



Erste Schritte mit Grid Manager

StorageGRID software

NetApp
January 15, 2026

Inhalt

Erste Schritte mit Grid Manager	1
Anforderungen an einen Webbrowser	1
Melden Sie sich beim Grid Manager an	1
Melden Sie sich beim Grid-Manager beim ersten Admin-Node an	2
Melden Sie sich bei einem anderen Admin-Node an	3
Melden Sie sich vom Grid Manager ab	4
Passwort ändern	4
Zeigen Sie StorageGRID Lizenzinformationen an	5
Aktualisieren Sie die StorageGRID-Lizenzinformationen	6
Verwenden Sie die API	7
Verwenden Sie die Grid-Management-API	7
Grid-Management-API-Vorgänge	10
Die Grid Management API-Versionierung	11
Schutz vor standortübergreifenden Anfrageschmieden (CSRF)	13
Verwenden Sie die API, wenn Single Sign-On aktiviert ist	14
Deaktivieren Sie Funktionen mit der API	28

Erste Schritte mit Grid Manager

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Stellen Sie das Browserfenster auf eine empfohlene Breite ein.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Melden Sie sich beim Grid Manager an

Sie greifen auf die Anmeldeseite des Grid Manager zu, indem Sie den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse eines Admin-Knotens in die Adressleiste eines unterstützten Webbrowsers eingeben.

Jedes StorageGRID System umfasst einen primären Admin-Node und eine beliebige Anzahl nicht primärer Admin-Nodes. Sie können sich bei einem beliebigen Admin-Knoten beim Grid-Manager anmelden, um das StorageGRID-System zu verwalten. Einige Wartungsverfahren können jedoch nur über den primären Admin-Node durchgeführt werden.

Stellen Sie eine Verbindung mit der HA-Gruppe her

Wenn Admin-Nodes in einer HA-Gruppe (High Availability, Hochverfügbarkeit) enthalten sind, stellen Sie eine Verbindung über die virtuelle IP-Adresse der HA-Gruppe oder einen vollständig qualifizierten Domännennamen her, der der der virtuellen IP-Adresse zugeordnet ist. Der primäre Admin-Node sollte als primäre Schnittstelle der Gruppe ausgewählt werden, sodass Sie beim Zugriff auf den Grid Manager auf den primären Admin-Knoten zugreifen, wenn der primäre Admin-Node nicht verfügbar ist. Siehe "[Management von Hochverfügbarkeitsgruppen](#)".

Verwenden Sie SSO

Die Anmeldeschritte sind etwas anders, wenn "[Single Sign-On \(SSO\) wurde konfiguriert](#)".

Melden Sie sich beim Grid-Manager beim ersten Admin-Node an

Bevor Sie beginnen

- Sie haben Ihre Anmeldedaten.
- Sie verwenden einen "[Unterstützter Webbrowser](#)".
- Cookies sind in Ihrem Webbrowser aktiviert.
- Sie gehören einer Benutzergruppe an, die über mindestens eine Berechtigung verfügt.
- Sie haben die URL für den Grid-Manager:

`https://FQDN_or_Admin_Node_IP/`

Sie können den vollständig qualifizierten Domännennamen, die IP-Adresse eines Admin-Node oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Nodes verwenden.

Um auf einen anderen Port als den Standardport für HTTPS (443) auf den Grid-Manager zuzugreifen, geben Sie die Portnummer in die URL ein:

`https://FQDN_or_Admin_Node_IP:port/`



SSO ist auf dem eingeschränkten Grid Manager-Port nicht verfügbar. Sie müssen Port 443 verwenden.

Schritte

1. Starten Sie einen unterstützten Webbrowser.
2. Geben Sie in der Adressleiste des Browsers die URL für den Grid Manager ein.
3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten. Siehe "[Verwalten von Sicherheitszertifikaten](#)".
4. Melden Sie sich beim Grid Manager an.

Der angezeigte Anmeldebildschirm hängt davon ab, ob Single Sign-On (SSO) für StorageGRID konfiguriert wurde.

SSO wird nicht verwendet

- a. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein.
- b. Wählen Sie **Anmelden**.

SSO wird verwendet

- Wenn StorageGRID SSO verwendet und Sie zum ersten Mal auf die URL in diesem Browser zugreifen:
 - i. Wählen Sie **Anmelden**. Sie können die 0 im Feld „Konto“ belassen.
 - ii. Geben Sie Ihre Standard-SSO-Anmeldeinformationen auf der SSO-Anmeldeseite Ihrer Organisation ein.

Wenn StorageGRID beispielsweise SSO verwendet und Sie zuvor auf den Grid Manager oder ein Mandantenkonto zugegriffen haben:

- A. Geben Sie **0** (die Konto-ID für den Grid-Manager) ein oder wählen Sie **Grid-Manager** aus, wenn er in der Liste der letzten Konten angezeigt wird.
- B. Wählen Sie **Anmelden**.
- C. Melden Sie sich mit Ihren Standard-SSO-Anmeldedaten auf der SSO-Anmeldeseite Ihres Unternehmens an.

Wenn Sie angemeldet sind, wird die Startseite des Grid-Managers angezeigt, die das Dashboard enthält. Informationen zu den bereitgestellten Informationen finden Sie unter "[Das Dashboard anzeigen und verwalten](#)".

Melden Sie sich bei einem anderen Admin-Node an

Führen Sie die folgenden Schritte aus, um sich bei einem anderen Admin-Node anzumelden.

SSO wird nicht verwendet

Schritte

1. Geben Sie in der Adressleiste des Browsers den vollständig qualifizierten Domännennamen oder die IP-Adresse des anderen Admin-Knotens ein. Geben Sie die Portnummer nach Bedarf an.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein.
3. Wählen Sie **Anmelden**.

SSO wird verwendet

Wenn StorageGRID SSO verwendet und Sie sich bei einem Admin-Knoten angemeldet haben, können Sie auf andere Admin-Knoten zugreifen, ohne sich erneut anmelden zu müssen.

Schritte

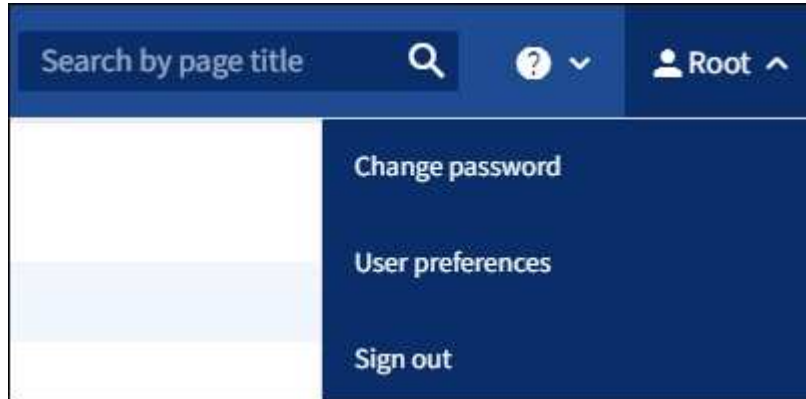
1. Geben Sie den vollständig qualifizierten Domännennamen oder die IP-Adresse des anderen Admin-Knotens in die Adressleiste des Browsers ein.
2. Wenn Ihre SSO-Sitzung abgelaufen ist, geben Sie Ihre Anmeldedaten erneut ein.

Melden Sie sich vom Grid Manager ab

Wenn Sie die Arbeit mit dem Grid-Manager abgeschlossen haben, müssen Sie sich abmelden, um sicherzustellen, dass nicht autorisierte Benutzer keinen Zugriff auf das StorageGRID-System haben. Wenn Sie Ihren Browser schließen, werden Sie möglicherweise aufgrund der Cookie-Einstellungen des Browsers nicht aus dem System abgesendet.

Schritte

1. Wählen Sie oben rechts Ihren Benutzernamen aus.



2. Wählen Sie **Abmelden**.

Option	Beschreibung
SSO wird nicht verwendet	<p>Sie sind vom Admin-Knoten abgemeldet.</p> <p>Die Anmeldeseite des Grid Manager wird angezeigt.</p> <p>Hinweis: Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.</p>
SSO aktiviert	<p>Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugreifen konnten. Die Seite StorageGRID-Anmeldung wird angezeigt. Grid Manager wird standardmäßig im Dropdown-Menü Letzte Konten aufgeführt, und im Feld Konto-ID wird 0 angezeigt.</p> <p>Hinweis: Wenn SSO aktiviert ist und Sie auch beim Tenant Manager angemeldet sind, müssen Sie auch "melden Sie sich vom Mieterkonto ab" Zu "von SSO abmelden" .</p>

Passwort ändern

Wenn Sie ein lokaler Benutzer des Grid Managers sind, können Sie Ihr eigenes Passwort ändern.

Bevor Sie beginnen

Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).

Über diese Aufgabe

Wenn Sie sich bei StorageGRID als föderierter Benutzer anmelden oder Single Sign-On (SSO) aktiviert ist, können Sie Ihr Passwort im Grid-Manager nicht ändern. Stattdessen müssen Sie Ihr Passwort in der externen Identitätsquelle ändern, z. B. Active Directory oder OpenLDAP.

Schritte

1. Wählen Sie in der Kopfzeile des Grid Managers **your Name > Passwort ändern** aus.
2. Geben Sie Ihr aktuelles Kennwort ein.
3. Geben Sie ein neues Passwort ein.

Ihr Kennwort muss mindestens 8 und höchstens 32 Zeichen enthalten. Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.

4. Geben Sie das neue Passwort erneut ein.
5. Wählen Sie **Speichern**.

Zeigen Sie StorageGRID Lizenzinformationen an

Sie können die Lizenzinformationen für Ihr StorageGRID-System anzeigen, z. B. die maximale Storage-Kapazität eines Grids, wann immer sie benötigt werden.

Bevor Sie beginnen

Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).

Über diese Aufgabe

Wenn es ein Problem mit der Softwarelizenz für dieses StorageGRID-System gibt, enthält die Statuskarte für den Systemzustand auf dem Dashboard ein Lizenzstatus-Symbol und einen Link **Lizenz**. Die Zahl gibt die Anzahl der lizenzbezogenen Probleme an.



Schritte

1. Rufen Sie die Lizenzseite auf, indem Sie einen der folgenden Schritte ausführen:
 - Wählen Sie **Wartung > System > Lizenz**.

- Wählen Sie auf der Statuskarte für den Systemzustand im Dashboard das Symbol Lizenzstatus oder den Link **Lizenz** aus.

Dieser Link wird nur angezeigt, wenn ein Problem mit der Lizenz vorliegt.

2. Anzeigen der schreibgeschützten Details für die aktuelle Lizenz:

- StorageGRID System-ID. Hierbei handelt es sich um die eindeutige Identifikationsnummer für diese StorageGRID Installation
- Seriennummer der Lizenz
- Lizenztyp, entweder **Perpetual** oder **Subscription**
- Lizenzierte Storage-Kapazität des Grid
- Unterstützte Storage-Kapazität
- Enddatum der Lizenz. **N/A** erscheint für eine unbefristete Lizenz.
- Enddatum des Supports

Dieses Datum wird aus der aktuellen Lizenzdatei gelesen und ist möglicherweise veraltet, wenn Sie den Supportvertrag nach Erhalt der Lizenzdatei verlängert oder verlängert haben. Informationen zum Aktualisieren dieses Werts finden Sie unter "[Aktualisieren Sie die StorageGRID-Lizenzinformationen](#)". Sie können auch das tatsächliche Enddatum des Vertrags mithilfe von Active IQ anzeigen.

- Inhalt der Lizenztext-Datei

Aktualisieren Sie die StorageGRID-Lizenzinformationen

Sie müssen die Lizenzinformationen für Ihr StorageGRID-System jederzeit aktualisieren, wenn sich die Bedingungen Ihrer Lizenz ändern. Sie müssen beispielsweise die Lizenzinformationen aktualisieren, wenn Sie zusätzliche Speicherkapazität für Ihr Grid erwerben.

Bevor Sie beginnen

- Sie haben eine neue Lizenzdatei für Ihr StorageGRID-System.
- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".
- Sie haben die Provisionierungs-Passphrase.

Schritte

1. Wählen Sie **Wartung > System > Lizenz**.
2. Wählen Sie im Abschnitt Lizenz aktualisieren die Option **Durchsuchen** aus.
3. Suchen und wählen Sie die neue Lizenzdatei (.txt).

Die neue Lizenzdatei wird validiert und angezeigt.

4. Geben Sie die Provisionierungs-Passphrase ein.
5. Wählen Sie **Speichern**.

Verwenden Sie die API

Verwenden Sie die Grid-Management-API

Sie können Systemmanagementaufgaben mithilfe der Grid Management REST-API anstelle der Grid Manager-Benutzeroberfläche ausführen. Möglicherweise möchten Sie beispielsweise die API zur Automatisierung von Vorgängen verwenden oder mehrere Einheiten, wie beispielsweise Benutzer, schneller erstellen.

Allgemeine Ressourcen

Die Grid Management API bietet die folgenden Ressourcen auf oberster Ebene:

- `/grid`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen.
- `/org`: Der Zugriff ist auf Benutzer beschränkt, die zu einer lokalen oder föderierten LDAP-Gruppe für ein Mandantenkonto gehören. Weitere Informationen finden Sie unter "[Verwenden Sie ein Mandantenkonto](#)".
- `/private`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen. Die privaten APIs können ohne Vorankündigung geändert werden. Private StorageGRID-Endpunkte ignorieren auch die API-Version der Anforderung.

API-Anforderungen ausgeben

Die Grid Management API verwendet die Swagger Open-Source-API-Plattform. Swagger bietet eine intuitive Benutzeroberfläche, die es Entwicklern und nicht-Entwicklern ermöglicht, mit der API Echtzeit-Operationen in StorageGRID durchzuführen.

Die Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jeden API-Vorgang.

Bevor Sie beginnen

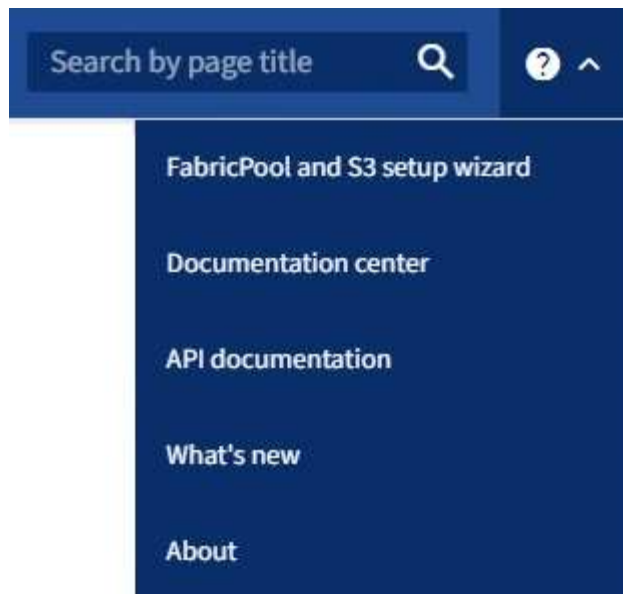
- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".



Alle API-Operationen, die Sie mit der API-Dokumentations-Webseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Schritte

1. Wählen Sie im Grid Manager Header das Hilfesymbol aus und wählen Sie **API documentation**.



2. Um eine Operation mit der privaten API durchzuführen, wählen Sie auf der StorageGRID Management API-Seite **Gehe zur privaten API-Dokumentation** aus.

Die privaten APIs können ohne Vorankündigung geändert werden. Private StorageGRID-Endpunkte ignorieren auch die API-Version der Anforderung.

3. Wählen Sie den gewünschten Vorgang aus.

Wenn Sie einen API-Vorgang erweitern, werden die verfügbaren HTTP-Aktionen angezeigt, z. B. GET, PUT, UPDATE und DELETE.

4. Wählen Sie eine HTTP-Aktion aus, um die Anforderungsdetails anzuzeigen, einschließlich der Endpunkt-URL, einer Liste aller erforderlichen oder optionalen Parameter, einem Beispiel für den Anforderungskörper (falls erforderlich) und den möglichen Antworten.

GET /grid/groups Lists Grid Administrator Groups

Parameters
Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated <input type="text" value="--"/>
limit integer (query)	maximum number of results Default value : 25 <input type="text" value="25"/>
marker string (query)	marker-style pagination offset (value is Group's URN) <input type="text" value="marker - marker-style pagination offset (value"/>
includeMarker boolean (query)	if set, the marker element is also returned <input type="text" value="--"/>
order string (query)	pagination order (desc requires marker) Available values : asc, desc <input type="text" value="--"/>

Responses
Response content type application/json

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers",</pre>

- Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, z. B. eine Gruppe oder eine Benutzer-ID. Dann erhalten Sie diese Werte. Sie müssen möglicherweise zuerst eine andere API-Anfrage stellen, um die Informationen zu erhalten, die Sie benötigen.
- Bestimmen Sie, ob Sie den Text für die Beispielanforderung ändern müssen. In diesem Fall können Sie **Modell** wählen, um die Anforderungen für jedes Feld zu erfahren.
- Wählen Sie **Probieren Sie es aus**.
- Geben Sie alle erforderlichen Parameter ein, oder ändern Sie den Anforderungskörper nach Bedarf.
- Wählen Sie **Ausführen**.
- Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Grid-Management-API-Vorgänge

Die Grid Management API organisiert die verfügbaren Vorgänge in die folgenden Abschnitte.



Diese Liste umfasst nur Vorgänge, die in der öffentlichen API verfügbar sind.

- **Accounts:** Operationen zur Verwaltung von Storage-Mandanten-Konten, einschließlich der Erstellung neuer Konten und dem Abruf der Speichernutzung für ein bestimmtes Konto.
- **Alert-history:** Operationen bei aufgelösten Warnmeldungen.
- **Alert-Receivers:** Operationen auf Alert-Notification-Receiver (E-Mail).
- **Alert-rules:** Operationen auf Warnungsregeln.
- **Alert-Silences:** Operationen bei Alarmstummzuständen.
- **Alerts:** Operationen bei Alerts.
- **Audit:** Operationen zum Auflisten und Aktualisieren der Überwachungskonfiguration.
- **Auth:** Operationen zur Authentifizierung der Benutzersitzung.

Die Grid Management API unterstützt das Authentifizierungsschema für das Inhabertoken. Um sich anzumelden, geben Sie einen Benutzernamen und ein Passwort im JSON-Textkörper der Authentifizierungsanfrage (d.h. `POST /api/v3/authorize`) an. Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss in der Kopfzeile der nachfolgenden API-Anforderungen ("Authorization: Bearer_Token_") angegeben werden. Das Token läuft nach 16 Stunden ab.



Wenn Single Sign-On für das StorageGRID-System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte durchführen. Siehe „Authentifizierung an der API, wenn Single Sign-On aktiviert ist“.

Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter „Schutz gegen standortübergreifende Forgery“.

- **Client-Certificates:** Operationen zur Konfiguration von Client-Zertifikaten, damit StorageGRID sicher über externe Überwachungstools aufgerufen werden kann.
- **Config:** Operationen im Zusammenhang mit der Produktfreigabe und den Versionen der Grid Management API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten Grid Management API auflisten und veraltete Versionen der API deaktivieren.
- **Deactivated-Features:** Operationen zum Anzeigen von Features, die möglicherweise deaktiviert wurden.
- **dns-Server:** Operationen zum Auflisten und Ändern von konfigurierten externen DNS-Servern.
- **Drive-Details:** Betrieb von Laufwerken für bestimmte Storage Appliance-Modelle.
- **Endpunktdomännennamen:** Operationen zum Auflisten und Ändern von S3-Endpunktdomännennamen.
- **Erase-Coding:** Operationen auf Erasure-Coding-Profilen.
- **Erweiterung:** Expansionsbetrieb (Verfahrensebene).
- **Expansion-Nodes:** Erweiterungsvorgänge (Node-Ebene).
- **Erweiterungsstandorte:** Expansionsbetrieb (Standort-Ebene).
- **Grid-Networks:** Operationen zum Auflisten und Ändern der Grid Network List.

- **Grid-passwords:** Operationen zur Grid-Passwortverwaltung.
- **Groups:** Operationen zur Verwaltung lokaler Grid-Administratorgruppen und zum Abrufen föderierter Grid-Administratorgruppen von einem externen LDAP-Server.
- **Identity-source:** Operationen zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm:** Operationen zum Information Lifecycle Management (ILM).
- **In-progress-procedures:** Ruft die derzeit laufenden Wartungsverfahren ab.
- **Lizenz:** Operationen zum Abrufen und Aktualisieren der StorageGRID-Lizenz.
- **Logs:** Operationen zum Sammeln und Herunterladen von Logfiles.V
- **Metrics:** Operationen auf StorageGRID-Metriken einschließlich sofortiger metrischer Abfragen an einem einzelnen Zeitpunkt und Range metrischer Abfragen über einen bestimmten Zeitraum. Die Grid Management API verwendet das Prometheus Systems Monitoring Tool als Backend-Datenquelle. Informationen zum Erstellen von Prometheus-Abfragen finden Sie auf der Prometheus-Website.



Metriken, die in ihren Namen enthalten *private* sind, sind nur für den internen Gebrauch bestimmt. Diese Kennzahlen können sich ohne Ankündigung zwischen StorageGRID Versionen ändern.

- **Node-Details:** Operationen für Node-Details.
- **Node-Health:** Operationen auf dem Node-Status.
- **Node-Storage-State:** Vorgänge im Speicherstatus der Knoten.
- **ntp-Server:** Operationen zum Auflisten oder Aktualisieren externer NTP-Server (Network Time Protocol).
- **Objekte:** Operationen an Objekten und Objektmetadaten.
- **Erholung:** Operationen für die Wiederherstellung.
- **recovery-package:** Vorgänge zum Herunterladen des Wiederherstellungspakets.
- **Regionen:** Operationen zum Anzeigen und Erstellen von Regionen.
- **s3-Object-Lock:** Operationen auf globalen S3 Object Lock Einstellungen.
- **Server-Zertifikat:** Operationen zum Anzeigen und Aktualisieren von Grid Manager-Serverzertifikaten.
- **snmp:** Operationen auf der aktuellen SNMP-Konfiguration.
- **Storage-Wasserzeichen:** Storage-Knoten Wasserzeichen.
- **Traffic-Klassen:** Operationen für Verkehrsklassifizierungsrichtlinien.
- **Nicht vertrauenswürdig-Client-Network:** Operationen auf der nicht vertrauenswürdig Client-Netzwerk-Konfiguration.
- **Benutzer:** Operationen zum Anzeigen und Verwalten von Grid Manager-Benutzern.

Die Grid Management API-Versionierung

Die Grid Management API verwendet Versionierung zur Unterstützung unterbrechungsfreier Upgrades.

Diese Anforderungs-URL gibt beispielsweise die Version 4 der API an.

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

Die Hauptversion der API wird bei Änderungen, die *nicht kompatibel* mit älteren Versionen sind, angestoßen. Die Minor-Version der API wird bei Änderungen, die *kompatibel* mit älteren Versionen gemacht werden, angestoßen. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften.

Das folgende Beispiel zeigt, wie die API-Version basierend auf dem Typ der vorgenommenen Änderungen angestoßen wird.

Typ der Änderung in API	Alte Version	Neue Version
Kompatibel mit älteren Versionen	2,1	2,2
Nicht kompatibel mit älteren Versionen	2,1	3,0

Wenn Sie die StorageGRID-Software zum ersten Mal installieren, wird nur die neueste Version der API aktiviert. Wenn Sie jedoch ein Upgrade auf eine neue Funktionsversion von StorageGRID durchführen, haben Sie weiterhin Zugriff auf die ältere API-Version für mindestens eine StorageGRID-Funktionsversion.



Sie können die unterstützten Versionen konfigurieren. Weitere Informationen finden Sie im Abschnitt **config** der Dokumentation zur Swagger API "[Grid Management API](#)". Sie sollten die Unterstützung für die ältere Version deaktivieren, nachdem Sie alle API-Clients aktualisiert haben, um die neuere Version zu verwenden.

Veraltete Anfragen werden wie folgt als veraltet markiert:

- Der Antwortkopf ist "Deprecated: True"
- Der JSON-Antwortkörper enthält „veraltet“: Wahr
- Eine veraltete Warnung wird nms.log hinzugefügt. Beispiel:

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

Legen Sie fest, welche API-Versionen in der aktuellen Version unterstützt werden

Verwenden Sie die `GET /versions` API-Anforderung, um eine Liste der unterstützten API-Hauptversionen zurückzugeben. Diese Anfrage befindet sich im Abschnitt **config** der Swagger API-Dokumentation.

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

Geben Sie eine API-Version für eine Anforderung an

Sie können die API-Version mit einem PATH-Parameter (`Api-Version: 4`)/`/api/v4` oder einem Header) angeben. Wenn Sie beide Werte angeben, überschreibt der Kopfzeilenwert den Pfadwert.

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

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

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

Sie können mithilfe von CSRF-Tokens die Authentifizierung verbessern, die Cookies verwendet, um Angriffe auf Cross-Site Request Forgery (CSRF) gegen StorageGRID zu schützen. Grid Manager und Tenant Manager aktivieren diese Sicherheitsfunktion automatisch; andere API-Clients können wählen, ob sie aktiviert werden sollen, wenn sie sich anmelden.

Ein Angreifer, der eine Anfrage an eine andere Website auslösen kann (z. B. mit einem HTTP-FORMULARPOST), kann dazu führen, dass bestimmte Anfragen mithilfe der Cookies des angemeldeten Benutzers erstellt werden.

StorageGRID schützt mit CSRF-Tokens vor CSRF-Angriffen. Wenn diese Option aktiviert ist, muss der Inhalt eines bestimmten Cookies mit dem Inhalt eines bestimmten Kopfes oder eines bestimmten POST-Body-Parameters übereinstimmen.

Um die Funktion zu aktivieren, setzen Sie den `csrfToken` Parameter während der Authentifizierung auf `true`. Der Standardwert ist `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"
```

Wenn wahr, wird ein `GridCsrfToken` Cookie mit einem zufälligen Wert für die Anmeldung beim Grid Manager gesetzt, und das `AccountCsrfToken` Cookie wird mit einem zufälligen Wert für die Anmeldung beim Tenant Manager gesetzt.

Wenn das Cookie vorhanden ist, müssen alle Anforderungen, die den Status des Systems (POST, PUT, PATCH, DELETE) ändern können, eine der folgenden Optionen enthalten:

- Die `X-Csrf-Token` Kopfzeile mit dem Wert der Kopfzeile auf den Wert des CSRF-Token-Cookies gesetzt.
- Für Endpunkte, die einen formularkodierte Körper akzeptieren: Einen `csrfToken` formularkodierte Anforderungskörper-Parameter.

Weitere Beispiele und Details finden Sie in der Online-API-Dokumentation.



Anforderungen, die ein CSRF-Token-Cookie gesetzt haben, erzwingen auch den "Content-Type: Application/json"-Header für jede Anforderung, die einen JSON-Request-Body als zusätzlichen Schutz gegen CSRF-Angriffe erwartet.

Verwenden Sie die API, wenn Single Sign-On aktiviert ist

Verwenden Sie die API, wenn Single Sign-On aktiviert ist (Active Directory).

Wenn Sie "[Konfiguration und Aktivierung von Single Sign On \(SSO\)](#)" und Sie Active Directory als SSO-Anbieter verwenden, müssen Sie eine Reihe von API-Anfragen stellen, um ein Authentifizierungstoken zu erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

Melden Sie sich bei der API an, wenn Single Sign-On aktiviert ist

Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitäts-Provider verwenden.

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Passwort für einen föderierten Benutzer, der einer StorageGRID-Benutzergruppe angehört.
- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, können Sie eines der folgenden Beispiele verwenden:

- Der `storagegrid-ssoauth.py` Python-Skript, das sich im Verzeichnis der StorageGRID

Installationsdateien befindet(./rpms für RHEL, ./debs für Ubuntu oder Debian und ./vsphere für VMware).

- Ein Beispielworkflow von Curl-Anforderungen.

Der Curl-Workflow kann sich aushalten, wenn Sie ihn zu langsam ausführen. Möglicherweise wird der Fehler angezeigt: A valid SubjectConfirmation was not found on this Response.



Der Beispiel-Curl-Workflow schützt das Passwort nicht vor der Sicht anderer Benutzer.

Wenn Sie ein Problem mit der URL-Kodierung haben, wird möglicherweise der Fehler angezeigt: Unsupported SAML version.

Schritte

1. Wählen Sie eine der folgenden Methoden aus, um ein Authentifizierungs-Token zu erhalten:
 - Verwenden Sie das `storagegrid-ssoauth.py` Python-Skript. Weiter mit Schritt 2.
 - Verwenden Sie Curl-Anforderungen. Weiter mit Schritt 3.
2. Wenn Sie das Skript verwenden möchten `storagegrid-ssoauth.py`, übergeben Sie das Skript an den Python Interpreter und führen Sie das Skript aus.

Geben Sie bei der entsprechenden Aufforderung Werte für die folgenden Argumente ein:

- Die SSO-Methode. Geben Sie ADFS oder adfs ein.
- Der SSO-Benutzername
- Die Domäne, in der StorageGRID installiert ist
- Die Adresse für StorageGRID
- Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten.

```
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
```

Das StorageGRID-Autorisierungs-Token wird in der Ausgabe bereitgestellt. Sie können das Token jetzt auch für andere Anforderungen verwenden. Dies entspricht der Verwendung der API, wenn SSO nicht verwendet wurde.

3. Wenn Sie Curl-Anforderungen verwenden möchten, gehen Sie wie folgt vor.
 - a. Deklarieren der Variablen, die für die Anmeldung erforderlich sind.

```
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'
```



Um auf die Grid-Management-API zuzugreifen, verwenden Sie 0 als TENANTACCOUNTID.

- b. Um eine signierte Authentifizierungs-URL zu erhalten, stellen Sie eine POST-Anforderung an `/api/v3/authorize-saml`, aus und entfernen Sie die zusätzliche JSON-Codierung aus der Antwort.

Dieses Beispiel zeigt eine POST-Anforderung für eine signierte Authentifizierungs-URL für TENANTACCOUNTID. Die Ergebnisse werden an `python -m json.tool` übergeben, um die JSON-Codierung zu entfernen.

```
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
```

Die Antwort für dieses Beispiel enthält eine signierte URL, die URL-codiert ist, aber nicht die zusätzliche JSON-Kodierungsschicht enthält.

```
{
  "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. Speichern Sie die `SAMLRequest` aus der Antwort für die Verwendung in nachfolgenden Befehlen.

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

- d. Rufen Sie eine vollständige URL ab, die die Client-Anforderungs-ID aus AD FS enthält.

Eine Möglichkeit besteht darin, das Anmeldeformular über die URL der vorherigen Antwort anzufordern.

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

Die Antwort umfasst die Client-Anforderungs-ID:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRT0MwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Speichern Sie die Client-Anforderungs-ID aus der Antwort.

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

f. Senden Sie Ihre Zugangsdaten an die Formularaktion aus der vorherigen Antwort.

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

AD FS gibt eine Umleitung 302 mit zusätzlichen Informationen in den Kopfzeilen zurück.



Wenn Multi-Faktor-Authentifizierung (MFA) für Ihr SSO-System aktiviert ist, enthält der Formularpost auch das zweite Passwort oder andere Anmeldedaten.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRT0MwFIZfhh...UJikvo77sXPw%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. Speichern Sie das MSISAuth Cookie aus der Antwort.

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

- h. Senden Sie eine GET-Anfrage an den angegebenen Ort mit den Cookies aus dem AUTHENTIFIZIERUNGPOST.

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

Die Antwortheader enthalten AD FS-Sitzungsdaten für die spätere Abmeldung, und der Antwortkörper enthält die SAMLResponse in einem verborgenen Formularfeld.

```
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=a3dpbnRlcnMtUHJpbWFyeS1BZG1pci0xNzgmRmFsc2Umcng4NnJDZmFKV
XFXvWw3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDk0Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
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="PHNhbwXwOlJlc3Bvb3N...1scDpsZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

- i. Speichern Sie den SAMLResponse aus dem ausgeblendeten Feld:

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

- j. Erstellen Sie mit dem gespeicherten `SAMLResponse` eine `StorageGRID-/api/saml-response`Anforderung, um ein `StorageGRID-Authentifizierungstoken` zu generieren.

Für `RelayState` verwenden Sie die Mandanten-Konto-ID oder verwenden Sie 0, wenn Sie sich bei der Grid Management API anmelden möchten.

```
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
```

Die Antwort umfasst das Authentifizierungs-Token.

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

- a. Speichern Sie das Authentifizierungstoken in der Antwort als `MYTOKEN`.

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

Sie können jetzt `MYTOKEN` für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet würde.

Melden Sie sich von der API ab, wenn Single Sign-On aktiviert ist

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen zum Abzeichnen der Grid Management API oder der Mandantenmanagement-API ausstellen. Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitäts-Provider verwenden

Über diese Aufgabe

Falls erforderlich, können Sie sich von der StorageGRID-API abmelden, indem Sie sich von der einzelnen Abmeldeseite Ihres Unternehmens abmelden. Alternativ können Sie einzelne Abmeldungen (SLO) von StorageGRID auslösen, was ein gültiges StorageGRID-Überträger-Token erfordert.

Schritte

1. Um eine Anforderung für eine signierte Abmeldung zu generieren, übergeben Sie `Cookie „sso=true“ an die SLO-API:

```
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
```

Es wird eine Abmeldung-URL zurückgegeben:

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

2. Speichern Sie die Abmeldung-URL.

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

3. Senden Sie eine Anfrage an die Logout-URL, um SLO auszulösen und zu StorageGRID zurückzukehren.

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

Die Antwort 302 wird zurückgegeben. Der Umleitungsort gilt nicht für die nur-API-Abmeldung.

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

4. Löschen Sie das StorageGRID-Überträger-Token.

Das Löschen des StorageGRID-Inhabertoken funktioniert auf die gleiche Weise wie ohne SSO. Wenn 'Cookie „sso=true“ nicht angegeben wird, wird der Benutzer ohne Beeinträchtigung des SSO-Status bei StorageGRID abgemeldet.

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

Eine 204 No Content Antwort zeigt an, dass der Benutzer jetzt abgemeldet ist.

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

Verwenden Sie die API, wenn Single Sign-On aktiviert ist (Entra-ID).

Wenn Sie ["Konfiguration und Aktivierung von Single Sign On \(SSO\)"](#) und Sie Entra ID als SSO-Anbieter verwenden, können Sie zwei Beispielskripte verwenden, um ein Authentifizierungstoken zu erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

Sign in , wenn die einmalige Anmeldung bei Entra ID aktiviert ist.

Diese Anweisungen gelten, wenn Sie Entra ID als SSO-Identitätsanbieter verwenden

Bevor Sie beginnen

- Sie kennen die SSO E-Mail-Adresse und das Passwort für einen föderierten Benutzer, der zu einer StorageGRID Benutzergruppe gehört.
- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, können Sie die folgenden Beispielskripte verwenden:

- Das `storagegrid-ssoauth-azure.py` Python-Skript
- Das `storagegrid-ssoauth-azure.js` Skript Node.js

Beide Skripte befinden sich im StorageGRID Installationsverzeichnis(`./rpms` für RHEL, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware).

Informationen zum Schreiben Ihrer eigenen API-Integration mit Entra ID finden Sie im `storagegrid-ssoauth-azure.py` Skript. Das Python-Skript sendet zwei Anfragen direkt an StorageGRID (zuerst, um die SAML-Anforderung abzurufen, und später, um das Autorisierungstoken abzurufen) und ruft außerdem das Node.js-Skript auf, um mit der Entra-ID zu interagieren und die SSO-Vorgänge durchzuführen.

SSO-Vorgänge können mithilfe einer Reihe von API-Anfragen ausgeführt werden, dies ist jedoch nicht ganz einfach. Das Puppeteer Node.js-Modul wird zum Scrapen der Entra ID SSO-Schnittstelle verwendet.

Wenn Sie ein Problem mit der URL-Kodierung haben, wird möglicherweise der Fehler angezeigt:
`Unsupported SAML version.`

Schritte

1. Installieren Sie die erforderlichen Abhängigkeiten:

- a. Installieren Sie Node.js (siehe "<https://nodejs.org/en/download/>").
- b. Installieren Sie die erforderlichen Node.js-Module (Puppenspieler und jsdom):

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

2. Übergeben Sie das Python-Skript an den Python-Interpreter, um das Skript auszuführen.

Das Python-Skript ruft dann das entsprechende Node.js-Skript auf, um die Entra ID SSO-Interaktionen durchzuführen.

3. Geben Sie bei Aufforderung Werte für die folgenden Argumente ein (oder geben Sie diese mit Hilfe von Parametern weiter):

- Die SSO-E-Mail-Adresse, die zur Anmeldung bei Entra ID verwendet wird
- Die Adresse für StorageGRID
- Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten

4. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein und seien Sie bereit, Entra ID auf Anfrage eine MFA-Autorisierung zu erteilen.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*****

Watch for and approve a 2FA authorization request
*****

StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



Das Skript geht davon aus, dass MFA mithilfe von Microsoft Authenticator ausgeführt wird. Möglicherweise müssen Sie das Skript ändern, um andere Formen von MFA zu unterstützen (z. B. die Eingabe eines Codes, der in einer Textnachricht empfangen wird).

Das StorageGRID-Autorisierungstoken wird in der Ausgabe bereitgestellt. Sie können das Token jetzt auch für andere Anforderungen verwenden. Dies entspricht der Verwendung der API, wenn SSO nicht verwendet wurde.

Verwenden Sie die API, wenn Single Sign-On aktiviert ist (PingFederate)

Wenn Sie "[Konfiguration und Aktivierung von Single Sign On \(SSO\)](#)" und Sie PingFederate als SSO-Anbieter verwenden, müssen Sie eine Reihe von API-Anfragen stellen, um ein Authentifizierungstoken zu erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

Melden Sie sich bei der API an, wenn Single Sign-On aktiviert ist

Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitäts-Provider verwenden

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Passwort für einen föderierten Benutzer, der einer StorageGRID-Benutzergruppe angehört.

- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, können Sie eines der folgenden Beispiele verwenden:

- Der `storagegrid-ssoauth.py` Python-Skript, das sich im Verzeichnis der StorageGRID Installationsdateien befindet (`./rpms` für RHEL, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware).
- Ein Beispielworkflow von Curl-Anforderungen.

Der Curl-Workflow kann sich aushalten, wenn Sie ihn zu langsam ausführen. Möglicherweise wird der Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response.`



Der Beispiel-Curl-Workflow schützt das Passwort nicht vor der Sicht anderer Benutzer.

Wenn Sie ein Problem mit der URL-Kodierung haben, wird möglicherweise der Fehler angezeigt: `Unsupported SAML version.`

Schritte

1. Wählen Sie eine der folgenden Methoden aus, um ein Authentifizierungs-Token zu erhalten:
 - Verwenden Sie das `storagegrid-ssoauth.py` Python-Skript. Weiter mit Schritt 2.
 - Verwenden Sie Curl-Anforderungen. Weiter mit Schritt 3.
2. Wenn Sie das Skript verwenden möchten `storagegrid-ssoauth.py`, übergeben Sie das Skript an den Python Interpreter und führen Sie das Skript aus.

Geben Sie bei der entsprechenden Aufforderung Werte für die folgenden Argumente ein:

- Die SSO-Methode. Sie können eine beliebige Variante von "pingfederate" eingeben (PINGFEDERATE, PINGFEDERATE usw.).
- Der SSO-Benutzername
- Die Domäne, in der StorageGRID installiert ist. Dieses Feld wird nicht für PingFederate verwendet. Sie können es leer lassen oder einen beliebigen Wert eingeben.
- Die Adresse für StorageGRID
- Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten.

```
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
```

Das StorageGRID-Autorisierungs-Token wird in der Ausgabe bereitgestellt. Sie können das Token jetzt

auch für andere Anforderungen verwenden. Dies entspricht der Verwendung der API, wenn SSO nicht verwendet wurde.

3. Wenn Sie Curl-Anforderungen verwenden möchten, gehen Sie wie folgt vor.

a. Deklarieren der Variablen, die für die Anmeldung erforderlich sind.

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



Um auf die Grid-Management-API zuzugreifen, verwenden Sie 0 als TENANTACCOUNTID.

b. Um eine signierte Authentifizierungs-URL zu erhalten, stellen Sie eine POST-Anforderung an `/api/v3/authorize-saml`, aus und entfernen Sie die zusätzliche JSON-Codierung aus der Antwort.

Dieses Beispiel zeigt eine POST-Anforderung für eine signierte Authentifizierungs-URL für TENANTACCOUNTID. Die Ergebnisse werden an Python `-m json.tool` übergeben, um die JSON-Codierung zu entfernen.

```
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
```

Die Antwort für dieses Beispiel enthält eine signierte URL, die URL-codiert ist, aber nicht die zusätzliche JSON-Kodierungsschicht enthält.

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

c. Speichern Sie die `SAMLRequest` aus der Antwort für die Verwendung in nachfolgenden Befehlen.

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

d. Exportieren Sie die Antwort und das Cookie, und wiederholen Sie die Antwort:

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

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

e. Exportieren Sie den Wert „pf.adapterId“, und geben Sie die Antwort ein:

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

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

f. Exportieren Sie den 'href'-Wert (entfernen Sie den hinteren Schrägstrich /), und wiederholen Sie die Antwort:

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

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

g. Den Wert „Aktion“ exportieren:

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

h. Senden von Cookies zusammen mit den Zugangsdaten:

```
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. Speichern Sie den SAMLResponse aus dem ausgeblendeten Feld:

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

j. Erstellen Sie mit dem gespeicherten SAMLResponse eine StorageGRID-/api/saml-responseAnforderung, um ein StorageGRID-Authentifizierungstoken zu generieren.

Für RelayState verwenden Sie die Mandanten-Konto-ID oder verwenden Sie 0, wenn Sie sich bei

der Grid Management API anmelden möchten.

```
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
```

Die Antwort umfasst das Authentifizierungs-Token.

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

a. Speichern Sie das Authentifizierungstoken in der Antwort als MYTOKEN.

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

Sie können jetzt MYTOKEN für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet würde.

Melden Sie sich von der API ab, wenn Single Sign-On aktiviert ist

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen zum Abzeichnen der Grid Management API oder der Mandantenmanagement-API ausstellen. Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitäts-Provider verwenden

Über diese Aufgabe

Falls erforderlich, können Sie sich von der StorageGRID-API abmelden, indem Sie sich von der einzelnen Abmeldeseite Ihres Unternehmens abmelden. Alternativ können Sie einzelne Abmeldungen (SLO) von StorageGRID auslösen, was ein gültiges StorageGRID-Überträger-Token erfordert.

Schritte

1. Um eine Anforderung für eine signierte Abmeldung zu generieren, übergeben Sie `Cookie „sso=true“` an die SLO-API:

```
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
```

Es wird eine Abmeldung-URL zurückgegeben:

```
{
  "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. Speichern Sie die Abmeldung-URL.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Senden Sie eine Anfrage an die Logout-URL, um SLO auszulösen und zu StorageGRID zurückzukehren.

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

Die Antwort 302 wird zurückgegeben. Der Umleitungsort gilt nicht für die nur-API-Abmeldung.

```
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. Löschen Sie das StorageGRID-Überträger-Token.

Das Löschen des StorageGRID-Inhabertoken funktioniert auf die gleiche Weise wie ohne SSO. Wenn 'Cookie „sso=true“ nicht angegeben wird, wird der Benutzer ohne Beeinträchtigung des SSO-Status bei StorageGRID abgemeldet.

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

Eine 204 No Content Antwort zeigt an, dass der Benutzer jetzt abgemeldet ist.

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

Deaktivieren Sie Funktionen mit der API

Mithilfe der Grid Management API können Sie bestimmte Funktionen im StorageGRID-System komplett deaktivieren. Wenn ein Feature deaktiviert ist, kann niemand Berechtigungen zum Ausführen der Aufgaben zugewiesen werden, die mit diesem Feature verbunden sind.

Über diese Aufgabe

Mit dem deaktivierten Features-System können Sie den Zugriff auf bestimmte Funktionen im StorageGRID-System verhindern. Die Deaktivierung einer Funktion ist der einzige Weg, um zu verhindern, dass Root-Benutzer oder Benutzer, die zu Admin-Gruppen mit **Root Access**-Berechtigung gehören, diese Funktion verwenden können.

Um zu verstehen, wie diese Funktionalität nützlich sein kann, gehen Sie folgendermaßen vor:

Unternehmen A ist ein Service Provider, der durch die Erstellung von Mandantenkonten die Storage-Kapazität ihres StorageGRID Systems least. Um die Sicherheit der Objekte ihrer Eigentümer zu schützen, möchte Unternehmen A sicherstellen, dass die eigenen Mitarbeiter nach der Bereitstellung des Kontos niemals auf ein Mandantenkonto zugreifen können.

*Unternehmen A kann dieses Ziel mithilfe des Systems Funktionen deaktivieren in der Grid Management API erreichen. Durch die vollständige Deaktivierung der Funktion **Change Tenant root password** im Grid Manager (sowohl die Benutzeroberfläche als auch die API) stellt Unternehmen A sicher, dass Admin-Benutzer - einschließlich des Root-Benutzers und Benutzer, die zu Gruppen mit der Berechtigung **Root-Zugriff** gehören - das Passwort für den Root-Benutzer eines Mandantenkontos nicht ändern können.*

Schritte

1. Rufen Sie die Swagger-Dokumentation für die Grid Management API auf. Siehe "[Verwenden Sie die Grid-Management-API](#)".
2. Suchen Sie den Endpunkt zum Deaktivieren von Funktionen.
3. Um eine Funktion, wie z.B. das Root-Passwort des Mandanten ändern, zu deaktivieren, senden Sie einen Text wie folgt an die API:

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

Nach Abschluss der Anforderung ist die Funktion Root-Passwort ändern deaktiviert. Die Verwaltungsberechtigung **Change Tenant root password** wird nicht mehr in der Benutzeroberfläche angezeigt, und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, schlägt mit "403 Verboten" fehl.

Deaktivieren Funktionen erneut aktivieren

Standardmäßig können Sie mit der Grid Management API eine deaktivierte Funktion reaktivieren. Wenn Sie jedoch verhindern möchten, dass deaktivierte Funktionen jemals wieder aktiviert werden, können Sie die **activateFeatures**-Funktion selbst deaktivieren.



Die Funktion **activateFeatures** kann nicht reaktiviert werden. Wenn Sie sich entscheiden, diese Funktion zu deaktivieren, beachten Sie, dass Sie die Möglichkeit verlieren, alle anderen deaktivierten Funktionen dauerhaft zu reaktivieren. Sie müssen sich an den technischen Support wenden, um verlorene Funktionen wiederherzustellen.

Schritte

1. Rufen Sie die Swagger-Dokumentation für die Grid Management API auf.
2. Suchen Sie den Endpunkt zum Deaktivieren von Funktionen.
3. Um alle Funktionen erneut zu aktivieren, senden Sie einen Text wie folgt an die API:

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

Wenn diese Anfrage abgeschlossen ist, werden alle Funktionen, einschließlich der Funktion Root-Passwort ändern, reaktiviert. Die Berechtigung zur Verwaltung von Stammpasswort* des Mandanten wird jetzt in der Benutzeroberfläche angezeigt, und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, wird erfolgreich sein, vorausgesetzt der Benutzer hat die Berechtigung * Root Access* oder **Change Tenant Root password** Management.



Das vorherige Beispiel führt dazu, dass *all* deaktivierte Funktionen reaktiviert werden. Wenn andere Features deaktiviert wurden, die deaktiviert bleiben sollen, müssen Sie diese explizit in der PUT-Anforderung angeben. Wenn Sie beispielsweise die Funktion zum Ändern des Stammkennworts für den Mandanten erneut aktivieren und die Berechtigung zum Verwalten von storageAdmin deaktivieren möchten, senden Sie diese PUT-Anforderung:

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.