



# グリッド管理APIを使用する StorageGRID

NetApp  
October 03, 2025

# 目次

グリッド管理APIを使用する .....	1
トップレベルのリソース .....	1
グリッド管理 API の処理 .....	1
API要求の実行 .....	3
グリッド管理 API のバージョン管理 .....	5
現在のリリースでサポートされているAPIバージョンを確認します .....	5
要求のAPIバージョンの指定 .....	6
クロスサイトリクエストフォージェリ（CSRF）の防止 .....	6
シングルサインオンが有効な場合は、APIを使用します .....	7
シングルサインオンが有効な場合は、APIへのサインイン .....	7
シングルサインオンが有効な場合は、APIからのサインアウト .....	12

# グリッド管理APIを使用する

Grid Manager のユーザインターフェイスの代わりにグリッド管理 REST API を使用して、システム管理タスクを実行できます。たとえば、API を使用して処理を自動化したり、ユーザなどの複数のエンティティを迅速に作成したりできます。

グリッド管理 API では、Swagger オープンソース API プラットフォームを使用します。Swagger のわかりやすいユーザインターフェイスを使用して、開発者および一般のユーザは StorageGRID で API を使用してリアルタイムの処理を実行できます。

## トップレベルのリソース

グリッド管理 API で使用可能な最上位のリソースは次のとおりです。

- `/grid` : Grid Manager ユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。
- `/org` : テナントアカウントのローカルまたはフェデレーテッドLDAPグループに属するユーザのみがアクセスできます。詳細については、テナントアカウントの使用に関する情報を参照してください。
- `/private` : Grid Manager ユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。これらのAPIは内部使用のみを目的としており、正式にドキュメント化されていません。また、これらのAPIは予告なく変更される場合があります。

### 関連情報

["テナントアカウントを使用する"](#)

["Prometheus : クエリの基本"](#)

## グリッド管理 API の処理

グリッド管理 API では、使用可能な API 処理が次のセクションに分類されます。

- `*accounts*` — 新規アカウントの作成や特定の使用状況の取得など 'ストレージ・テナント・アカウント' を管理するためのオペレーション
- `*alarms*` - 現在のアラーム（レガシーシステム）をリストし、現在のアラートやノード接続状態の概要など、グリッドの健全性に関する情報を返す処理。
- `*alert-history*` — 解決済みアラートに関する操作。
- `*alert-Receiver*` — アラート通知受信者（電子メール）に関する操作。
- `*alert-rules*` — アラートルールに関する操作
- `*alert-silences*` -- アラートのサイレンスに関するオペレーション。
- `*alerts*` — アラートの処理。
- `*audit*` — 監査構成をリストおよび更新する処理。
- `auth` — ユーザセッション認証を実行するための操作。

グリッド管理 API は、ベアトークン認証方式をサポートしています。サインインするには、認証要求

(つまり、POST /api/v3/authorize)。ユーザが認証されると、セキュリティトークンが返されます。このトークンは、後続の API 要求 (「Authorization : Bearer\_token\_」) のヘッダーで指定する必要があります。



StorageGRID システムでシングルサインオンが有効になっている場合は、別の手順による認証が必要です。「シングルサインオンが有効な場合の API へのサインイン」を参照してください。

認証セキュリティの向上については、「クロスサイトリクエストフォージェリに対する保護」を参照してください。

- **\* client-certificates \*** — 外部監視ツールを使用して StorageGRID に安全にアクセスできるようにクライアント証明書を設定する処理。
- **\* config \*** — 製品リリースと Grid Management API のバージョンに関連する操作。製品のリリースバージョンおよびそのリリースでサポートされているグリッド管理 API のメジャーバージョンをリストし、廃止されたバージョンの API を無効にすることができます。
- **\* deactivated-features \*** — 非アクティブ化された可能性のある機能を表示する操作。
- **\* dns-servers \*** — 設定済みの外部 DNS サーバをリストおよび変更する処理。
- **\* endpoint-domain-names \*** — エンドポイントドメイン名をリストおよび変更する処理。
- **\* erasure-coding \*** — イレイジャーコーディングプロファイルに対する処理。
- **\* expansion \*** -- 拡張の操作 ( プロシージャレベル ) 。
- **\* expansion-nodes \*** - 拡張処理 ( ノードレベル ) 。
- **\* expansion-sitites \*** — 拡張の操作 ( サイトレベル ) 。
- **\* grid-networks \*** — グリッドネットワークリストをリストおよび変更する処理。
- **\* grid-password \*** - グリッドパスワード管理の操作。
- **\* groups \*** — ローカルグリッド管理者グループを管理し、フェデレーテッドグリッド管理者グループを外部 LDAP サーバから取得するための処理。
- **\* identity-source \*** — 外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- **\* ilm \*** — 情報ライフサイクル管理 (ILM; 情報ライフサイクル管理 ) の操作。
- **\* license \*** — StorageGRID ライセンスを取得および更新する処理。
- **\* logs \*** — ログファイルを収集してダウンロードするための操作。
- **\* メトリクス \*** — ある時点での瞬時の指標クエリや、一定期間にわたる指標クエリなど、StorageGRID メトリックに対する処理。グリッド管理 API は、バックエンドのデータソースとして Prometheus システム監視ツールを使用します。Prometheus クエリの構築については、Prometheus の Web サイトを参照してください。



を含む指標 *private* 名前には、内部使用のみを目的としています。これらの指標は、StorageGRID のリリース間で予告なく変更される可能性があります。

- **\* node-health \*** - ノードのヘルスステータスに関する処理。
- **\* ntp-servers \*** — 外部ネットワークタイムプロトコル ( NTP ) サーバをリストまたは更新する処理。

- `* objects *` — オブジェクトおよびオブジェクトメタデータに対する処理。
- `* recovery` — リカバリ手順 の処理。
- `* recovery-package *` — リカバリパッケージをダウンロードする処理。
- `* regions *` — 領域の表示と作成のための操作。
- `* s3-object-lock *` — グローバルな S3 オブジェクトロック設定に対する処理。
- `* server-certificate *` — Grid Manager サーバ証明書を表示および更新する処理。
- `* snmp *` — 現在の SNMP 設定に対する操作。
- `* traffic-classes *` -- トラフィック分類ポリシーの操作。
- `* untrusted-client-network *` — 信頼されていないクライアントネットワーク構成に対する操作。
- `* users *` — Grid Manager ユーザーを表示および管理する操作。

## API要求の実行

Swagger のユーザインターフェイスでは、各 API 処理に関する詳細情報とドキュメントを参照できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。



API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

1. Grid Managerヘッダーから `* Help > API Documentation *` を選択します。
2. 目的の処理を選択します。

API 処理を拡張すると、GET、PUT、UPDATE、DELETE など、使用可能な HTTP アクションを確認できます。

3. HTTP アクションを選択して、要求の詳細を確認します。これには、エンドポイント URL、必須またはオプションのパラメータのリスト、要求の本文の例（必要な場合）、想定される応答が含まれます。

GET
/grid/groups
Lists Grid Administrator Groups

Parameters
Try it out

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

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>

- グループやユーザの ID など、要求で追加のパラメータが必要かどうかを確認します。次に、これらの値を取得します。必要な情報を取得するために、先に別の API 要求の問題 が必要になることがあります。
- 要求の本文の例を変更する必要があるかどうかを判断します。その場合は、[\*Model]をクリックして各フィールドの要件を確認できます。
- [\* 試してみてください \*] をクリックします。
- 必要なパラメータを指定するか、必要に応じて要求の本文を変更します。
- [\* Execute] をクリックします。
- 応答コードを確認し、要求が成功したかどうかを判断します。

# グリッド管理 API のバージョン管理

グリッド管理 API では、バージョン管理を使用して無停止アップグレードがサポートされます。

たとえば、次の要求 URL ではバージョン 3 の API が指定されています。

`https://hostname_or_ip_address/api/v3/authorize`

旧バージョンとの互換性がない `*_not compatible_*` の変更が行われると、テナント管理 API のメジャーバージョンが上がります。以前のバージョンと互換性がある `_*` の変更を行うと、テナント管理 API のマイナーバージョンが上がります。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。次の例は、変更のタイプに基づいて API バージョンがどのように更新されるかを示しています。

API に対する変更のタイプ	古いバージョン	新しいバージョン
旧バージョンと互換性があります	2.1	2.2.
旧バージョンとの互換性がありません	2.1	3.0

StorageGRID ソフトウェアを初めてインストールした時点では、グリッド管理 API の最新のバージョンのみが有効になっています。ただし、StorageGRID の新機能リリースにアップグレードした場合、少なくとも StorageGRID の機能リリース 1 つ分の間は、古い API バージョンにも引き続きアクセスできます。



グリッド管理 API を使用して、サポートされるバージョンを設定できます。詳細については、Swagger API のドキュメントの「config」セクションを参照してください。すべての Grid 管理 API クライアントを新しいバージョンを使用するように更新したら、古いバージョンのサポートを無効にする必要があります。

古い要求は、次の方法で廃止とマークされます。

- 応答ヘッダーが「Deprecated : true」となる。
- JSON 応答の本文に「deprecated : true」が追加される
- 廃止の警告が nms.log に追加される。例：

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

現在のリリースでサポートされている**APIバージョン**を確認します

サポートされている API のメジャーバージョンのリストを返すには、次の API 要求を使用します。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

## 要求のAPIバージョンの指定

パスパラメータを使用してAPIバージョンを指定できます (/api/v3) またはヘッダー (Api-Version: 3)。両方の値を指定した場合は、ヘッダー値がパス値よりも優先されます。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

## クロスサイトリクエストフォージェリ (CSRF) の防止

CSRF トークンを使用してクッキーによる認証を強化すると、StorageGRID に対するクロスサイトリクエストフォージェリ (CSRF) 攻撃を防ぐことができます。Grid Manager と Tenant Manager はこのセキュリティ機能を自動的に有効にします。他の API クライアントは、サインイン時にこの機能を有効にするかどうかを選択できます。

攻撃者が別のサイト（たとえば、HTTP フォーム POST を使用して）への要求をトリガーできる場合、サインインしているユーザのクッキーを使用して特定の要求を原因 が送信できます。

StorageGRID では、CSRF トークンを使用して CSRF 攻撃を防ぐことができます。有効にした場合、特定のクッキーの内容が特定のヘッダーまたは特定の POST パラメータの内容と一致する必要があります。

この機能を有効にするには、を設定します csrfToken パラメータの値 true 認証中です。デフォルトはです 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"
```



trueの場合は、Aです GridCsrfToken クッキーは、Grid Managerおよびへのサインインにランダムな値を使用して設定されます AccountCsrfToken クッキーは、Tenant Managerへのサインインではランダムな値で設定されます。

クッキーが存在する場合は、システムの状態を変更できるすべての要求（POST、PUT、PATCH、DELETE）には次のいずれかが含まれている必要があります。

- X-Csrf-Token CSRFトークンクッキーの値がヘッダーに設定されています。
- エンドポイントがフォームエンコードされた本文を受け入れる場合：A csrfToken フォームエンコードされた要求の本文パラメータ。

その他の例および詳細については、オンラインのAPIドキュメントを参照してください。



CSRFトークンクッキーが設定されている要求では、も適用されます "Content-Type: application/json" CSRF攻撃からの保護がさらに強化されるために、JSON要求の本文が必要なすべての要求のヘッダー。

## シングルサインオンが有効な場合は、**API**を使用します

StorageGRID システムでシングルサインオン（SSO）が有効になっている場合、標準の認証API要求を使用してグリッド管理APIまたはテナント管理APIにサインインおよびサインアウトすることはできません。

### シングルサインオンが有効な場合は、**API**へのサインイン

シングルサインオン（SSO）が有効になっている場合は、グリッド管理APIまたはテナント管理APIで有効なAD FSから認証トークンを取得するための一連のAPI要求を問題で処理する必要があります。

必要なもの

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO ユーザ名とパスワードが必要です。
- テナント管理 API にアクセスする場合は、テナントアカウント ID を確認しておきます。

このタスクについて

認証トークンを取得するには、次のいずれかの例を使用します。

- storagegrid-ssoauth.py Pythonスクリプト。StorageGRID インストールファイルのディレクトリにあります（./rpms Red Hat Enterprise LinuxまたはCentOSの場合：./debs UbuntuまたはDebianの場合は、および ./vsphere VMwareの場合）をクリックします。
- cURL 要求のワークフローの例。

cURL ワークフローは、実行に時間がかかりすぎるとタイムアウトする場合があります。「A valid SubjectConfirmation was not found on this Response」というエラーが表示される可能性があります。



cURL ワークフローの例では、パスワードが他のユーザに表示されないように保護されていません。

URLエンコード問題 がある場合は、「Unsupported SAML version」というエラーが表示される可能性があります。

#### 手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
  - を使用します `storagegrid-ssoauth.py` Pythonスクリプト。手順 2 に進みます。
  - `curl` 要求を使用します。手順 3 に進みます。
2. を使用する場合は、を参照してください `storagegrid-ssoauth.py` スクリプトを使用して、Pythonインタープリタにスクリプトを渡し、スクリプトを実行します。

プロンプトが表示されたら、次の引数の値を入力します。

- SSO ユーザ名
- StorageGRID がインストールされているドメイン
- StorageGRID のアドレス
- テナント管理APIにアクセスする場合は、テナントアカウントIDを入力します。

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

*****

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

[+]

StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

3. `cURL` 要求を使用する場合は、次の手順 を使用します。
  - a. サインインに必要な変数を宣言します。

```
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'
```



グリッド管理APIにアクセスするには、として0を使用します `TENANTACCOUNTID`。

- b. 署名付き認証URLを受信するには、へのPOST要求を問題 に送信します `/api/v3/authorize-saml` をクリックし、応答からJSONエンコードを削除します。

次の例は、の署名付き認証URLに対するPOST要求を示しています TENANTACCOUNTID。結果は python-m json ツールに渡され、JSON エンコードが削除されます。

```
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
```

この例の応答には、URL エンコードされた署名済み URL が含まれていますが、JSON エンコードされたレイヤは含まれていません。

```
{
  "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. を保存します SAMLRequest 後続のコマンドで使用する応答から。

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

d. AD FS からクライアント要求 ID を含む完全な URL を取得します。

1 つは、前の応答の URL を使用してログインフォームを要求する方法です。

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

応答にはクライアント要求 ID が含まれています。

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

e. 応答からクライアント要求 ID を保存します。

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

- f. 前の応答のフォームアクションにクレデンシャルを送信します。

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

AD FS からヘッダーに追加情報が含まれた 302 リダイレクトが返されます。



SSO システムで多要素認証（MFA）が有効になっている場合、フォームポストには 2 つ目のパスワードまたはその他のクレデンシャルも含まれます。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTomwFIZfhh...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. を保存します MSISAuth 応答からのCookie。

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

- h. 認証 POST からクッキーを使用して、指定した場所に GET 要求を送信します。

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

応答ヘッダーには、あとでログアウトに使用する AD FS セッション情報が含まれます。応答の本文には、非表示のフォームフィールドに SAMLResponse が含まれています。

```

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
XFxVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
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="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />

```

- i. を保存します SAMLResponse 非表示フィールドから：

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

- j. を使用して保存します `SAMLResponse` をクリックして、StorageGRID を作成します /api/saml-response StorageGRID 認証トークンの生成要求

の場合 `RelayState` をクリックします。グリッド管理APIにサインインする場合は、テナントアカウントIDを使用します。

```

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

```

応答には認証トークンが含まれています。

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

- a. 認証トークンを応答にという名前で保存します MYTOKEN。

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

これで、使用できます MYTOKEN その他の要求の場合は、SSOを使用していない場合のAPIの使用方法と同様です。

## シングルサインオンが有効な場合は、**API**からのサインアウト

シングルサインオン（SSO）が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を問題 で処理する必要があります。

このタスクについて

必要に応じて、組織のシングルログアウトページからログアウトするだけで、StorageGRID API からサインアウトできます。または、StorageGRID からシングルログアウト（SLO）を実行することもできます。この場合、有効な StorageGRID ベアラトークンが必要です。

手順

1. 署名されたログアウト要求を生成するには、合格します cookie "sso=true" SLO APIで次の処理を実行します。

```
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
```

ログアウト URL が返されます。

```
{
  "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. ログアウト URL を保存します。

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

## 3. 要求をログアウト URL に送信し、SLO を実行して StorageGRID にリダイレクトします。

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

302 応答が返されます。リダイレクト先は API のみのログアウトには適用されません。

```
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. StorageGRID Bearer トークンを削除します。

StorageGRID Bearer トークンを削除すると、SSO を使用しない場合と同じように動作します。状況 cookie "sso=true" を指定しないと、SSO の状態に影響を及ぼすことなくユーザが StorageGRID からログアウトされます。

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

A 204 No Content 応答として、ユーザがサインアウトしたことが示されます。

HTTP/1.1 204 No Content



## 著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。