Usa la API

StorageGRID software

NetApp
July 23, 2026

Sommario

Usa la API

Utilizzare l'API di gestione della griglia StorageGRID

Puoi eseguire le 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.

${post_edited_translations.segment}

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 i dettagli, consulta "Usa un tenant account".
- `/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. Gli endpoint privati di StorageGRID ignorano anche la versione dell'API della richiesta.

Invia richieste API

L'API di gestione Grid utilizza la piattaforma API open source Swagger. Swagger fornisce un'interfaccia utente intuitiva che permette a sviluppatori e non sviluppatori di eseguire operazioni in real-time in StorageGRID tramite l'API.

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

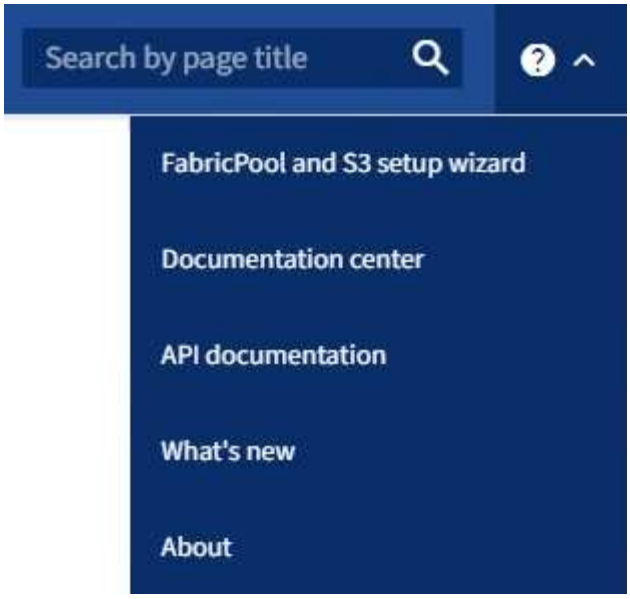
Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

> Qualsiasi operazione API che esegui tramite la pagina web della documentazione API è un'operazione live. Fai attenzione a non creare, aggiornare o eliminare per errore dati di configurazione o altri dati.

Passaggi

1. Dall'intestazione di Grid Manager, seleziona l'icona di aiuto e seleziona **API documentation**.



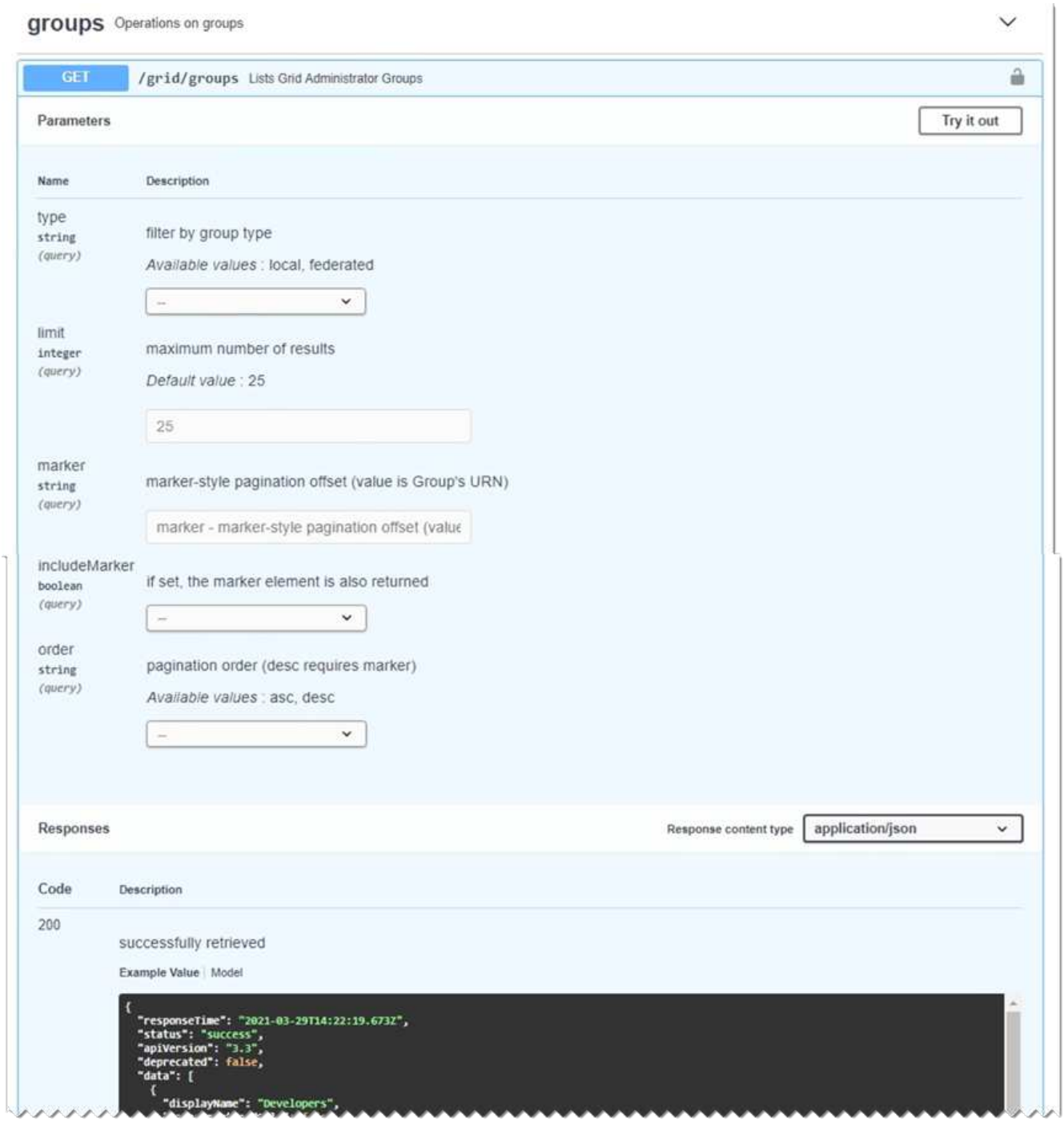
2. Per eseguire un'operazione con l'API privata, seleziona **Vai alla documentazione dell'API privata** nella pagina StorageGRID Management API.

   Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione dell'API della richiesta.

3. ${post_edited_translations.segment}

   Quando espandi un'operazione API, puoi vedere le azioni HTTP disponibili, come GET, PUT, UPDATE e DELETE.

4. ${post_edited_translations.segment}



5. Verifica se la richiesta richiede parametri aggiuntivi, come un ID di gruppo o un ID utente. Quindi, recupera questi valori. Potresti dover prima effettuare una richiesta API diversa per ottenere le informazioni di cui hai bisogno.
6. Determina se devi modificare il corpo della richiesta di esempio. In tal caso, puoi selezionare **Model** per conoscere i requisiti di ciascun campo.
7. ${post_edited_translations.segment}
8. Fornisci i parametri richiesti o modifica il corpo della richiesta come necessario.
9. Seleziona **Esegui**.
10. Esamina il codice di risposta per determinare se la richiesta è andata a buon fine.

Operazioni Grid Management API in StorageGRID

${post_edited_translations.segment}

${post_edited_translations.segment}

- **accounts**: Operazioni per gestire gli account tenant di archiviazione, inclusa la creazione di nuovi account e il recupero dell'utilizzo dello storage per un determinato account.
- **alert-history**: Operazioni sugli avvisi risolti.
- ${post_edited_translations.segment}
- **alert-rules**: Operazioni sulle regole di alert.
- **alert-silences**: Operazioni sui silenziamenti di allerta.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **auth**: Operazioni per eseguire l'autenticazione della sessione utente.

  L'API Grid Management supporta lo schema di autenticazione Bearer Token. Per accedere, fornisci un nome utente e una password nel corpo JSON della richiesta di autenticazione (cioè `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*"). Il token scade dopo 16 ore.

  Se il single sign-on è abilitato per il sistema StorageGRID, devi eseguire passaggi diversi per autenticarti. Vedi "Autenticazione nell'API se il single sign-on è abilitato".

  Consulta "Proteggere da Cross-Site Request Forgery" per informazioni su come migliorare la sicurezza con autenticazione.

- ${post_edited_translations.segment}
- **config**: Operazioni relative alla release del prodotto e alle versioni della Grid Management API. Puoi visualizzare la versione della release del prodotto e le versioni principali della Grid Management API supportate da quella release, e puoi disabilitare le versioni obsolete dell'API.
- **funzionalità-disattivate**: Operazioni per visualizzare le funzionalità che potrebbero essere state disattivate.
- **dns-servers**: Operazioni per elencare e modificare i server DNS esterni configurati.
- **dettagli unità**: Operazioni sulle unità per modelli specifici di storage appliance.
- **endpoint-domain-names**: Operazioni per elencare e modificare i nomi di dominio degli endpoint S3.
- **codifica di cancellazione**: Operazioni sui profili di codifica di cancellazione.
- **espansione**: Operazioni su espansione (a livello di procedura).
- **expansion-nodes**: Operazioni sull'espansione (a livello di nodo).
- **expansion-sites**: Operazioni di espansione (a livello di sito).
- **grid-networks**: Operazioni per visualizzare e modificare l'elenco delle reti Grid.
- **grid-passwords**: Operazioni per la gestione delle password della griglia.
- **gruppi**: Operazioni per gestire i gruppi di amministratori Grid locali e per recuperare i gruppi di

amministratori Grid federati da un LDAP server esterno.

- **identity-source**: Operazioni per configurare un'origine di identità esterna e per sincronizzare manualmente le informazioni di gruppi e utenti federati.
- ${post_edited_translations.segment}
- **in-progress-procedures**: Recupera le procedure di manutenzione attualmente in corso.
- **licenza**: Operazioni per recuperare e aggiornare la licenza di StorageGRID.
- **logs**: Operazioni per la raccolta e il download dei file di log.v
- **metrics**: Operazioni sulle metriche di StorageGRID, incluse query di metriche istantanee in un singolo momento e query di metriche su un intervallo di tempo. La Grid Management API utilizza lo strumento di monitoraggio dei sistemi Prometheus come backend data source. Per informazioni sulla creazione di query Prometheus, consulta il sito web di Prometheus.

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

- ${post_edited_translations.segment}
- **node-health**: Operazioni sullo stato di salute del nodo.
- ${post_edited_translations.segment}
- **ntp-servers**: Operazioni per elencare o aggiornare i server esterni Network Time Protocol (NTP).
- **oggetti**: Operazioni su oggetti e metadati degli oggetti.
- **recupero**: Operazioni per la procedura di recupero.
- ${post_edited_translations.segment}
- **regioni**: Operazioni per visualizzare e creare regioni.
- **s3-object-lock**: Operazioni sulle impostazioni globali di S3 Object Lock.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **classi-di-traffico**: Operazioni per le policy di classificazione del traffico.
- ${post_edited_translations.segment}
- **Utenti**: Operazioni per visualizzare e gestire gli utenti di Grid Manager.

Versioning dell'API Grid Management in StorageGRID

${post_edited_translations.segment}

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 non 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 incrementata in base al tipo di modifiche apportate.

${post_edited_translations.segment}	Vecchia versione	${post_edited_translations.segment}
${post_edited_translations.segment}	2,1	2,2
Non compatibile con le versioni precedenti	2,1	3,0

Quando installi il software StorageGRID per la prima volta, viene abilitata solo la versione più recente dell'API. Tuttavia, quando esegui l'upgrade a una nuova release di funzionalità di StorageGRID, continui ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.

> Puoi configurare le versioni supportate. Consulta la sezione **config** della documentazione dell'API Swagger per "API di gestione della griglia" ulteriori informazioni. Dovresti disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API alla versione più recente.

Le richieste obsolete sono contrassegnate come deprecate nei seguenti modi:

- L'intestazione della risposta è "Deprecated: true"
- Il corpo della risposta JSON include "deprecated": true
- Viene aggiunto un avviso di deprecazione a nms.log. Ad esempio:

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

Determina quali versioni API sono supportate nella release corrente

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

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

Specifica una versione API per una richiesta

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

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

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

Proteggi contro gli attacchi Cross-Site Request Forgery (CSRF) in StorageGRID

Puoi aiutare a proteggerti dagli attacchi Cross-Site Request Forgery (CSRF) contro StorageGRID usando i token CSRF per rafforzare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; gli altri client API possono scegliere se abilitarla quando effettuano l'accesso.

Un utente malintenzionato in grado di attivare una richiesta a un sito diverso (ad esempio tramite un modulo HTTP POST) può far sì che determinate richieste vengano effettuate utilizzando i cookie dell'utente autenticato.

StorageGRID contribuisce a proteggere dagli attacchi CSRF tramite l'utilizzo di token CSRF. Quando questa funzionalità è abilitata, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro specifico del corpo di una richiesta POST.

Per abilitare la funzione, imposta il `csrfToken` parametro su `true` durante l'autenticazione. Il valore predefinito 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 true, viene impostato un cookie `GridCsrfToken` con un valore casuale per gli accessi al Grid Manager e il cookie `AccountCsrfToken` viene impostato con un valore casuale per gli accessi al Tenant Manager.

${post_edited_translations.segment}

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

Consulta la documentazione API online per altri esempi e dettagli.

> Le richieste che includono un cookie CSRF token impongono anche l'intestazione "Content-Type: application/json" per qualsiasi richiesta che si aspetti un corpo della richiesta in formato JSON, come ulteriore protezione contro gli attacchi CSRF.

${post_edited_translations.segment}

Utilizzare l'API StorageGRID se il single sign-on è abilitato (Active Directory)

Se hai "${post_edited_translations.segment}" e usi Active Directory come provider di single sign-on, devi inviare una serie di richieste API per ottenere un token di autenticazione valido per la Grid Management API o la Tenant Management API.

${post_edited_translations.segment}

Queste istruzioni si applicano se usi Active Directory come provider di identità SSO.

Prima di iniziare

- ${post_edited_translations.segment}
- Se vuoi accedere all'API di gestione dei tenant, devi conoscere l'ID account del tenant.

Informazioni su questa attività

${post_edited_translations.segment}

- Lo `storagegrid-ssoauth.py`script Python, che si trova nella directory dei file di installazione di StorageGRID (./rpms`per RHEL, `./debs`per Ubuntu o Debian, e `./vsphere`per VMware).
- Esempio di workflow di richieste curl.

  Il workflow curl potrebbe andare in timeout se lo esegui troppo lentamente. Potresti visualizzare l'errore: `A valid SubjectConfirmation was not found on this Response`.

  > ${post_edited_translations.segment}

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

Passaggi

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

   Quando richiesto, inserisci 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
- L'ID account tenant, se vuoi 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 di StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se l'SSO non fosse utilizzato.

3. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

```
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 alla Grid Management API, usa 0 come `TENANTACCOUNTID`.

   b. Per ricevere un URL di autenticazione firmato, invia una richiesta POST a `/api/v3/authorize-saml` e rimuovi 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
```

${post_edited_translations.segment}

```
{
    "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 `SAMLRequest` dalla risposta per utilizzarlo nei comandi successivi.

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

d. ${post_edited_translations.segment}

${post_edited_translations.segment}

```
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 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=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 modulo inviato 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. ${post_edited_translations.segment}

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

${post_edited_translations.segment}

```
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 le informazioni salvate `SAMLResponse`, effettua una richiesta StorageGRID`/api/saml-response` per generare un token di autenticazione StorageGRID.

Per `RelayState`, usa l'ID account tenant oppure usa 0 se vuoi accedere alla Grid Management API.

```
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, proprio come faresti con l'API se non stessi usando il single sign-on.

Disconnettiti dall'API se il single sign-on è abilitato

Se il single sign-on (SSO) è stato abilitato, devi inviare una serie di richieste API per disconnetterti dall'API di gestione della Grid o dall'API di gestione del tenant. Queste istruzioni si applicano se usi Active Directory come provider di identità SSO.

Informazioni su questa attività

Se necessario, puoi disconnetterti dall'API di StorageGRID effettuando il logout dalla pagina di single logout della tua organizzazione. Oppure puoi attivare il single logout (SLO) da StorageGRID, che richiede un bearer token di StorageGRID valido.

Passaggi

1. Per generare una richiesta di logout firmata, passa il 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. Invia una richiesta all'URL di logout per attivare SLO e per reindirizzare a StorageGRID.

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

Viene restituita la risposta 302. L'indirizzo di reindirizzamento non è applicabile al logout 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. Elimina il token bearer di StorageGRID.

L'eliminazione del token bearer di StorageGRID funziona allo stesso modo di quando non è attivo l'SSO. Se non viene specificato il cookie "sso=true", vieni disconnesso da StorageGRID senza che ciò influisca sullo stato dell'SSO.

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

Una `204 No Content`risposta indica che ora sei disconnesso.

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

Utilizzare l'API StorageGRID se single sign-on è abilitato (Entra ID)

Se hai "${post_edited_translations.segment}" e usi Entra ID come provider SSO, puoi utilizzare due script di esempio per ottenere un token di autenticazione valido per la Grid Management API o la Tenant Management API.

${post_edited_translations.segment}

Queste istruzioni si applicano se usi Entra ID 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 dei tenant, devi conoscere l'ID account del tenant.

Informazioni su questa attività

${post_edited_translations.segment}

- Lo `storagegrid-ssoauth-azure.py`script Python
- Lo `storagegrid-ssoauth-azure.js` script Node.js

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

Per scrivere la tua integrazione API con Entra ID, consulta lo script `storagegrid-ssoauth-azure.py`. Lo script Python effettua due richieste direttamente a StorageGRID (la prima per ottenere la SAMLRequest e la seconda per ottenere il token di autorizzazione) e richiama anche lo script Node.js per interagire con Entra ID ed eseguire le operazioni di single sign-on.

Le operazioni SSO possono essere eseguite tramite una serie di richieste API, ma la procedura non è semplice. Il modulo Puppeteer per Node.js viene utilizzato per estrarre dati dall'interfaccia SSO di Entra ID.

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

Passaggi

1. Installa le dipendenze necessarie come segue:
   a. Installa Node.js (vedi "https://nodejs.org/en/download/").
   b. Installa i moduli Node.js necessari (puppeteer e jsdom):

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

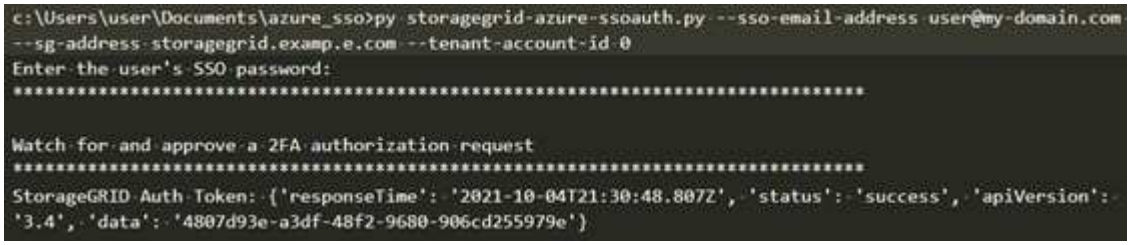
2. Passa lo script Python all'interprete Python per eseguire lo script.

   Lo script Python richiamerà quindi il corrispondente script Node.js per eseguire le interazioni single sign-on di Entra ID.

3. Quando richiesto, inserisci i valori per i seguenti argomenti (o passali usando i parametri):
   - L'indirizzo email SSO utilizzato per accedere a Entra ID
   - L'indirizzo per StorageGRID

- L'ID account tenant, se vuoi accedere alla Tenant Management API

4. Quando richiesto, inserisci la password e preparati a fornire un'autorizzazione MFA a Entra ID se richiesto.



> Lo script presuppone che l'autenticazione a più fattori (MFA) venga eseguita tramite Microsoft Authenticator. Potresti dover modificare lo script per supportare altre forme di MFA (come l'inserimento di un codice ricevuto tramite SMS).

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

Utilizzare l'API StorageGRID se il single sign-on è abilitato (PingFederate)

Se hai "${post_edited_translations.segment}" e usi PingFederate come provider SSO, devi inviare una serie di richieste API per ottenere un token di autenticazione valido per la Grid Management API o la Tenant Management API.

${post_edited_translations.segment}

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

Prima di iniziare

- ${post_edited_translations.segment}
- Se vuoi accedere all'API di gestione dei tenant, devi conoscere l'ID account del tenant.

Informazioni su questa attività

${post_edited_translations.segment}

- Lo `storagegrid-ssoauth.py`script Python, che si trova nella directory dei file di installazione di StorageGRID (./rpms`per RHEL, `./debs`per Ubuntu o Debian, e `./vsphere`per VMware).
- Esempio di workflow di richieste curl.

  Il workflow curl potrebbe andare in timeout se lo esegui troppo lentamente. Potresti visualizzare l'errore: `A valid SubjectConfirmation was not found on this Response`.

  > ${post_edited_translations.segment}

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

Passaggi

1. Seleziona uno dei seguenti metodi per ottenere un token di autenticazione:

- Usa lo `storagegrid-ssoauth.py` script Python. Vai al passaggio 2.
- Usa le richieste curl. Vai al passaggio 3.

2. Se vuoi usare lo script `storagegrid-ssoauth.py`, passa lo script all'interprete Python ed esegui lo script.

   Quando richiesto, inserisci i valori per i seguenti argomenti:

   - Il metodo SSO. Puoi inserire qualsiasi variante di "pingfederate" (PINGFEDERATE, pingfederate e così via).
   - Il nome utente SSO
   - Il dominio in cui è installato StorageGRID. Questo campo non viene utilizzato per PingFederate. Puoi lasciarlo vuoto o inserire un valore qualsiasi.
   - L'indirizzo per StorageGRID
   - L'ID account tenant, se vuoi 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 di StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se l'SSO non fosse utilizzato.

3. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

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

   Per accedere alla Grid Management API, usa 0 come `TENANTACCOUNTID`.

   b. Per ricevere un URL di autenticazione firmato, invia una richiesta POST a `/api/v3/authorize-saml` e rimuovi 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
```

${post_edited_translations.segment}

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

c. Salva `SAMLRequest` dalla risposta per utilizzarlo nei comandi successivi.

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

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

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

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

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

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

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

g. Esporta il valore 'action':

```
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 le informazioni salvate `SAMLResponse`, effettua una richiesta StorageGRID `/api/saml-response` per generare un token di autenticazione StorageGRID.

Per `RelayState`, usa l'ID account tenant oppure usa 0 se vuoi accedere alla Grid Management API.

```
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, proprio come faresti con l'API se non stessi usando il single sign-on.

Disconnettiti dall'API se il single sign-on è abilitato

Se il single sign-on (SSO) è stato abilitato, devi inviare una serie di richieste API per disconnetterti dalla Grid Management API o dalla Tenant Management API. Queste istruzioni si applicano se stai usando PingFederate come provider di identità SSO.

Informazioni su questa attività

Se necessario, puoi disconnetterti dall'API di StorageGRID effettuando il logout dalla pagina di single logout della tua organizzazione. Oppure puoi attivare il single logout (SLO) da StorageGRID, che richiede un bearer token di StorageGRID valido.

Passaggi

1. Per generare una richiesta di logout firmata, passa il 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. Invia una richiesta all'URL di logout per attivare SLO e per reindirizzare a StorageGRID.

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

Viene restituita la risposta 302. L'indirizzo di reindirizzamento non è applicabile al logout 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. Elimina il token bearer di StorageGRID.

   L'eliminazione del token bearer di StorageGRID funziona allo stesso modo di quando non è attivo l'SSO. Se non viene specificato il cookie "sso=true", vieni disconnesso da StorageGRID senza che ciò influisca sullo stato dell'SSO.

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

   Una `204 No Content`risposta indica che ora sei disconnesso.

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

Disattiva le funzionalità di StorageGRID tramite l'API

Puoi usare l'API Grid Management per disattivare completamente alcune funzionalità nel sistema StorageGRID. Quando una funzionalità viene disattivata, nessuno può ricevere le autorizzazioni per svolgere le attività relative a quella funzionalità.

Informazioni su questa attività

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

Per capire come questa funzionalità potrebbe esserti utile, considera il seguente scenario:

Company A è un service provider che affitta la capacità di archiviazione del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei propri leaseholder, Company A vuole assicurarsi che i propri dipendenti non possano mai accedere ad alcun account tenant dopo che l'account è stato attivato._

Company A può raggiungere questo obiettivo utilizzando il sistema Deactivate Features nell'API di Grid Management. Disattivando completamente la funzionalità **Change tenant root password** in Grid Manager (sia nell'interfaccia utente che nell'API), Company A si assicura che gli utenti Admin, inclusi l'utente root e gli utenti appartenenti a gruppi con il permesso **Root access**, non possano cambiare la password dell'utente root di nessun account tenant.

Passaggi

1. Accedi alla documentazione Swagger per l'API di gestione della griglia. Vedi "Usa l'API di gestione della griglia".
2. Individua l'endpoint Disattiva funzionalità.
3. ${post_edited_translations.segment}

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

Quando la richiesta è completata, la funzionalità "Cambia password di root del tenant" viene disabilitata. Il permesso di gestione **Change tenant root password** non viene più visualizzato nell'interfaccia utente e qualsiasi richiesta API che tenta di cambiare la password di root per un tenant fallirà con "403 Forbidden".

Riattiva le funzionalità disattivate

Per impostazione predefinita, puoi usare l'API Grid Management per riattivare una funzionalità che è stata disattivata. Tuttavia, se vuoi impedire che le funzionalità disattivate vengano mai riattivate, puoi disattivare la funzionalità **activateFeatures** stessa.

La funzionalità **activateFeatures** non può essere riattivata. Se decidi di disattivare questa funzionalità, tieni presente che perderai in modo permanente la possibilità di riattivare qualsiasi altra funzionalità disattivata. Devi contattare il supporto tecnico per ripristinare qualsiasi funzionalità persa.

Passaggi

1. Accedi alla documentazione Swagger per l'API di gestione della griglia.
2. Individua l'endpoint Disattiva funzionalità.
3. ${post_edited_translations.segment}

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

Quando questa richiesta è completata, tutte le funzionalità, inclusa la funzionalità **Cambia password di root del tenant**, vengono riattivate. L'autorizzazione di gestione **Cambia password di root del tenant** ora appare nell'interfaccia utente e qualsiasi richiesta API che tenta di cambiare la password di root per un tenant avrà successo, a condizione che l'utente abbia l'autorizzazione di gestione **Access root** o **Cambia password di 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, devi specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzionalità Cambia password root del tenant e continuare a disattivare l'autorizzazione di gestione storageAdmin, invia questa richiesta PUT: `{ "grid": {"storageAdmin": true} }`