Erste Schritte mit Grid Manager

StorageGRID software

NetApp
October 21, 2025

Inhalt

Erste Schritte mit Grid Manager

Anforderungen an den Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Mindestens unterstützte Version
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimum	1280

Sign in

Sie greifen auf die Anmeldeseite des Grid Managers zu, indem Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse eines Admin-Knotens in die Adressleiste eines unterstützten Webbrowsers eingeben.

Jedes StorageGRID -System umfasst einen primären Admin-Knoten und eine beliebige Anzahl nicht-primärer Admin-Knoten. Sie können sich auf jedem Admin-Knoten beim Grid Manager anmelden, um das StorageGRID -System zu verwalten. Einige Wartungsvorgänge können jedoch nur vom primären Admin-Knoten aus durchgeführt werden.

Mit HA-Gruppe verbinden

Wenn Admin-Knoten in einer Hochverfügbarkeitsgruppe (HA) enthalten sind, stellen Sie die Verbindung über die virtuelle IP-Adresse der HA-Gruppe oder einen vollqualifizierten Domänennamen her, der der virtuellen IP-Adresse zugeordnet ist. Der primäre Admin-Knoten sollte als primäre Schnittstelle der Gruppe ausgewählt werden, sodass Sie beim Zugriff auf den Grid Manager über den primären Admin-Knoten darauf zugreifen, es sei denn, der primäre Admin-Knoten ist nicht verfügbar. Sehen "Verwalten von Hochverfügbarkeitsgruppen" .

Verwenden von SSO

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

Sign in

Bevor Sie beginnen

- Sie haben Ihre Anmeldedaten.
- Sie verwenden eine"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 vollqualifizierten Domänennamen, die IP-Adresse eines Admin-Knotens oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Knoten verwenden.

  Um auf den Grid Manager über einen anderen Port als den Standardport für HTTPS (443) zuzugreifen, fügen 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 eine Sicherheitswarnung angezeigt wird, installieren Sie das Zertifikat mithilfe des Installationsassistenten des Browsers. Sehen "Sicherheitszertifikate verwalten" .
4. Sign in .

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

Kein SSO verwenden

a. Geben Sie Ihren Benutzernamen und Ihr Passwort für den Grid Manager ein.

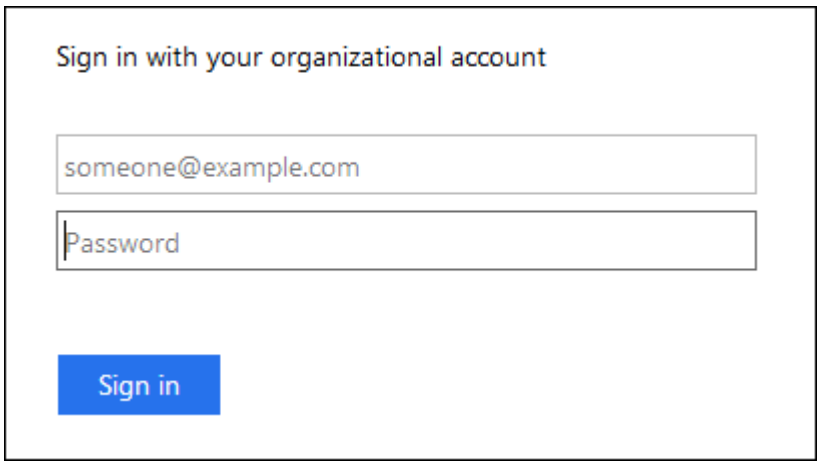
b. Wählen Sie **Anmelden**.

Verwenden von SSO

- Wenn StorageGRID SSO verwendet und Sie die URL zum ersten Mal in diesem Browser aufrufen:

  i. Wählen Sie * Sign in*. Die 0 können Sie im Feld Konto stehen lassen.

  ii. Geben Sie Ihre Standard-SSO-Anmeldeinformationen auf der SSO-Anmeldeseite Ihrer Organisation ein. Beispiel:



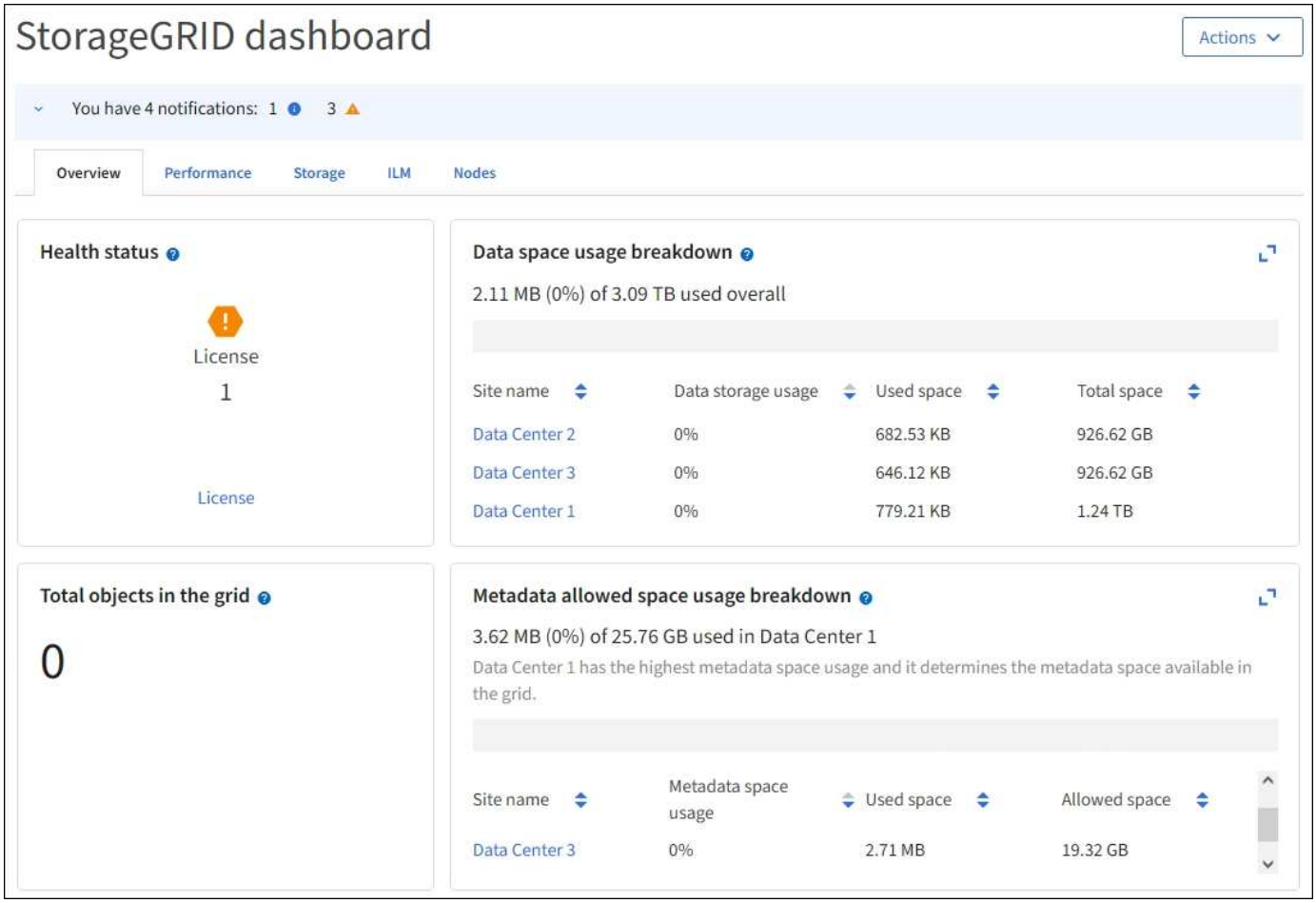
- Wenn StorageGRID SSO verwendet und Sie zuvor auf den Grid Manager oder ein Mandantenkonto zugegriffen haben:

i. Geben Sie **0** ein (die Konto-ID für den Grid Manager) oder wählen Sie **Grid Manager** aus, wenn dieser in der Liste der letzten Konten angezeigt wird.

ii. Wählen Sie * Sign in*.

iii. Sign in mit Ihren Standard-SSO-Anmeldeinformationen auf der SSO-Anmeldeseite Ihrer Organisation an.

Wenn Sie angemeldet sind, wird die Startseite des Grid Managers angezeigt, die das Dashboard enthält. Um zu erfahren, welche Informationen bereitgestellt werden, siehe"Anzeigen und Verwalten des Dashboards" .



Melden Sie sich bei einem anderen Admin-Knoten an

Befolgen Sie diese Schritte, um sich bei einem anderen Admin-Knoten anzumelden.

Kein SSO verwenden

Schritte

1. Geben Sie in der Adressleiste des Browsers den vollqualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens ein. Geben Sie bei Bedarf die Portnummer an.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort für den Grid Manager ein.
3. Wählen Sie **Anmelden**.

Verwenden von SSO

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

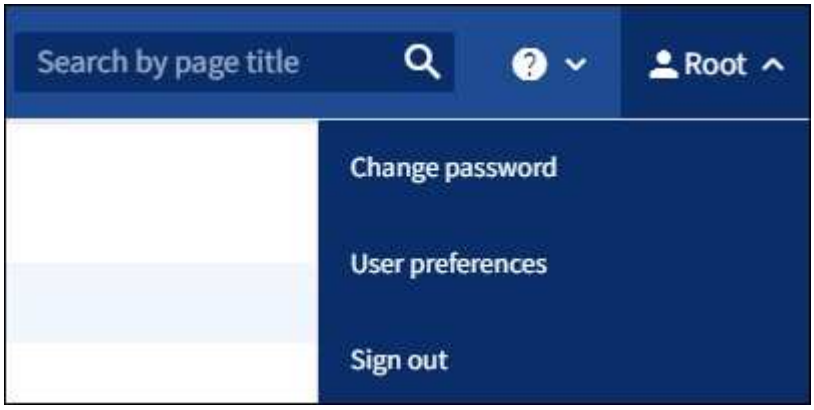
1. Geben Sie den vollqualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens in die Adressleiste des Browsers ein.
2. Wenn Ihre SSO-Sitzung abgelaufen ist, geben Sie Ihre Anmeldeinformationen erneut ein.

Vom Grid Manager abmelden

Wenn Sie mit der Arbeit mit dem Grid Manager fertig sind, müssen Sie sich abmelden, um sicherzustellen, dass nicht autorisierte Benutzer nicht auf das StorageGRID -System zugreifen können. Wenn Sie Ihren Browser schließen, werden Sie je nach den Cookie-Einstellungen Ihres Browsers möglicherweise nicht vom System abgemeldet.

Schritte

1. Wählen Sie oben rechts Ihren Benutzernamen aus.



2. Wählen Sie **Abmelden**.

Option	Beschreibung
SSO wird nicht verwendet	Sie sind vom Admin-Knoten abgemeldet. Die Anmeldeseite des Grid Managers wird angezeigt. **Hinweis:** Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.
SSO aktiviert	Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugegriffen haben. Die StorageGRID -Anmeldeseite wird angezeigt. **Grid Manager** wird im Dropdown-Menü **Letzte Konten** als Standard aufgeführt und das Feld **Konto-ID** zeigt 0 an. **Hinweis:** Wenn SSO aktiviert ist und Sie auch beim Tenant Manager angemeldet sind, müssen Sie auch"Melden Sie sich vom Mieterkonto ab" Zu"Abmelden von SSO" .

Ändern Sie Ihr Passwort

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

Bevor Sie beginnen

Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .

Informationen zu diesem Vorgang

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

Schritte

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

   Ihr Passwort muss mindestens 8 und darf nicht mehr als 32 Zeichen enthalten. Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

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

StorageGRID Lizenzinformationen anzeigen

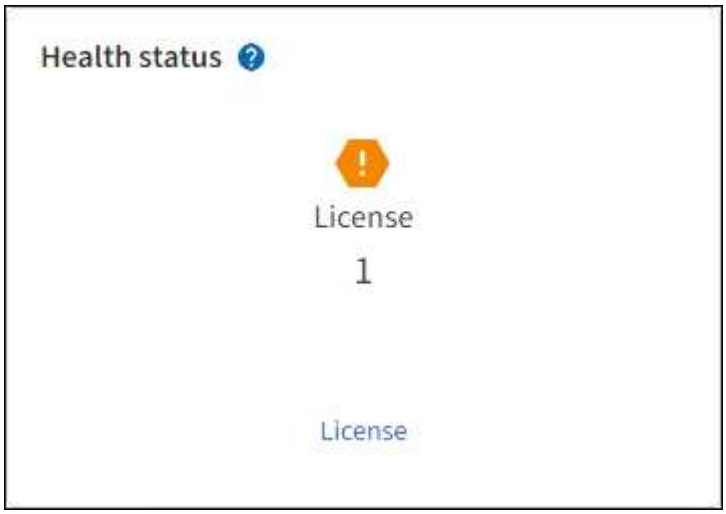
Sie können die Lizenzinformationen für Ihr StorageGRID -System, beispielsweise die maximale Speicherkapazität Ihres Grids, bei Bedarf einsehen.

Bevor Sie beginnen

Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .

Informationen zu diesem Vorgang

Wenn ein Problem mit der Softwarelizenz für dieses StorageGRID -System vorliegt, enthält die Integritätsstatuskarte auf dem Dashboard ein Lizenzstatussymbol und einen **Lizenz**-Link. Die Zahl gibt die Anzahl der lizenzbezogenen Probleme an.



Schritte

1. Greifen Sie auf die Lizenzseite zu, indem Sie einen der folgenden Schritte ausführen:
   - Wählen Sie **WARTUNG** > **System** > **Lizenz**.
   - Wählen Sie auf der Gesundheitsstatuskarte im Dashboard das Lizenzstatussymbol oder den Link **Lizenz** aus.

     Dieser Link wird nur angezeigt, wenn ein Problem mit der Lizenz vorliegt.
2. Zeigen Sie die schreibgeschützten Details für die aktuelle Lizenz an:
   - StorageGRID -System-ID, die eindeutige Identifikationsnummer für diese StorageGRID Installation
   - Lizenzseriennummer
   - Lizenztyp, entweder **Dauerlizenz** oder **Abonnement**
   - Lizenzierte Speicherkapazität des Netzes
   - Unterstützte Speicherkapazität
   - Enddatum der Lizenz. **N/A** wird für eine unbefristete Lizenz angezeigt.
   - Support-Enddatum

     Dieses Datum wird aus der aktuellen Lizenzdatei gelesen und kann veraltet sein, wenn Sie den Support-Servicevertrag nach Erhalt der Lizenzdatei verlängert oder erneuert haben. Informationen zum Aktualisieren dieses Werts finden Sie unter"Aktualisieren Sie die StorageGRID -Lizenzinformationen" . Sie können das tatsächliche Vertragsende auch mit Active IQ einsehen.
   - Inhalt der Lizenztextdatei

Aktualisieren Sie die StorageGRID -Lizenzinformationen

Sie müssen die Lizenzinformationen für Ihr StorageGRID -System jedes Mal

aktualisieren, wenn sich die Bedingungen Ihrer Lizenz ändern. Beispielsweise müssen Sie die Lizenzinformationen aktualisieren, wenn Sie zusätzliche Speicherkapazität für Ihr Grid erwerben.

Bevor Sie beginnen

- Sie haben eine neue Lizenzdatei, die Sie auf Ihr StorageGRID -System anwenden können.
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die Bereitstellungspassphrase.

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 Bereitstellungspassphrase ein.
5. Wählen Sie **Speichern**.

Verwenden der API

Verwenden Sie die Grid Management API

Sie können Systemverwaltungsaufgaben mithilfe der Grid Management REST API anstelle der Grid Manager-Benutzeroberfläche ausführen. Beispielsweise möchten Sie die API möglicherweise verwenden, um Vorgänge zu automatisieren oder mehrere Entitäten, z. B. Benutzer, schneller zu erstellen.

Top-Level-Ressourcen

Die Grid Management API bietet die folgenden Ressourcen der obersten Ebene:

- `/grid`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen.
- `/org`: Der Zugriff ist auf Benutzer beschränkt, die einer lokalen oder föderierten LDAP-Gruppe für ein Mandantenkonto angehören. Weitere Informationen finden Sie unter "Verwenden eines Mandantenkontos" .
- `/private`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen. Die privaten APIs können ohne vorherige Ankündigung geändert werden. Private StorageGRID Endpunkte ignorieren auch die API-Version der Anfrage.

API-Anfragen stellen

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

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

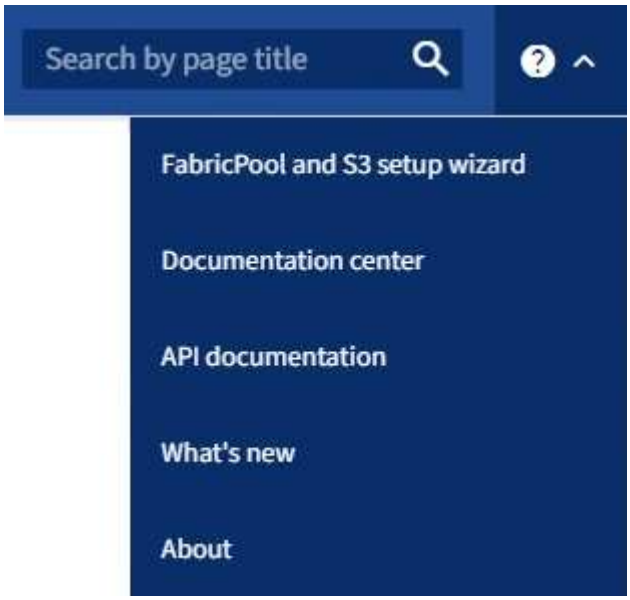
Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .

> Alle API-Operationen, die Sie über die API-Dokumentationswebseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Sie nicht versehentlich Konfigurationsdaten oder andere Daten erstellen, aktualisieren oder löschen.

Schritte

1. Wählen Sie in der Kopfzeile des Grid Managers das Hilfesymbol und dann **API-Dokumentation** aus.



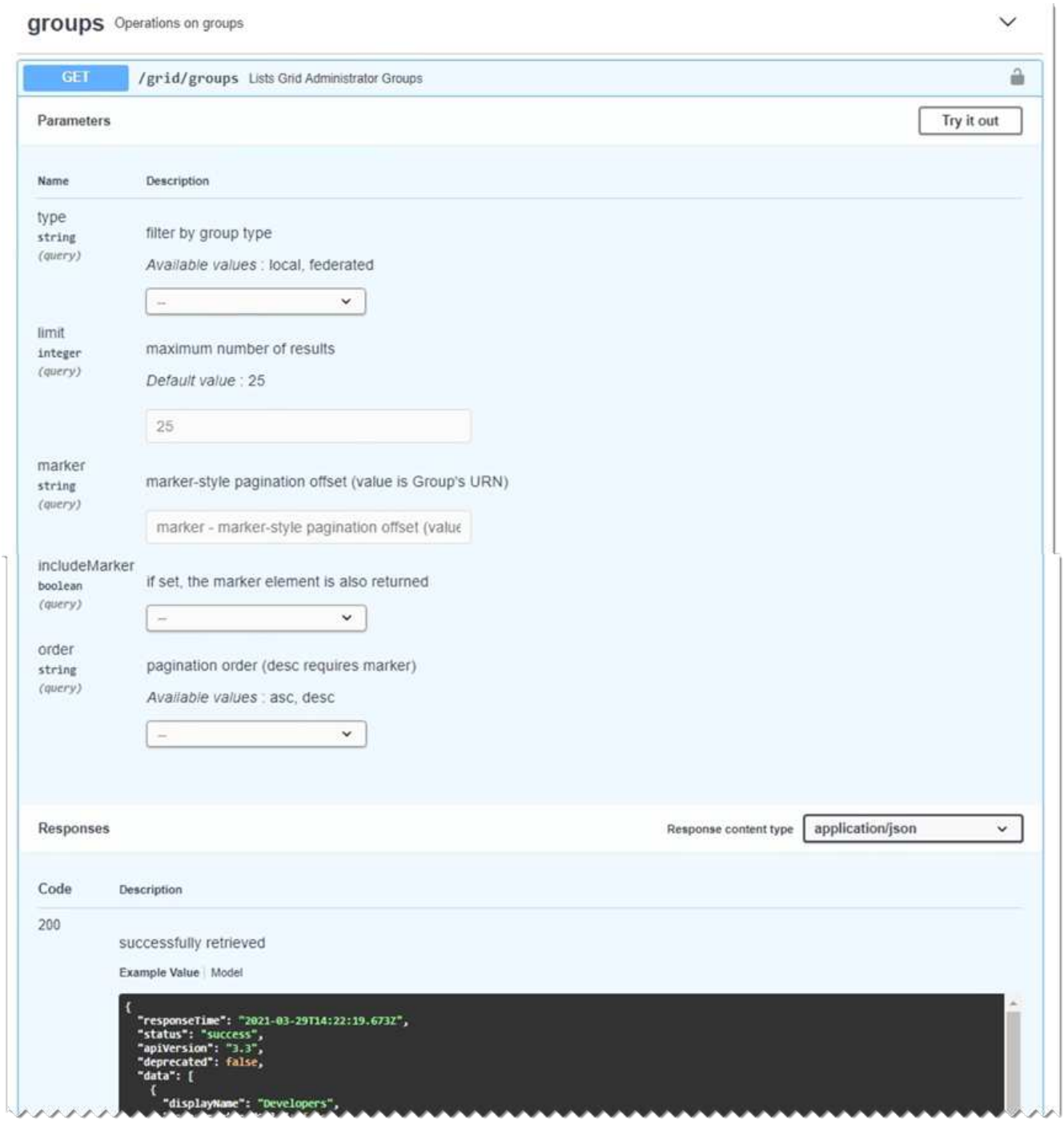
2. Um einen Vorgang mit der privaten API durchzuführen, wählen Sie auf der StorageGRID Management-API-Seite **Zur privaten API-Dokumentation gehen**.

   Die privaten APIs können ohne vorherige Ankündigung geändert werden. Private StorageGRID Endpunkte ignorieren auch die API-Version der Anfrage.

3. Wählen Sie die gewünschte Operation aus.

   Wenn Sie eine API-Operation erweitern, können Sie die verfügbaren HTTP-Aktionen wie GET, PUT, UPDATE und DELETE sehen.

4. Wählen Sie eine HTTP-Aktion aus, um die Anforderungsdetails anzuzeigen, einschließlich der Endpunkt-URL, einer Liste aller erforderlichen oder optionalen Parameter, eines Beispiels des Anforderungstexts (falls erforderlich) und der möglichen Antworten.



5. Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, beispielsweise eine Gruppen- oder Benutzer-ID. Besorgen Sie sich dann diese Werte. Möglicherweise müssen Sie zuerst eine andere API-Anfrage stellen, um die benötigten Informationen zu erhalten.
6. Stellen Sie fest, ob Sie den Beispielanforderungstext ändern müssen. Wenn ja, können Sie **Modell** auswählen, um die Anforderungen für jedes Feld zu erfahren.
7. Wählen Sie **Ausprobieren**.
8. Geben Sie alle erforderlichen Parameter an oder ändern Sie den Anforderungstext nach Bedarf.
9. Wählen Sie **Ausführen**.
10. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Grid Management-API-Operationen

Die Grid Management API organisiert die verfügbaren Vorgänge in den folgenden Abschnitten.

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

- **Konten**: Vorgänge zum Verwalten von Speichermandantenkonten, einschließlich Erstellen neuer Konten und Abrufen der Speichernutzung für ein bestimmtes Konto.
- **Alarmverlauf**: Vorgänge für gelöste Alarme.
- **Alarmempfänger**: Vorgänge für Empfänger von Alarmbenachrichtigungen (E-Mail).
- **alert-rules**: Vorgänge für Alarmregeln.
- **alert-silences**: Vorgänge zum Stummschalten von Alarmen.
- **Alarme**: Vorgänge für Alarme.
- **Audit**: Vorgänge zum Auflisten und Aktualisieren der Audit-Konfiguration.
- **auth**: Vorgänge zum Durchführen der Benutzersitzungsauthentifizierung.

  Die Grid Management API unterstützt das Bearer Token Authentication Scheme. Um sich anzumelden, geben Sie im JSON-Text der Authentifizierungsanfrage einen Benutzernamen und ein Kennwort ein (das heißt, `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss im Header nachfolgender API-Anfragen bereitgestellt werden („Authorization: Bearer *token*“). Das Token verfällt nach 16 Stunden.

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

  Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter „Schutz vor Cross-Site Request Forgery“.

- **Client-Zertifikate**: Vorgänge zum Konfigurieren von Client-Zertifikaten, sodass mithilfe externer Überwachungstools sicher auf StorageGRID zugegriffen werden kann.
- **config**: Vorgänge im Zusammenhang mit der Produktversion und den Versionen der Grid Management API. Sie können die Produktversion und die Hauptversionen der Grid Management-API auflisten, die von dieser Version unterstützt werden, und Sie können veraltete Versionen der API deaktivieren.
- **deaktivierte Funktionen**: Vorgänge zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **DNS-Server**: Vorgänge zum Auflisten und Ändern konfigurierter externer DNS-Server.
- **Laufwerksdetails**: Vorgänge auf Laufwerken für bestimmte Speichergerätemodelle.
- **Endpunktdomänennamen**: Vorgänge zum Auflisten und Ändern von S3-Endpunktdomänennamen.
- **Erasure-Coding**: Operationen an Erasure-Coding-Profilen.
- **Erweiterung**: Operationen zur Erweiterung (Prozedurebene).
- **Expansion-Nodes**: Operationen auf Expansionsebene (Knotenebene).
- **expansion-sites**: Operationen zur Erweiterung (Site-Ebene).
- **grid-networks**: Vorgänge zum Auflisten und Ändern der Grid-Netzwerkliste.

- **grid-passwords**: Vorgänge für die Grid-Passwortverwaltung.
- **Gruppen**: Vorgänge zum Verwalten lokaler Grid-Administratorgruppen und zum Abrufen föderierter Grid-Administratorgruppen von einem externen LDAP-Server.
- **Identitätsquelle**: Vorgänge zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm**: Vorgänge im Bereich Information Lifecycle Management (ILM).
- **in-progress-procedures**: Ruft die Wartungsvorgänge ab, die derzeit ausgeführt werden.
- **Lizenz**: Vorgänge zum Abrufen und Aktualisieren der StorageGRID -Lizenz.
- **logs**: Vorgänge zum Sammeln und Herunterladen von Protokolldateien.v
- **Metriken**: Vorgänge an StorageGRID -Metriken, einschließlich sofortiger Metrikabfragen zu einem bestimmten Zeitpunkt und Bereichsmetrikabfragen über einen bestimmten Zeitraum. Die Grid Management API verwendet das Systemüberwachungstool Prometheus als Backend-Datenquelle. Informationen zum Erstellen von Prometheus-Abfragen finden Sie auf der Prometheus-Website.

> Metriken, die Folgendes umfassen:`private` in ihren Namen sind nur für den internen Gebrauch bestimmt. Diese Kennzahlen können sich zwischen den StorageGRID Versionen ohne Vorankündigung ändern.

- **Knotendetails**: Operationen an Knotendetails.
- **Knotengesundheit**: Vorgänge zum Knotengesundheitsstatus.
- **node-storage-state**: Vorgänge zum Knotenspeicherstatus.
- **ntp-servers**: Vorgänge zum Auflisten oder Aktualisieren externer Network Time Protocol (NTP)-Server.
- **Objekte**: Operationen an Objekten und Objektmetadaten.
- **Wiederherstellung**: Vorgänge für das Wiederherstellungsverfahren.
- **recovery-package**: Vorgänge zum Herunterladen des Wiederherstellungspakets.
- **Regionen**: Vorgänge zum Anzeigen und Erstellen von Regionen.
- **s3-object-lock**: Vorgänge an globalen S3-Objektsperreinstellungen.
- **Serverzertifikat**: Vorgänge zum Anzeigen und Aktualisieren von Grid Manager-Serverzertifikaten.
- **snmp**: Vorgänge an der aktuellen SNMP-Konfiguration.
- **storage-watermarks**: Wasserzeichen des Speicherknotens.
- **Verkehrsklassen**: Vorgänge für Verkehrsklassifizierungsrichtlinien.
- **untrusted-client-network**: Vorgänge an der nicht vertrauenswürdigen Client-Netzwerkkonfiguration.
- **Benutzer**: Vorgänge zum Anzeigen und Verwalten von Grid Manager-Benutzern.

Grid Management API-Versionierung

Die Grid Management API verwendet Versionierung, um unterbrechungsfreie Upgrades zu unterstützen.

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

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

Die Hauptversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen *nicht kompatibel* sind. Die Nebenversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen *kompatibel* sind. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften.

Das folgende Beispiel veranschaulicht, wie die API-Version je nach Art der vorgenommenen Änderungen erhöht wird.

Art der Änderung an der 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, ist nur die neueste Version der API aktiviert. Wenn Sie jedoch auf eine neue Funktionsversion von StorageGRID aktualisieren, 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 Swagger-API-Dokumentation."Grid-Management-API" für weitere Informationen. 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 auf folgende Weise als veraltet gekennzeichnet:

- Der Antwortheader lautet „Deprecated: true“
- Der JSON-Antworttext enthält „deprecated“: true
- Zu nms.log wird eine veraltete Warnung hinzugefügt. Beispiel:

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

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

Verwenden Sie die `GET /versions` API-Anforderung zum Zurückgeben einer Liste der unterstützten API-Hauptversionen. 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
  ]
}
```

Angeben einer API-Version für eine Anfrage

Sie können die API-Version mithilfe eines Pfadparameters angeben(`/api/v4`) oder eine Kopfzeile(`Api-Version: 4`). Wenn Sie beide Werte angeben, überschreibt der Header-Wert den Pfadwert.

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

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

Schutz vor Cross-Site Request Forgery (CSRF)

Sie können zum Schutz vor Cross-Site Request Forgery (CSRF)-Angriffen auf StorageGRID beitragen, indem Sie CSRF-Token verwenden, um die Authentifizierung mithilfe von Cookies zu verbessern. Der Grid Manager und der Tenant Manager aktivieren diese Sicherheitsfunktion automatisch. Andere API-Clients können bei der Anmeldung auswählen, ob sie diese aktivieren möchten.

Ein Angreifer, der eine Anfrage an eine andere Site auslösen kann (z. B. mit einem HTTP-Formular-POST), kann dafür sorgen, dass bestimmte Anfragen unter Verwendung der Cookies des angemeldeten Benutzers gestellt werden.

StorageGRID schützt durch die Verwendung von CSRF-Token vor CSRF-Angriffen. Wenn diese Option aktiviert ist, muss der Inhalt eines bestimmten Cookies mit dem Inhalt eines bestimmten Headers oder eines bestimmten POST-Body-Parameters übereinstimmen.

Um die Funktion zu aktivieren, legen Sie die `csrfToken` Parameter auf `true` während der Authentifizierung. Die Standardeinstellung 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 dies zutrifft, `GridCsrfToken` Cookie wird mit einem zufälligen Wert für Anmeldungen am Grid Manager gesetzt, und die `AccountCsrfToken` Für die Anmeldung beim Tenant Manager wird ein Cookie mit einem zufälligen Wert gesetzt.

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

- Der `X-Csrf-Token` Header, wobei der Wert des Headers auf den Wert des CSRF-Token-Cookies gesetzt ist.
- Für Endpunkte, die einen formkodierten Textkörper akzeptieren: A `csrfToken` formcodierter Anforderungstextparameter.

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

> Anfragen, für die ein CSRF-Token-Cookie gesetzt ist, erzwingen außerdem den Header „Content-Type: application/json“ für alle Anfragen, die einen JSON-Anforderungstext erwarten, als zusätzlichen Schutz vor CSRF-Angriffen.

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

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

Wenn Sie"Single Sign-On (SSO) konfiguriert und aktiviert" 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.

Sign in , wenn Single Sign-On aktiviert ist

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

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Kennwort für einen Verbundbenutzer, der zu einer StorageGRID -Benutzergruppe gehört.
- Wenn Sie auf die Tenant Management API zugreifen möchten, kennen Sie die Mandantenkonto-ID.

Informationen zu diesem Vorgang

Um ein Authentifizierungstoken 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 Red Hat Enterprise Linux, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware).

- Ein Beispiel-Workflow für Curl-Anfragen.

  Wenn Sie den Curl-Workflow zu langsam ausführen, kann es zu einer Zeitüberschreitung kommen. Möglicherweise wird der folgende Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response`.

  > Der beispielhafte Curl-Workflow schützt das Kennwort nicht davor, von anderen Benutzern eingesehen zu werden.

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

Schritte

1. Wählen Sie eine der folgenden Methoden aus, um ein Authentifizierungstoken zu erhalten:
   - Verwenden Sie die `storagegrid-ssoauth.py` Python-Skript. Fahren Sie mit Schritt 2 fort.
   - Verwenden Sie Curl-Anfragen. Fahren Sie mit Schritt 3 fort.
2. Wenn Sie die `storagegrid-ssoauth.py` Skript, übergeben Sie das Skript an den Python-Interpreter und führen Sie das Skript aus.

   Geben Sie bei entsprechender 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 Mandantenverwaltungs-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 Autorisierungstoken wird in der Ausgabe bereitgestellt. Sie können das Token jetzt für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet würde.

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

   a. Deklarieren Sie die für die Anmeldung erforderlichen Variablen.

```
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, senden Sie eine POST-Anfrage an `/api/v3/authorize-saml` , und entfernen Sie die zusätzliche JSON-Kodierung aus der Antwort.

Dieses Beispiel zeigt eine POST-Anforderung für eine signierte Authentifizierungs-URL für `TENANTACCOUNTID` . Die Ergebnisse werden weitergeleitet an `python -m json.tool` um die JSON-Kodierung 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, jedoch nicht die zusätzliche JSON-Codierungsebene.

```
{
    "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 zur Verwendung in nachfolgenden Befehlen.

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

d. Rufen Sie eine vollständige URL ab, die die Clientanforderungs-ID von AD FS enthält.

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

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

Die Antwort enthält 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=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-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 Anmeldeinformationen 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=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS gibt eine 302-Weiterleitung mit zusätzlichen Informationen in den Headern zurück.

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

```
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. Speichern Sie die `MSISAuth` Cookie aus der Antwort.

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

h. Senden Sie eine GET-Anfrage mit den Cookies aus dem Authentifizierungs-POST an den angegebenen Speicherort.

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

Die Antwortheader enthalten AD FS-Sitzungsinformationen für die spätere Abmeldung und der Antworttext enthält die SAML-Antwort in einem ausgeblendeten 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=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. Speichern Sie die `SAMLResponse` aus dem versteckten Feld:

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

j. Mit den gespeicherten `SAMLResponse` , erstellen Sie ein StorageGRID`/api/saml-response` Anforderung zum Generieren eines StorageGRID Authentifizierungstokens.

   Für `RelayState` , verwenden Sie die Mandantenkonto-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 enthält das Authentifizierungstoken.

```
{
    "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, 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 wurde, müssen Sie eine Reihe von API-Anfragen stellen, um sich von der Grid Management API oder der Tenant Management API abzumelden. Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitätsanbieter verwenden

Informationen zu diesem Vorgang

Bei Bedarf können Sie sich von der StorageGRID -API abmelden, indem Sie sich von der Single-Logout-Seite Ihrer Organisation abmelden. Oder Sie können Single Logout (SLO) von StorageGRID auslösen, wofür ein gültiges StorageGRID Bearer-Token erforderlich ist.

Schritte

1. Um eine signierte Abmeldeanforderung 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 Abmelde-URL zurückgegeben:

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

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

3. Senden Sie eine Anfrage an die Abmelde-URL, um SLO auszulösen und zurück zu StorageGRID umzuleiten.

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

Die 302-Antwort wird zurückgegeben. Der Umleitungsort ist nicht auf die reine API-Abmeldung anwendbar.

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

Das Löschen des StorageGRID Bearer-Tokens funktioniert genauso wie ohne SSO. Wenn „Cookie „sso=true““ nicht angegeben ist, wird der Benutzer von StorageGRID abgemeldet, ohne dass der SSO-Status beeinträchtigt wird.

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

A `204 No Content` Die 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 (Azure).

Wenn Sie"Single Sign-On (SSO) konfiguriert und aktiviert" und Sie Azure als SSO-Anbieter verwenden, können Sie mithilfe von zwei Beispielskripten ein Authentifizierungstoken erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

Sign in , wenn Azure Single Sign-On aktiviert ist.

Diese Anweisungen gelten, wenn Sie Azure als SSO-Identitätsanbieter verwenden.

Bevor Sie beginnen

- Sie kennen die SSO-E-Mail-Adresse und das Kennwort für einen Verbundbenutzer, der zu einer StorageGRID Benutzergruppe gehört.
- Wenn Sie auf die Tenant Management API zugreifen möchten, kennen Sie die Mandantenkonto-ID.

Informationen zu diesem Vorgang

Um ein Authentifizierungstoken zu erhalten, können Sie die folgenden Beispielskripte verwenden:

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

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

Informationen zum Schreiben Ihrer eigenen API-Integration mit Azure 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 Azure zu interagieren und die SSO-Vorgänge auszuführen.

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 Azure SSO-Schnittstelle verwendet.

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

Schritte

1. Installieren Sie die erforderlichen Abhängigkeiten wie folgt:

a. Installieren Sie Node.js (siehe "https://nodejs.org/en/download/").

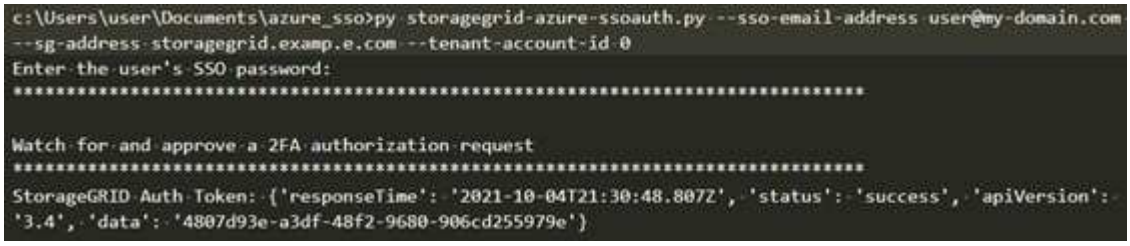
b. Installieren Sie die erforderlichen Node.js-Module (Puppeteer und jsdom):

```
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 Azure SSO-Interaktionen durchzuführen.

3. Geben Sie bei entsprechender Aufforderung Werte für die folgenden Argumente ein (oder übergeben Sie sie mithilfe von Parametern):
   - Die SSO-E-Mail-Adresse, die zur Anmeldung bei Azure verwendet wird
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, wenn Sie auf die Mandantenverwaltungs-API zugreifen möchten
4. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein und seien Sie bereit, Azure bei Bedarf eine MFA-Autorisierung bereitzustellen.



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

Das StorageGRID Autorisierungstoken wird in der Ausgabe bereitgestellt. Sie können das Token jetzt für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet würde.

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

Wenn Sie"Single Sign-On (SSO) konfiguriert und aktiviert" 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.

Sign in , wenn Single Sign-On aktiviert ist

Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitätsanbieter verwenden

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Kennwort für einen Verbundbenutzer, der zu einer StorageGRID -Benutzergruppe gehört.
- Wenn Sie auf die Tenant Management API zugreifen möchten, kennen Sie die Mandantenkonto-ID.

Informationen zu diesem Vorgang

Um ein Authentifizierungstoken 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 Red Hat Enterprise Linux, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware).
- Ein Beispiel-Workflow für Curl-Anfragen.

  Wenn Sie den Curl-Workflow zu langsam ausführen, kann es zu einer Zeitüberschreitung kommen. Möglicherweise wird der folgende Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response`.

  > Der beispielhafte Curl-Workflow schützt das Kennwort nicht davor, von anderen Benutzern eingesehen zu werden.

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

Schritte

1. Wählen Sie eine der folgenden Methoden aus, um ein Authentifizierungstoken zu erhalten:
   - Verwenden Sie die `storagegrid-ssoauth.py` Python-Skript. Fahren Sie mit Schritt 2 fort.
   - Verwenden Sie Curl-Anfragen. Fahren Sie mit Schritt 3 fort.
2. Wenn Sie die `storagegrid-ssoauth.py` Skript, übergeben Sie das Skript an den Python-Interpreter und führen Sie das Skript aus.

   Geben Sie bei entsprechender Aufforderung Werte für die folgenden Argumente ein:

   - Die SSO-Methode. Sie können jede beliebige Variante von „pingfederate“ eingeben (PINGFEDERATE, pingfederate usw.).
   - Der SSO-Benutzername
   - Die Domäne, in der StorageGRID installiert ist. Dieses Feld wird für PingFederate nicht verwendet. Sie können es leer lassen oder einen beliebigen Wert eingeben.
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, wenn Sie auf die Mandantenverwaltungs-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 Autorisierungstoken wird in der Ausgabe bereitgestellt. Sie können das Token jetzt für

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

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

   a. Deklarieren Sie die für die Anmeldung erforderlichen Variablen.

```
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, senden Sie eine POST-Anfrage an `/api/v3/authorize-saml` , und entfernen Sie die zusätzliche JSON-Kodierung aus der Antwort.

   Dieses Beispiel zeigt eine POST-Anfrage für eine signierte Authentifizierungs-URL für TENANTACCOUNTID. Die Ergebnisse werden an python -m json.tool übergeben, um die JSON-Kodierung 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, jedoch nicht die zusätzliche JSON-Codierungsebene.

```
{
    "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 zur Verwendung in nachfolgenden Befehlen.

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

   d. Exportieren Sie die Antwort und das Cookie und geben Sie die Antwort wieder:

```
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 aus:

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

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

f. Exportieren Sie den „href“-Wert (entfernen Sie den abschließenden Schrägstrich /) und geben Sie die Antwort aus:

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

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

g. Exportieren Sie den „Aktionswert“:

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

h. Senden Sie Cookies zusammen mit Anmeldeinformationen:

```
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 die `SAMLResponse` aus dem versteckten Feld:

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

j. Mit den gespeicherten `SAMLResponse` , erstellen Sie ein StorageGRID`/api/saml-response` Anforderung zum Generieren eines StorageGRID Authentifizierungstokens.

   Für `RelayState` , verwenden Sie die Mandantenkonto-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 enthält das Authentifizierungstoken.

```
{
    "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, 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 wurde, müssen Sie eine Reihe von API-Anfragen stellen, um sich von der Grid Management API oder der Tenant Management API abzumelden. Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitätsanbieter verwenden

Informationen zu diesem Vorgang

Bei Bedarf können Sie sich von der StorageGRID -API abmelden, indem Sie sich von der Single-Logout-Seite Ihrer Organisation abmelden. Oder Sie können Single Logout (SLO) von StorageGRID auslösen, wofür ein gültiges StorageGRID Bearer-Token erforderlich ist.

Schritte

1. Um eine signierte Abmeldeanforderung 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 Abmelde-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 Abmelde-URL.

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

3. Senden Sie eine Anfrage an die Abmelde-URL, um SLO auszulösen und zurück zu StorageGRID umzuleiten.

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

Die 302-Antwort wird zurückgegeben. Der Umleitungsort ist nicht auf die reine API-Abmeldung anwendbar.

```
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 Bearer-Token.

Das Löschen des StorageGRID Bearer-Tokens funktioniert genauso wie ohne SSO. Wenn „Cookie „sso=true““ nicht angegeben ist, wird der Benutzer von StorageGRID abgemeldet, ohne dass der SSO-Status beeinträchtigt wird.

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

A `204 No Content` Die Antwort zeigt an, dass der Benutzer jetzt abgemeldet ist.

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

Funktionen mit der API deaktivieren

Sie können die Grid Management API verwenden, um bestimmte Funktionen im StorageGRID -System vollständig zu deaktivieren. Wenn eine Funktion deaktiviert ist, können niemandem Berechtigungen zum Ausführen der mit dieser Funktion verbundenen Aufgaben zugewiesen werden.

Informationen zu diesem Vorgang

Mit dem System „Deaktivierte Funktionen“ können Sie den Zugriff auf bestimmte Funktionen im StorageGRID -System verhindern. Das Deaktivieren einer Funktion ist die einzige Möglichkeit, den Root-Benutzer oder Benutzer, die zu Administratorgruppen mit der Berechtigung **Root-Zugriff** gehören, daran zu hindern, diese Funktion zu verwenden.

Um zu verstehen, wie nützlich diese Funktionalität sein kann, betrachten Sie das folgende Szenario:

Unternehmen A ist ein Dienstanbieter, der die Speicherkapazität seines StorageGRID -Systems durch die Erstellung von Mieterkonten mietet. Um die Sicherheit der Objekte ihrer Mieter zu gewährleisten, möchte Unternehmen A sicherstellen, dass seine eigenen Mitarbeiter nach der Bereitstellung des Kontos niemals auf ein Mieterkonto zugreifen können.

*Unternehmen A kann dieses Ziel erreichen, indem es das System zum Deaktivieren von Funktionen in der Grid Management-API verwendet. Durch die vollständige Deaktivierung der Funktion **Root-Passwort des Mandanten ändern** im Grid Manager (sowohl in der Benutzeroberfläche als auch in der API) stellt Unternehmen A sicher, dass Administratorbenutzer – 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. Greifen Sie auf die Swagger-Dokumentation für die Grid Management API zu. Sehen "Verwenden Sie die Grid Management API" .
2. Suchen Sie den Endpunkt „Funktionen deaktivieren“.
3. Um eine Funktion zu deaktivieren, z. B. „Stammkennwort des Mandanten ändern“, senden Sie einen Text wie diesen an die API:

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

   Wenn die Anfrage abgeschlossen ist, wird die Funktion „Stammkennwort des Mandanten ändern“ deaktiviert. Die Verwaltungsberechtigung **Stammkennwort des Mandanten ändern** wird nicht mehr in der Benutzeroberfläche angezeigt und jede API-Anforderung, die versucht, das Stammkennwort für einen Mandanten zu ändern, schlägt mit „403 Forbidden“ fehl.

Deaktivierte Funktionen reaktivieren

Standardmäßig können Sie die Grid Management API verwenden, um eine deaktivierte Funktion wieder zu aktivieren. Wenn Sie jedoch verhindern möchten, dass deaktivierte Funktionen jemals wieder aktiviert werden, können Sie die Funktion **activateFeatures** selbst deaktivieren.

> Die Funktion **activateFeatures** kann nicht erneut aktiviert werden. Wenn Sie sich entscheiden, diese Funktion zu deaktivieren, beachten Sie, dass Sie dadurch dauerhaft die Möglichkeit verlieren, andere deaktivierte Funktionen wieder zu aktivieren. Sie müssen sich an den technischen Support wenden, um verlorene Funktionen wiederherzustellen.

Schritte

1. Greifen Sie auf die Swagger-Dokumentation für die Grid Management API zu.
2. Suchen Sie den Endpunkt „Funktionen deaktivieren“.
3. Um alle Funktionen wieder zu aktivieren, senden Sie einen Text wie diesen an die API:

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

   Wenn diese Anforderung abgeschlossen ist, werden alle Funktionen, einschließlich der Funktion „Stammkennwort des Mandanten ändern“, wieder aktiviert. Die Verwaltungsberechtigung **Root-Passwort des Mandanten ändern** wird jetzt in der Benutzeroberfläche angezeigt und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, ist erfolgreich, vorausgesetzt, der Benutzer verfügt über die Verwaltungsberechtigung **Root-Zugriff** oder **Root-Passwort des Mandanten ändern**.

   Das vorherige Beispiel bewirkt, dass *alle* deaktivierten Funktionen wieder aktiviert werden. Wenn andere Funktionen deaktiviert wurden und deaktiviert bleiben sollen, müssen Sie diese in der PUT-Anforderung explizit angeben. Um beispielsweise die Funktion „Stammkennwort des Mandanten ändern“ erneut zu aktivieren und die Verwaltungsberechtigung „storageAdmin“ weiterhin zu deaktivieren, senden Sie diese PUT-Anfrage:
   `{ "grid": {"storageAdmin": true} }`