGRID" . È anche possibile visualizzare la data di fine effettiva del contratto utilizzando Active IQ.

    - Contenuto del file di testo della licenza

Aggiorna le informazioni sulla licenza StorageGRID

È necessario aggiornare le informazioni sulla licenza del sistema StorageGRID ogni volta che cambiano i termini della licenza. Ad esempio, è necessario aggiornare le informazioni sulla licenza se si acquista capacità di archiviazione aggiuntiva per la propria rete.

Prima di iniziare

- Hai un nuovo file di licenza da applicare al tuo sistema StorageGRID .
- Hai"autorizzazioni di accesso specifiche" .
- Hai la passphrase di provisioning.

Passi

1. Selezionare **MANUTENZIONE** > **Sistema** > **Licenza**.
2. Nella sezione Aggiorna licenza, seleziona **Sfoglia**.
3. Individuare e selezionare il nuovo file di licenza(`.txt`).

   Il nuovo file di licenza viene convalidato e visualizzato.

4. Immettere la passphrase di provisioning.
5. Seleziona **Salva**.

Utilizzare la API

Utilizzare l'API di gestione della griglia

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Grid Management anziché l'interfaccia utente di Grid Manager. Ad esempio, potresti voler utilizzare l'API per automatizzare le operazioni o per creare più entità, come gli utenti, più

rapidamente.

Risorse di alto livello

L'API di gestione della griglia 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 maggiori dettagli, vedere "Utilizzare un account tenant" .
- `/private`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate. Le API private sono soggette a modifiche senza preavviso. Anche gli endpoint privati StorageGRID ignorano la versione API della richiesta.

Inviare richieste API

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

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

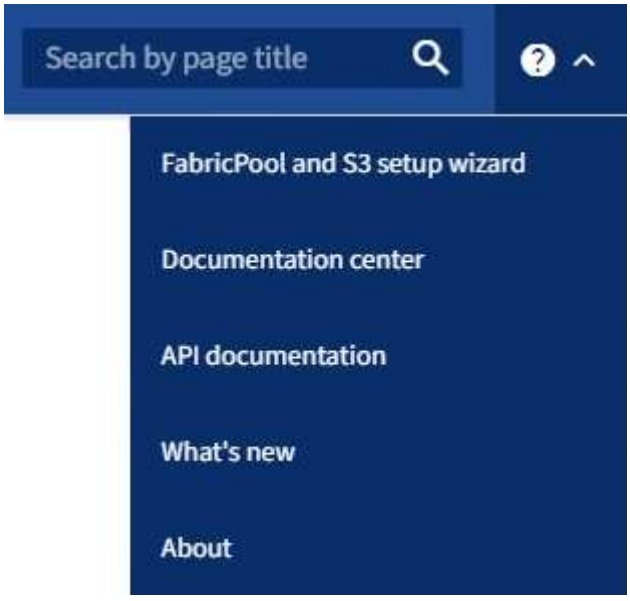
Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

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

Passi

1. Dall'intestazione di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API**.



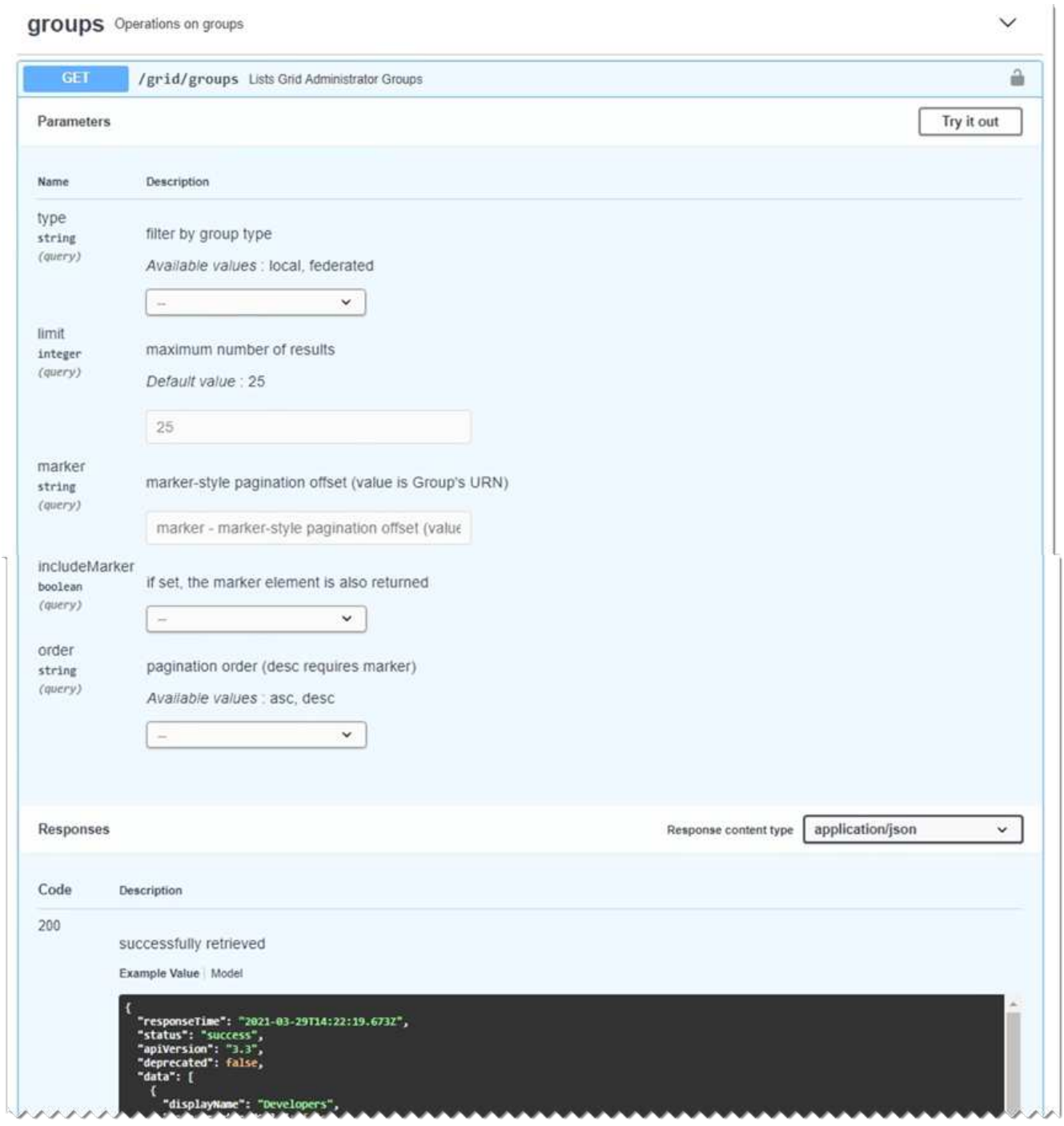
2. Per eseguire un'operazione con l'API privata, seleziona **Vai alla documentazione dell'API privata** nella pagina dell'API di gestione StorageGRID .

Le API private sono soggette a modifiche senza preavviso. Anche gli endpoint privati StorageGRID ignorano la versione API della richiesta.

3. Selezionare l'operazione desiderata.

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

4. 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.



5. Determina se la richiesta richiede parametri aggiuntivi, come un gruppo o un ID utente. Quindi, ottieni

questi valori. Potrebbe essere necessario inviare prima una richiesta API diversa per ottenere le informazioni necessarie.

6. Determina se è necessario modificare il corpo della richiesta di esempio. In tal caso, puoi selezionare **Modello** per conoscere i requisiti per ciascun campo.
7. Seleziona **Provalo**.
8. Fornire tutti i parametri richiesti o modificare il corpo della richiesta come richiesto.
9. Selezionare **Esegui**.
10. Esaminare il codice di risposta per determinare se la richiesta è andata a buon fine.

Operazioni dell'API di gestione della griglia

L'API di gestione della griglia organizza le operazioni disponibili nelle seguenti sezioni.

Questo elenco include solo le operazioni disponibili nell'API pubblica.

- **account**: operazioni per gestire gli account dei tenant di archiviazione, tra cui la creazione di nuovi account e il recupero dell'utilizzo dello spazio di archiviazione per un determinato account.
- **alert-history**: Operazioni sugli avvisi risolti.
- **alert-receivers**: Operazioni sui destinatari delle notifiche di avviso (e-mail).
- **alert-rules**: Operazioni sulle regole di avviso.
- **alert-silences**: Operazioni sui silenzi degli avvisi.
- **avvisi**: Operazioni sugli avvisi.
- **audit**: Operazioni per elencare e aggiornare la configurazione di audit.
- **auth**: Operazioni per eseguire l'autenticazione della sessione utente.

  L'API di gestione della griglia supporta lo schema di autenticazione Bearer Token. Per effettuare l'accesso, è necessario fornire 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 successive richieste API ("Authorization: Bearer *token*"). Il token scade dopo 16 ore.

  Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "Autenticazione all'API se è abilitato l'accesso singolo".

  Per informazioni su come migliorare la sicurezza dell'autenticazione, vedere "Protezione contro la falsificazione delle richieste tra siti".

- **client-certificates**: Operazioni per configurare i certificati client in modo che StorageGRID sia accessibile in modo sicuro tramite strumenti di monitoraggio esterni.
- **config**: Operazioni relative alla versione del prodotto e alle versioni dell'API di gestione della griglia. È possibile elencare la versione di rilascio del prodotto e le versioni principali dell'API Grid Management supportate da tale versione, nonché disabilitare le versioni obsolete dell'API.
- **deactivated-features**: Operazioni per visualizzare le funzionalità che potrebbero essere state disattivate.
- **dns-servers**: Operazioni per elencare e modificare i server DNS esterni configurati.
- **drive-details**: Operazioni sulle unità per modelli specifici di dispositivi di archiviazione.

- **endpoint-domain-names**: Operazioni per elencare e modificare i nomi di dominio degli endpoint S3.
- **erasure-coding**: Operazioni sui profili di codifica di cancellazione.
- **espansione**: Operazioni di espansione (a livello di procedura).
- **expansion-nodes**: 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 delle reti di griglia.
- **grid-passwords**: Operazioni per la gestione delle password della griglia.
- **gruppi**: operazioni per gestire i gruppi di amministratori di griglia locali e per recuperare i gruppi di amministratori di griglia federati da un server LDAP esterno.
- **identity-source**: Operazioni per configurare una fonte di identità esterna e per sincronizzare manualmente le informazioni sui gruppi federati e sugli utenti.
- **ilm**: Operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **in-progress-procedures**: Recupera le procedure di manutenzione attualmente in corso.
- **licenza**: Operazioni per recuperare e aggiornare la licenza StorageGRID .
- **logs**: Operazioni per la raccolta e il download dei file di registro.
- **metriche**: operazioni sulle metriche StorageGRID , tra cui query di metriche istantanee in un singolo punto nel tempo e query di metriche di intervallo in un intervallo di tempo. L'API di gestione della griglia utilizza lo strumento di monitoraggio dei sistemi Prometheus come fonte di dati backend. Per informazioni sulla creazione di query Prometheus, consultare il sito web di Prometheus.

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

- **node-details**: Operazioni sui dettagli del nodo.
- **node-health**: Operazioni sullo stato di integrità del nodo.
- **node-storage-state**: Operazioni sullo stato di archiviazione del nodo.
- **ntp-servers**: operazioni per elencare o aggiornare i server NTP (Network Time Protocol) esterni.
- **oggetti**: Operazioni sugli oggetti e sui metadati degli oggetti.
- **recovery**: Operazioni per la procedura di recupero.
- **recovery-package**: Operazioni per scaricare il pacchetto di ripristino.
- **regioni**: Operazioni per visualizzare e creare regioni.
- **s3-object-lock**: Operazioni sulle impostazioni globali di S3 Object Lock.
- **server-certificate**: Operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp**: Operazioni sulla configurazione SNMP corrente.
- **storage-watermarks**: Filigrane del nodo di archiviazione.
- **traffic-classes**: Operazioni per le policy di classificazione del traffico.
- **untrusted-client-network**: Operazioni sulla configurazione della rete client non attendibile.
- **utenti**: operazioni per visualizzare e gestire gli utenti di Grid Manager.

Controllo delle versioni dell'API di gestione della griglia

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

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

`https://hostname_or_ip_address/api/v4/authorize`

La versione principale dell'API viene aggiornata quando vengono apportate modifiche che non sono compatibili con le versioni precedenti. La versione secondaria dell'API viene aggiornata quando vengono apportate modifiche *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o nuove proprietà.

L'esempio seguente illustra come la versione dell'API viene aumentata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Vecchia versione	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con le versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene abilitata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova versione delle funzionalità di StorageGRID, si continua ad avere accesso alla versione API precedente per almeno una versione delle funzionalità StorageGRID .

> È possibile configurare le versioni supportate. Consultare la sezione **config** della documentazione dell'API Swagger per"API di gestione della griglia" per maggiori informazioni. Dopo aver aggiornato tutti i client API per utilizzare la versione più recente, è necessario disattivare il supporto per la versione precedente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Obsoleto: vero"
- Il corpo della risposta JSON include "deprecated": true
- Un avviso obsoleto è stato aggiunto a nms.log. Per esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determina quali versioni API sono supportate nella versione corrente

Utilizzare il `GET /versions` Richiesta API per restituire un elenco delle principali versioni API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione API utilizzando un parametro di percorso(`/api/v4`) o un'intestazione(`Api-Version: 4`). Se si specificano entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protezione contro la falsificazione delle richieste tra siti (CSRF)

È possibile contribuire a proteggersi dagli attacchi CSRF (Cross-Site Request Forgery) 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 abilitarla o meno al momento dell'accesso.

Un aggressore in grado di attivare una richiesta a un sito diverso (ad esempio con un modulo HTTP POST) può far sì che determinate richieste vengano effettuate utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggersi dagli attacchi CSRF utilizzando i token CSRF. Se abilitato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro del corpo POST specifico.

Per abilitare 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 è impostato con un valore casuale per gli accessi a Grid Manager e `AccountCsrfToken` il cookie viene impostato con un valore casuale per gli accessi al Tenant Manager.

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

- IL `X-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie token CSRF.
- Per gli endpoint che accettano un corpo codificato in formato: A `csrfToken` parametro del corpo della richiesta codificato nel modulo.

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

> Le richieste che hanno impostato un cookie token CSRF applicheranno anche l'intestazione "Content-Type: application/json" per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare l'API se è abilitato l'accesso singolo

Utilizzare l'API se è abilitato l'accesso singolo (Active Directory)

Se hai"configurato e abilitato l'accesso singolo (SSO)" e si utilizza Active Directory come provider SSO, è necessario inviare una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso singolo

Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO.

Prima di iniziare

- Conosci il nome utente e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

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

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

- Un esempio di flusso di lavoro delle richieste curl.

  Il flusso di lavoro curl potrebbe interrompersi se eseguito troppo lentamente. Potresti visualizzare l'errore: `A valid SubjectConfirmation was not found on this Response`.

  > Il flusso di lavoro curl di esempio non protegge la password dalla visualizzazione da parte di altri utenti.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version`.

Passi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
   - Utilizzare il `storagegrid-ssoauth.py` Script Python. Vai al passaggio 2.
   - Utilizzare le richieste curl. Vai al passaggio 3.
2. Se vuoi usare il `storagegrid-ssoauth.py` script, passa lo script all'interprete Python ed esegui lo script.

   Quando richiesto, immettere i valori per i seguenti argomenti:

   - Il metodo SSO. Inserisci ADFS o adfs.
   - Il nome utente SSO
   - Il dominio in cui è installato StorageGRID
   - L'indirizzo per StorageGRID
   - ID dell'account tenant, se si desidera accedere all'API di gestione tenant.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   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. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.
3. Se si desidera utilizzare le richieste curl, attenersi alla seguente procedura.
   a. Dichiarare le variabili necessarie per effettuare 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 di gestione della griglia, utilizzare 0 come `TENANTACCOUNTID` .

b. Per ricevere un URL di autenticazione firmato, inviare una richiesta 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 saranno trasmessi 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 codificato in URL, ma non include il livello 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. Salva il `SAMLRequest` dalla risposta per utilizzarla nei comandi successivi.

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

d. Ottieni un URL completo che includa l'ID della richiesta client da AD FS.

Un'opzione è quella di 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. Salva l'ID della richiesta del client dalla risposta.

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

f. Invia le tue credenziali all'azione del modulo dalla 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=FormsAuthentication" --include
```

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

> Se l'autenticazione a più fattori (MFA) è abilitata per il tuo 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. Salva il `MSISAuth` cookie dalla risposta.

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

h. Invia una richiesta GET alla posizione specificata con i cookie dal POST di autenticazione.

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

Le intestazioni della risposta conterranno informazioni sulla sessione AD FS per un successivo utilizzo in caso di disconnessione, mentre il corpo della risposta conterrà SAMLResponse in un campo modulo 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. Salva il `SAMLResponse` dal campo nascosto:

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

j. Utilizzando il salvato `SAMLResponse` , crea uno StorageGRID`/api/saml-response` richiesta di generazione di un token di autenticazione StorageGRID .

Per `RelayState` , utilizzare l'ID dell'account tenant oppure utilizzare 0 se si desidera accedere all'API di gestione della griglia.

```
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. Salva il token di autenticazione nella risposta come `MYTOKEN` .

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

Ora puoi usare `MYTOKEN` per altre richieste, in modo simile a come utilizzeresti l'API se non si utilizzasse l'SSO.

Disconnettersi dall'API se è abilitato l'accesso singolo

Se è stato abilitato l'accesso singolo (SSO), è necessario inviare una serie di richieste API per disconnettersi dall'API di gestione della griglia o dall'API di gestione dei tenant. Queste istruzioni si applicano se si utilizza Active Directory come provider di identità SSO

Informazioni su questo compito

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

Passi

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. Salva l'URL di disconnessione.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...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 solo tramite API.

```
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 portatore StorageGRID .

L'eliminazione del token portatore StorageGRID funziona allo stesso modo dell'eliminazione senza SSO. Se non viene specificato `cookie "sso=true", l'utente viene disconnesso da StorageGRID senza che ciò influisca sullo stato SSO.

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

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

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

Utilizzare l'API se è abilitato l'accesso Single Sign-On (Azure)

Se hai"configurato e abilitato l'accesso singolo (SSO)" e si utilizza Azure come provider SSO, è possibile utilizzare due script di esempio per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso Single Sign-On di Azure

Queste istruzioni si applicano se si utilizza Azure come provider di identità SSO

Prima di iniziare

- Conosci l'indirizzo email e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, è possibile utilizzare i seguenti script di esempio:

- IL `storagegrid-ssoauth-azure.py` Script Python
- IL `storagegrid-ssoauth-azure.js` Script Node.js

Entrambi gli script si trovano nella directory dei file di installazione StorageGRID(`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian, e `./vsphere` per VMware).

Per scrivere la tua integrazione API con Azure, consulta `storagegrid-ssoauth-azure.py` sceneggiatura. Lo script Python invia direttamente due richieste a StorageGRID (prima per ottenere SAMLRequest e poi per ottenere il token di autorizzazione) e chiama anche lo script Node.js per interagire con Azure ed eseguire le operazioni SSO.

Le operazioni SSO possono essere eseguite utilizzando una serie di richieste API, ma non è un'operazione semplice. Il modulo Puppeteer Node.js viene utilizzato per eseguire lo scraping dell'interfaccia Azure SSO.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version` .

Passi

1. Installare le dipendenze richieste, come segue:
   a. Installa Node.js (vedi "https://nodejs.org/en/download/").

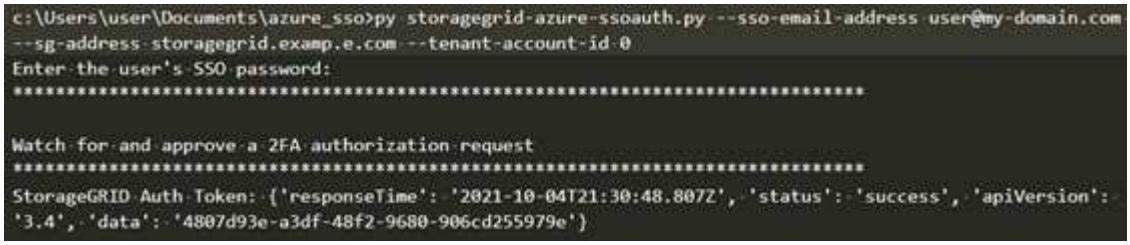
b. Installa i moduli Node.js richiesti (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passare lo script Python all'interprete Python per eseguirlo.

   Lo script Python chiamerà quindi lo script Node.js corrispondente per eseguire le interazioni SSO di Azure.

3. Quando richiesto, immettere i valori per i seguenti argomenti (o passarli utilizzando i parametri):
   - L'indirizzo e-mail SSO utilizzato per accedere ad Azure
   - L'indirizzo per StorageGRID
   - ID dell'account tenant, se si desidera accedere all'API di gestione tenant
4. Quando richiesto, immettere la password e prepararsi a fornire un'autorizzazione MFA ad Azure, se richiesto.



> Lo script presuppone che l'autenticazione MFA venga eseguita tramite Microsoft Authenticator. Potrebbe essere necessario modificare lo script per supportare altre forme di MFA (ad esempio l'inserimento di un codice ricevuto in un messaggio di testo).

Il token di autorizzazione StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

Utilizzare l'API se è abilitato l'accesso singolo (PingFederate)

Se hai"configurato e abilitato l'accesso singolo (SSO)" e utilizzi PingFederate come provider SSO, devi inviare una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso singolo

Queste istruzioni si applicano se si utilizza PingFederate come provider di identità SSO

Prima di iniziare

- Conosci il nome utente e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

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

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

VMware).

- Un esempio di flusso di lavoro delle richieste curl.

  Il flusso di lavoro curl potrebbe interrompersi se eseguito troppo lentamente. Potresti visualizzare l'errore: `A valid SubjectConfirmation was not found on this Response`.

  > Il flusso di lavoro curl di esempio non protegge la password dalla visualizzazione da parte di altri utenti.

  Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version`.

Passi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
   - Utilizzare il `storagegrid-ssoauth.py` Script Python. Vai al passaggio 2.
   - Utilizzare le richieste curl. Vai al passaggio 3.
2. Se vuoi usare il `storagegrid-ssoauth.py` script, passa lo script all'interprete Python ed esegui lo script.

   Quando richiesto, immettere i valori per i seguenti argomenti:

   - Il metodo SSO. È possibile immettere qualsiasi variante di "pingfederate" (PINGFEDERATE, pingfederate e così via).
   - Il nome utente SSO
   - Il dominio in cui è installato StorageGRID . Questo campo non è utilizzato per PingFederate. Puoi lasciarlo vuoto o inserire qualsiasi valore.
   - L'indirizzo per StorageGRID
   - ID dell'account tenant, se si desidera accedere all'API di gestione tenant.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_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. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

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

   a. Dichiarare le variabili necessarie per effettuare l'accesso.

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

Per accedere all'API di gestione della griglia, utilizzare 0 come `TENANTACCOUNTID` .

b. Per ricevere un URL di autenticazione firmato, inviare una richiesta 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 codificato in URL, ma non include il livello di codifica JSON aggiuntivo.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salva il `SAMLRequest` dalla risposta per utilizzarla nei comandi successivi.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Esporta la risposta e il cookie e ripeti la risposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Esporta il valore 'pf.adapterId' e riproduci la risposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Esporta il valore 'href' (rimuovi la barra finale /) e riproduci la risposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Esporta il valore 'azione':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Invia i cookie insieme alle credenziali:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Salva il `SAMLResponse` dal campo nascosto:

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

j. Utilizzando il salvato `SAMLResponse` , crea uno StorageGRID `/api/saml-response` richiesta di generazione di un token di autenticazione StorageGRID .

Per `RelayState` , utilizzare l'ID dell'account tenant oppure utilizzare 0 se si desidera accedere all'API di gestione della griglia.

```
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. Salva il token di autenticazione nella risposta come `MYTOKEN` .

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

Ora puoi usare `MYTOKEN` per altre richieste, in modo simile a come utilizzeresti l'API se non si utilizzasse l'SSO.

Disconnettersi dall'API se è abilitato l'accesso singolo

Se è stato abilitato l'accesso singolo (SSO), è necessario inviare una serie di richieste API per disconnettersi dall'API di gestione della griglia o dall'API di gestione dei tenant. Queste istruzioni si applicano se si utilizza PingFederate come provider di identità SSO

Informazioni su questo compito

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

Passi

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://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Salva l'URL di disconnessione.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...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 solo tramite API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Eliminare il token portatore StorageGRID .

L'eliminazione del token portatore StorageGRID funziona allo stesso modo dell'eliminazione senza SSO. Se non viene specificato `cookie "sso=true", l'utente viene disconnesso da StorageGRID senza che ciò influisca sullo stato SSO.

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

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

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

Disattivare le funzionalità con l'API

È possibile utilizzare l'API Grid Management per disattivare completamente determinate funzionalità nel sistema StorageGRID . Quando una funzionalità viene disattivata, a nessuno può essere assegnata l'autorizzazione per eseguire le attività correlate a tale funzionalità.

Informazioni su questo compito

Il sistema Funzionalità disattivate consente di impedire l'accesso a determinate funzionalità del sistema StorageGRID . La disattivazione di una funzionalità è l'unico modo per impedire all'utente root o agli utenti che appartengono a gruppi di amministratori con autorizzazione di **accesso root** di utilizzare tale funzionalità.

Per capire come questa funzionalità potrebbe essere utile, consideriamo il seguente scenario:

_La società A è un fornitore di servizi che affitta la capacità di archiviazione del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei propri locatari, la Società A desidera garantire che i propri dipendenti non possano mai accedere all'account di un locatario dopo che l'account è stato distribuito.

_L'azienda A può raggiungere questo obiettivo utilizzando il sistema Disattiva funzionalità nell'API di gestione della griglia. Disattivando completamente la funzionalità **Modifica password root del tenant** in Grid Manager (sia nell'interfaccia utente che nell'API), la Società A garantisce che gli utenti amministratori, inclusi l'utente root e gli utenti appartenenti a gruppi con autorizzazione di **Accesso root**, non possano modificare la password per l'utente root di alcun account tenant.

Passi

1. Accedi alla documentazione Swagger per l'API Grid Management. Vedere "Utilizzare l'API di gestione della griglia" .
2. Individuare l'endpoint Disattiva funzionalità.
3. Per disattivare una funzionalità, ad esempio Modifica password root del tenant, invia un corpo all'API in questo modo:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Una volta completata la richiesta, la funzionalità Modifica password root del tenant viene disabilitata. L'autorizzazione di gestione **Modifica password root del tenant** non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password root per un tenant fallirà con "403 Forbidden".

Riattiva le funzionalità disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzionalità che è stata disattivata. Tuttavia, se si desidera impedire che le funzionalità disattivate vengano riattivate, è possibile disattivare la funzionalità **activateFeatures** stessa.

> La funzione **activateFeatures** non può essere riattivata. Se decidi di disattivare questa funzione, tieni presente che perderai definitivamente la possibilità di riattivare qualsiasi altra funzione disattivata. Per ripristinare eventuali funzionalità perse è necessario contattare l'assistenza tecnica.

Passi

1. Accedi alla documentazione Swagger per l'API Grid Management.
2. Individuare l'endpoint Disattiva funzionalità.
3. Per riattivare tutte le funzionalità, invia un corpo all'API in questo modo:

```
{ "grid": null }
```

Una volta completata questa richiesta, tutte le funzionalità, inclusa la funzionalità Modifica password root del tenant, vengono riattivate. L'autorizzazione di gestione **Modifica password root del tenant** ora viene visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password root per un tenant avrà esito positivo, a condizione che l'utente disponga dell'autorizzazione di gestione **Accesso root** o **Modifica password root del tenant**.

L'esempio precedente fa sì che tutte le funzionalità disattivate vengano riattivate. Se sono state disattivate altre funzionalità che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzionalità Modifica password root del tenant e continuare a disattivare l'autorizzazione di gestione storageAdmin, inviare questa richiesta PUT:

```
{ "grid": {"storageAdmin": true} }
```

Informazioni sul copyright

Informazioni sul marchio commerciale