



# アクセス管理

## SANtricity software

NetApp  
November 03, 2025

# 目次

アクセス管理	1
SANtricity Unified Managerのアクセス管理について学ぶ	1
どのような認証方式を使用できますか。	1
アクセス管理を設定するにはどうすればよいですか。	1
概念	1
SANtricity Unified Manager におけるアクセス管理の仕組み	1
SANtricity Unified Managerのアクセス管理用語について学ぶ	2
マッピングされたロールの権限	3
SANtricity Unified Manager のローカル ユーザー ロールによるアクセス管理	4
SANtricity Unified Manager のディレクトリ サービスによるアクセス管理	4
SANtricity Unified Manager における SAML を使用したアクセス管理	5
ローカルユーザロールを使用する	6
ローカルユーザロールを表示します	6
SANtricity Unified Manager のローカル ユーザー プロファイルのパスワードを変更する	7
SANtricity Unified Managerでローカルユーザーのパスワード設定を変更する	8
ディレクトリサービスを使用する	9
SANtricity Unified Managerにディレクトリサーバーを追加する	9
SANtricity Unified Managerでディレクトリサーバーの設定と役割のマッピングを編集する	15
ディレクトリサーバを削除します	18
SAMLを使用する	18
SANtricity Unified ManagerでSAMLを設定する	18
SANtricity Unified Manager で SAML ロール マッピングを変更する	22
SANtricity Unified ManagerでSAMLサービスプロバイダーファイルをエクスポートする	23
SANtricity Unified Manager のユーザー アクセス管理に関する FAQ	24
ログインできない理由は何ですか？	24
ディレクトリサーバを追加するときは、どのような点に注意する必要がありますか？	25
ストレージレイのロールをマッピングするときは、どのような点に注意する必要がありますか？	25
SAMLを設定および有効にするときは、どのような点に注意する必要がありますか？	26
ローカルユーザとは何ですか？	27

# アクセス管理

## SANtricity Unified Managerのアクセス管理について学ぶ

アクセス管理では、SANtricity Unified Managerでユーザ認証を設定することができます。

どのような認証方式を使用できますか。

次の認証方式を使用できます。

- ローカルユーザーの役割-- RBAC（役割ベースのアクセス制御）機能を使用して認証を管理します。ローカルユーザロールには、事前定義されたユーザプロフィールと、特定のアクセス権限を持つロールが含まれます。
- ディレクトリサービス-- LDAP (Lightweight Directory Access Protocol)サーバとディレクトリサービス(MicrosoftのActive Directoryなど)を介して認証を管理します
- \*saml \*-- SAML 2.0を使用して、アイデンティティプロバイダ (IdP) を介して認証を管理します。

詳細はこちら。

- ["アクセス管理の仕組み"](#)
- ["アクセス管理の用語"](#)
- ["マッピングされたロールの権限"](#)
- ["SAML"](#)

アクセス管理を設定するにはどうすればよいですか。

SANtricity ソフトウェアは、ローカルユーザロールを使用するように事前に設定されています。LDAPを使用する場合は、[Access Management]ページでLDAPを設定できます。

詳細はこちら。

- ["ローカルユーザロールを使用したアクセス管理"](#)
- ["ディレクトリサービスを使用したアクセス管理"](#)
- ["SAMLを設定する"](#)

## 概念

### SANtricity Unified Manager におけるアクセス管理の仕組み

アクセス管理を使用してSANtricity Unified Managerでのユーザ認証を確立する。

設定ワークフロー

アクセス管理の設定は次のように行います。

## 1. Security Adminの権限を含むユーザプロフィールでUnified Managerにログインします。



初めてのログインでは'ユーザ名adminが自動的に表示され'変更することはできませんadminユーザは'システムのすべての機能にフル・アクセスできます初回ログイン時にパスワードを設定する必要があります。

2. ユーザインターフェイスでアクセス管理に移動します。事前に設定されているローカルユーザロールが表示されます。これらのロールはRBAC（ロールベースアクセス制御）機能の実装です。
3. 管理者は、次の認証方式を1つ以上設定します。
  - ローカルユーザの役割-- RBAC機能を使用して認証を管理しますローカルユーザロールには、事前定義されたユーザと、特定のアクセス権限を持つロールが含まれます。管理者は、これらのローカルユーザロールを単一の認証方式として使用することも、ディレクトリサービスと組み合わせて使用することもできます。ユーザのパスワードを設定する以外に必要な設定はありません。
  - ディレクトリサービス-- LDAP (Lightweight Directory Access Protocol)サーバとディレクトリサービス(MicrosoftのActive Directoryなど)を介して認証を管理します管理者がLDAPサーバに接続し、ローカルユーザロールにLDAPユーザをマッピングします。
  - \*saml \*-- Security Assertion Markup Language (SAML) 2.0を使用してアイデンティティプロバイダ (IdP) を介して認証を管理します。管理者がIdPシステムとストレージレイの間の通信を確立し、ストレージレイに組み込まれているローカルユーザロールにIdPユーザをマッピングします。
4. Unified Managerのログインクレデンシャルをユーザに割り当てます。
5. ユーザが自身のクレデンシャルを入力してシステムにログインします。ログイン時には、次のバックグラウンドタスクが実行されます。
  - ユーザ名とパスワードをユーザアカウントと照合して認証します。
  - 割り当てられたロールに基づいてユーザの権限が決まります。
  - ユーザインターフェイスの機能にユーザがアクセスできるようにします。
  - 上部のバナーにユーザ名が表示されます。

## Unified Managerで使用できる機能

機能へのアクセスは、ユーザに割り当てられたロールによって次のように異なります。

- \* Storage admin \*--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません
- \* Security admin \*--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
- \* Support admin \*--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
- \*Monitor \*--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

使用できない機能は、ユーザインターフェイスではグレー表示されるか、非表示になります。

## SANtricity Unified Managerのアクセス管理用語について学ぶ

SANtricity Unified Managerに関連するアクセス管理の用語を次に示します。

期間	説明
Active Directory	Active Directory (AD) は、Windowsドメインネットワーク用のLDAPを使用するMicrosoftのディレクトリサービスです。
結合	バインド処理は、ディレクトリサーバに対するクライアントの認証に使用されます。通常はアカウントとパスワードのクレデンシャルが必要ですが、匿名のバインド処理が可能なサーバもあります。
できます	認証局 (CA) は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子文書を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。
証明書	証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明 (署名) する信頼されたエンティティのIDが含まれます。
LDAP	Lightweight Directory Access Protocol (LDAP) は、分散型のディレクトリ情報サービスへのアクセスと管理に使用されるアプリケーションプロトコルです。このプロトコルを使用すると、さまざまなアプリケーションやサービスがLDAPサーバに接続してユーザを検証できます。
RBAC	ロールベースアクセス制御 (RBAC) は、コンピュータやネットワークリソースへのアクセスを個々のユーザのロールに基づいて制御する手法です。Unified Managerには事前定義されたロールがあります
SAML	Security Assertion Markup Language (SAML) は、2つのエンティティ間の認証と許可に使用されるXMLベースの標準規格です。SAMLは、ユーザの認証時に複数の項目 (パスワードとフィンガープリントなど) を求める多要素認証に対応しています。ストレージレイに組み込まれているSAML機能は、アイデンティティのアサーション、認証、および許可に関してSAML2.0に準拠しています。
SSO	シングルサインオン (SSO) は、1組のログインクレデンシャルで複数のアプリケーションにアクセスできるようにする認証サービスです。
Web Services Proxyの使用 方法	Web Services Proxyは標準のHTTPSメカニズムによるアクセスを提供するプロキシで、管理者にストレージレイの管理サービスの設定を許可します。このプロキシは、WindowsホストまたはLinuxホストにインストールできます。Unified ManagerインターフェイスはWeb Services Proxyで使用できます。

## マッピングされたロールの権限

ロールベースアクセス制御 (RBAC) 機能には、1つ以上のロールがマッピングされた事前定義済みのユーザが含まれています。各ロールには、SANtricity Unified Managerのタスクにアクセスするための権限が含まれています。

これらのロールにより、次のタスクへのアクセスが可能になります。

- \* Storage admin \*--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません
- \* Security admin \*--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
- \* Support admin \*--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
- \* Monitor \*--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

ユーザに特定の機能に対する権限がない場合、その機能は選択できないか、ユーザインターフェイスに表示されません。

## SANtricity Unified Manager のローカル ユーザー ロールによるアクセス管理

管理者は、SANtricity Unified Managerに組み込みのロールベースアクセス制御（RBAC）機能を使用できます。これらの機能は、「ローカルユーザロール」と呼ばれます。

### 設定ワークフロー

ローカルユーザロールはシステムで事前に設定されています。認証にローカルユーザロールを使用する場合、管理者は次の操作を行うことができます。

1. Security Adminの権限を含むユーザプロファイルでUnified Managerにログインします。



adminユーザはシステムのすべての機能にフル・アクセスできます

2. ユーザプロファイルを確認します。ユーザプロファイルは事前に定義されており、変更することはできません。
3. 必要に応じて、各ユーザプロファイルに新しいパスワードを割り当てます。
4. ユーザは各自に割り当てられたクレデンシャルでシステムにログインします。

### 管理

認証にローカルユーザロールのみを使用する場合、管理者は次の管理タスクを実行できます。

- パスワードを変更します。
- パスワードの最小文字数を設定する。
- パスワードなしでのログインをユーザに許可します。

## SANtricity Unified Manager のディレクトリ サービスによるアクセス管理

LDAP（Lightweight Directory Access Protocol）サーバとディレクトリサービス（MicrosoftのActive Directoryなど）を使用して認証を管理することができます。

### 設定ワークフロー

ネットワークでLDAPサーバとディレクトリサービスが使用されている場合、設定は次のようになります。

1. Security Adminの権限を含むユーザプロファイルでUnified Managerにログインします。



adminユーザはシステムのすべての機能にフル・アクセスできます

2. LDAPサーバの設定を入力します。これには、ドメイン名、URL、バインドアカウント情報が含まれます。
3. LDAPサーバでセキュアなプロトコル（LDAPS）を使用している場合、LDAPサーバとホストシステム（Webサービスプロキシがインストールされているシステム）の間の認証に使用する認証局（CA）証明書チェーンをアップロードします。
4. サーバ接続が確立されたら、ユーザグループをローカルユーザロールにマッピングします。これらのロールは事前に定義されており、変更できません。
5. LDAPサーバとWebサービスプロキシの間の接続をテストします。
6. ユーザは各自に割り当てられたLDAP /ディレクトリサービスのクレデンシャルを使用してシステムにログインします。

## 管理

認証にディレクトリサービスを使用する場合、管理者は次の管理タスクを実行できます。

- ディレクトリサーバを追加します。
- ディレクトリサーバの設定を編集します。
- LDAPユーザをローカルユーザロールにマッピングする。
- ディレクトリサーバを削除する。
- パスワードを変更します。
- パスワードの最小文字数を設定する。
- パスワードなしでのログインをユーザに許可します。

## SANtricity Unified Manager における SAML を使用したアクセス管理

管理者は、アレイに組み込みのSecurity Assertion Markup Language（SAML）2.0の機能をアクセス管理に使用できます。

### 設定ワークフロー

SAMLの設定は次のように行います。

1. Security Adminの権限を含むユーザプロファイルでUnified Managerにログインします。



adminユーザはSystem Managerのすべての機能にフル・アクセスできます

2. 管理者は、[アクセス管理]の下の[\*SAML \*]タブに移動します。
3. アイデンティティプロバイダ（IdP）との通信を設定します。IdPは、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するための外部システムです。ストレージアレイとの通信を設定するには、IdPシステムからIdPメタデータファイルをダウンロードし、Unified Managerを使用してそのファイルをストレージアレイにアップロードします。

4. サービスプロバイダとIdP間の信頼関係を確立します。サービスプロバイダはユーザ権限を制御します。このケースでは、ストレージレイ内のコントローラがサービスプロバイダの役割を果たします。通信を設定するために、管理者はUnified Managerを使用してコントローラのサービスプロバイダメタデータファイルをエクスポートします。次に、IdPシステムからメタデータファイルをIdPにインポートします。



また、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。

5. ストレージレイのロールをIdPで定義されているユーザ属性にマッピングします。そのためには、管理者はUnified Managerを使用してマッピングを作成します。
6. IdP URLへのSSOログインをテストします。このテストで、ストレージレイとIdPが通信できることを確認します。



SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

7. Unified Managerで、ストレージレイのSAMLを有効にします。
8. ユーザが自身のSSOクレデンシャルを使用してシステムにログインします。

## 管理

認証にSAMLを使用している場合、管理者は次の管理タスクを実行できます。

- 新しいロールマッピングを変更または作成します
- サービスプロバイダファイルをエクスポート

## アクセス制限

SAMLが有効な場合、ユーザは従来のStorage Managerインターフェイスからそのレイのストレージを検出または管理できません。

また、次のクライアントはストレージレイのサービスとリソースにアクセスできません。

- Enterprise Management Window (EMW)
- コマンドラインインターフェイス (CLI)
- ソフトウェア開発キット (SDK) クライアント
- インバンドクライアント
- HTTPベーシック認証REST APIクライアント
- 標準のREST APIエンドポイントを使用してログインします

## ローカルユーザロールを使用する

ローカルユーザロールを表示します

[ローカルユーザの役割]タブでは、ユーザーとデフォルトの役割とのマッピングを表示

できます。これらのマッピングは、SANtricity Unified ManagerのWebサービスプロキシで適用されるRBAC（ロールベースアクセス制御）の一部です。

作業を開始する前に

Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

このタスクについて

ユーザとマッピングは変更できません。変更できるのはパスワードだけです。

手順

1. アクセス管理\*を選択します。
2. [ローカルユーザー役割\* (Local User Roles \*) ]タブを選択します。

表にユーザが表示されます。

- **admin**--システム内のすべての機能にアクセスできるスーパー管理者。このユーザにはすべてのロールが含まれています
- **\* storage \***--すべてのストレージ・プロビジョニングを担当する管理者。このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。
- **\* security \***--アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザには、Security AdminとMonitorのロールが含まれています。
- **\* support \***--ハードウェアリソース、障害データ、ファームウェアアップグレードを担当するユーザー。このユーザには、Support AdminとMonitorのロールが含まれています。
- **\* monitor \***--システムへの読み取り専用アクセス権を持つユーザー。このユーザにはMonitorロールのみが含まれています。
- **\* rw \*** (読み取り/書き込み) -このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。
- **\* ro \*** (読み取り専用) --このユーザーには、Monitorロールのみが含まれています。

## SANtricity Unified Manager のローカル ユーザー プロファイルのパスワードを変更する

アクセス管理で各ユーザのユーザパスワードを変更できます。

作業を開始する前に

- Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。
- ローカル管理者のパスワードを確認しておく必要があります。

このタスクについて

パスワードを選択する際は、次のガイドラインに注意してください。

- 新しいローカルユーザパスワードは、最小パスワードの現在の設定 ([表示/編集の設定]) 以上である必要があります。
- パスワードは大文字と小文字を区別します。

- パスワードの末尾のスペースは削除されません。パスワードにスペースが含まれている場合は、スペースを含めるようにしてください。
- セキュリティを強化するために、パスワードには15文字以上の英数字を使用し、頻繁に変更してください。

#### 手順

1. アクセス管理\*を選択します。
2. [ローカルユーザー役割\* (Local User Roles \*) ]タブを選択します。
3. 表からユーザを選択します。

[パスワードの変更]ボタンが使用可能になります。

4. [パスワードの変更\*]を選択します。

[パスワードの変更]ダイアログボックスが開きます。

5. ローカルユーザパスワードに対して最小文字数が設定されていない場合は、システムにアクセスするユーザにパスワードの入力を求めるチェックボックスを選択できます。
6. 選択したユーザの新しいパスワードを2つのフィールドに入力します。
7. この操作を確認するためにローカル管理者パスワードを入力し、\*変更\*をクリックします。

#### 結果

ユーザが現在ログインしている場合、パスワードを変更するとユーザのアクティブなセッションが終了します。

## SANtricity Unified Managerでローカルユーザーのパスワード設定を変更する

すべての新規または更新されるローカルユーザパスワードの最小文字数を設定できます。また、ローカルユーザがパスワードを入力せずにシステムにアクセスできるようにすることもできます。

#### 作業を開始する前に

Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。

#### このタスクについて

ローカルユーザパスワードの最小文字数を設定する際には、次のガイドラインに注意してください。

- 設定を変更しても既存のローカルユーザパスワードには影響しません。
- ローカルユーザパスワードの最小文字数は、0~30文字にする必要があります。
- 新しいローカルユーザパスワードは、現在の最小文字数の設定以上にする必要があります。
- ローカルユーザがパスワードを入力せずにシステムにアクセスできるようにする場合は、パスワードの最小文字数を設定しないでください。

#### 手順

1. アクセス管理\*を選択します。

2. [ローカルユーザー役割\* (Local User Roles \*) ]タブを選択します。

3. 「表示/設定の編集」を選択します。

[ローカルユーザーパスワードの設定]ダイアログボックスが開きます。

4. 次のいずれかを実行します。

- ローカルユーザがパスワードを入力せずにsystem\_にアクセスできるようにするには、「すべてのローカルユーザパスワードを最低必要とする」チェックボックスをオフにします。
- すべてのローカルユーザパスワードの最小文字数を設定するには、「すべてのローカルユーザパスワードを少なくとも必要とする」チェックボックスを選択し、スピンボックスを使用してすべてのローカルユーザパスワードの最小文字数を設定します。

新しいローカルユーザパスワードは、現在の設定以上の長さにする必要があります。

5. [保存 ( Save ) ]をクリックします。

## ディレクトリサービスを使用する

### SANtricity Unified Managerにディレクトリサーバーを追加する

アクセス管理用の認証を設定するには、LDAPサーバとSANtricity Unified ManagerのWebサービスプロキシを実行するホストの間の通信を確立します。その後、LDAPユーザグループをローカルユーザロールにマッピングします。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ユーザグループがディレクトリサービスに定義されている必要があります。
- LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバのURLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
- セキュアなプロトコルを使用するLDAPSサーバの場合は、LDAPサーバの証明書チェーンがローカルマシンにインストールされている必要があります。

このタスクについて

ディレクトリサーバの追加は、2つのステップで行います。まず、ドメイン名とURLを入力します。サーバでセキュアなプロトコルを使用している場合、認証に使用するCA証明書が標準の署名機関によって署名されていない場合、その証明書もアップロードする必要があります。バインドアカウントのクレデンシャルがある場合は、そのアカウント名とパスワードも入力できます。次に、LDAPサーバのユーザグループをローカルユーザロールにマッピングします。

手順

1. アクセス管理\*を選択します。

2. [ディレクトリサービス]タブで、[ディレクトリサーバーの追加]を選択します。

[ディレクトリサーバーの追加]ダイアログボックスが開きます。

3. [サーバー設定]タブで、LDAPサーバーの資格情報を入力します。

フィールドの詳細

設定	説明
構成設定	ドメイン
<p>LDAPサーバのドメイン名を入力します。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン (<i>username@domain</i>) で、認証するディレクトリサーバを指定するために使用されます。</p>	サーバURL
<p>LDAPサーバにアクセスするためのURLを'<code>ldap[s]://host:*port*</code>'の形式で入力します</p>	証明書のアップロード (オプション)
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px; text-align: center;">  </div> <div> <p>このフィールドは、上記のサーバURLフィールドにLDAP Sプロトコルが指定されている場合にのみ表示されます。</p> </div> </div> <p><b>[Browse]</b>をクリックして、アップロードするCA証明書を選択します。これは、LDAPサーバの認証に使用される信頼された証明書または証明書チェーンです。</p>	バインドアカウント (オプション)

設定	説明
<p>LDAPサーバに対する検索クエリやグループ内の検索で使用する読み取り専用のユーザアカウントを入力します。アカウント名はLDAPタイプの形式で入力します。たとえば、バインドユーザの名前が「bindacct」であれば、「CN=bindacct、CN=Users、DC=cpoc、DC=local」などと入力します。</p>	<p>バインドパスワード (オプション)</p>
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  </div> <div> <p>このフィールドは、バインドアカウントを入力した場合に表示されません。</p> </div> </div> <p>バインドアカウントのパスワードを入力します。</p>	<p>追加する前にサーバ接続をテストします</p>
<p>入力したLDAPサーバの設定でシステムと通信できるかどうかを確認するには、このチェックボックスを選択します。このテストは、ダイアログボックスの下部にある*追加* (* Add *) をクリックした後に実行されます。</p> <p>このチェックボックスをオンにした場合、テストに失敗すると設定は追加されません。設定を追加するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。</p>	<p>権限の設定</p>

設定	説明
検索ベースDN	ユーザを検索するLDAPコンテキストを入力します。通常は、の形式で入力します CN=Users, DC=cpoc, DC=local。
ユーザー名属性	認証用のユーザIDにバインドされた属性を入力します。例: 「sAMAccountName」。
グループ属性	グループとロールのマッピングに使用される、ユーザの一連のグループ属性を入力します。例: memberOf, managedObjects`

4. [役割マッピング (Role Mapping \*) ]タブをクリックします。
5. 事前定義されたロールにLDAPグループを割り当てます。1つのグループに複数のロールを割り当てることができます。

設定	説明
マッピング	グループDN
マッピングするLDAPユーザグループの識別名 (DN) を指定します。正規表現がサポートされます。正規表現パターンに含まれていない場合は、これらの特殊な正規表現文字をバックスラッシュ (\) でエスケープする必要があります。 \.[]{}()<>*+ -=!/?^\$	
ロール	<p>フィールド内をクリックし、グループDNにマッピングするローカルユーザロールを選択します。このグループに含めるロールを個別に選択する必要があります。MonitorロールはSANtricity Unified Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。各ロールの権限は次のとおりです。</p> <ul style="list-style-type: none"> <li>• * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません</li> <li>• * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。</li> <li>• * Support admin *--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。</li> <li>• *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。</li> </ul>



Monitorロールは、管理者を含むすべてのユーザに必要です。

- 必要に応じて、\*別のマッピングを追加\*をクリックして、グループとロールのマッピングをさらに入力します。
- マッピングが終了したら、\*追加\*をクリックします。

ストレージアレイとLDAPサーバが通信できるかどうかの検証がシステムによって実行されます。エラーメッセージが表示された場合は、ダイアログボックスで入力したクレデンシャルを確認し、必要に応じて情報を再入力します。

## SANtricity Unified Managerでディレクトリサーバーの設定と役割のマッピングを編集する

アクセス管理でディレクトリサーバを設定済みの場合は、いつでも設定を変更できます。設定には、サーバ接続情報とグループとロールのマッピングが含まれます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ディレクトリサーバが定義されている必要があります。

手順

1. アクセス管理\*を選択します。
2. [ディレクトリサービス]タブを選択します。
3. 複数のサーバが定義されている場合は、編集するサーバを表から選択します。
4. 「表示/設定の編集」を選択します。

[ディレクトリサーバーの設定]ダイアログボックスが開きます。

5. サーバー設定\*タブで、必要な設定を変更します。

## フィールドの詳細

設定	説明
構成設定	ドメイン
LDAPサーバのドメイン名。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン ( <i>username@domain</i> ) で、認証するディレクトリサーバを指定するために使用されます。	サーバURL
LDAPサーバにアクセスするためのURL。形式はです <code>ldap[s]://host:port</code> 。	バインドアカウント (オプション)
LDAPサーバに対する検索クエリやグループ内の検索で使用する読み取り専用のユーザアカウント。	バインドパスワード (オプション)
バインドアカウントのパスワード (このフィールドはバインドアカウントを入力した場合に表示されます)。	保存する前にサーバ接続をテストします
システムがLDAPサーバの設定と通信できることを確認します。[保存 (Save)] をクリックすると、テストが実行されます。このチェックボックスをオンにした場合、テストに失敗すると設定は変更されません。設定を編集するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。	権限の設定

設定	説明
検索ベースDN	ユーザを検索するLDAPコンテキスト。通常は、の形式です CN=Users, DC=cpsc, DC=local。
ユーザー名属性	認証用のユーザIDにバインドされた属性。例: 「sAMAccountName」。
グループ属性	グループとロールのマッピングに使用される、ユーザのグループ属性のリスト。例: memberOf, managedObjects`

6. [役割マッピング]タブで、目的のマッピングを変更します。

フィールドの詳細

設定	説明
マッピング	グループDN
マッピングするLDAPユーザグループのドメイン名。正規表現がサポートされます。正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュ (\) でエスケープする必要があります。	
<code>\.[]{}()&lt;&gt;*+.= ! ? ^ \$</code>	
ロール	<p>グループDNにマッピングするロール。このグループに含めるロールを個別に選択する必要があります。MonitorロールはSANtricity Unified Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。ロールには次のものがあります。</p> <ul style="list-style-type: none"> <li>• * Storage admin *--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません</li> <li>• * Security admin *--アクセス管理と証明書管理のセキュリティ設定へのアクセス。</li> <li>• * Support admin *--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。</li> <li>• *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。</li> </ul>



Monitorルールは、管理者を含むすべてのユーザに必要です。

7. 必要に応じて、\*別のマッピングを追加\*をクリックして、グループとロールのマッピングをさらに入力します。
8. [保存 ( Save ) ]をクリックします。

#### 結果

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザセッションのみが保持されます。

### ディレクトリサーバを削除します

ディレクトリサーバとWebサービスプロキシの間の接続を解除するには、アクセス管理ページからサーバ情報を削除します。このタスクは、新しいサーバを設定して古いサーバを削除する場合などに実行します。

#### 作業を開始する前に

Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

#### このタスクについて

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザセッションのみが保持されます。

#### 手順

1. アクセス管理\*を選択します。
2. [ディレクトリサービス]タブを選択します。
3. リストから、削除するディレクトリサーバを選択します。
4. [削除 ( Remove ) ]をクリックします。

[ディレクトリサーバーの削除]ダイアログボックスが開きます。

5. フィールドに「remove」と入力し、「\* Remove \*」をクリックします。

ディレクトリサーバの構成設定、権限設定、およびロールのマッピングが削除されます。ユーザは、このサーバからのクレデンシャルを使用してログインできなくなります。

## SAMLを使用する

### SANtricity Unified ManagerでSAMLを設定する

アクセス管理の認証を設定する場合、ストレージレイに組み込みのSecurity Assertion Markup Language (SAML) 機能を使用することができます。この設定により、アイデンティティプロバイダとストレージプロバイダの間の接続が確立されます。

作業を開始する前に

- Security Adminの権限を含むユーザプロフィールでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ストレージレイのコントローラのIPアドレスまたはドメイン名を確認しておく必要があります。
- IdP管理者がIdPシステムの設定を完了している必要があります。
- IdP管理者が、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。
- IdPサーバとコントローラのクロックが同期されていることを確認しておきます（NTPサーバを使用するかコントローラのクロックの設定を調整します）。
- IdPのメタデータファイルをIdPシステムからダウンロードし、Unified Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。

このタスクについて

アイデンティティプロバイダ（IdP）は、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するために使用される外部のシステムです。多要素認証にも対応し、Active Directoryなどの任意のユーザデータベースを使用するように設定できます。IdPの保守はセキュリティチームが行います。サービスプロバイダ（SP）は、ユーザの認証とアクセスを制御するシステムです。アクセス管理にSAMLを設定すると、ストレージレイがアイデンティティプロバイダに認証を要求するサービスプロバイダとして機能します。IdPとストレージレイの間の接続を確立するには、この2つのエンティティ間でメタデータファイルを共有します。その後、IdPのユーザエンティティをストレージレイのロールにマッピングします。最後に、接続とSSOログインをテストしたうえでSAMLを有効にします。



- SAMLとディレクトリサービス\*。認証方式としてディレクトリサービスを設定している場合にSAMLを有効にすると、Unified ManagerではSAMLがディレクトリサービスよりも優先されます。あとでSAMLを無効にすると、元の設定に戻ってディレクトリサービスが使用されます。



- SAMLを編集および無効化しています。\* SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

SAML認証の設定は複数の手順からなる手順です。

手順1：IdPのメタデータファイルをアップロードする

ストレージレイにIdPの接続情報を提供するには、Unified ManagerにIdPメタデータをインポートします。このメタデータは、IdPシステムが認証要求を正しいURLにリダイレクトし、受信した応答を検証するために必要です。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML \*タブを選択します。

設定手順の概要が表示されます。

3. アイデンティティプロバイダ（IdP）ファイルのインポート\*リンクをクリックします。

アイデンティティプロバイダファイルのインポートダイアログボックスが開きます。

4. Browse \*をクリックして、ローカルシステムにコピーしたIdPメタデータファイルを選択してアップロードします。

ファイルを選択すると、IdPのエンティティIDが表示されます。

5. [\* インポート \*]をクリックします。

## 手順2：サービスプロバイダのファイルをエクスポートする

IdPとストレージレイの間の信頼関係を確立するために、サービスプロバイダのメタデータをIdPにインポートします。このメタデータは、IdPがコントローラとの信頼関係を確立し、許可要求を処理するために必要です。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPがサービスプロバイダと通信するために必要な情報が含まれています。

### 手順

1. [サービスプロバイダファイルのエクスポート\*]リンクをクリックします。

[Export Service Provider Files]ダイアログボックスが開きます。

2. コントローラのIPアドレスまたはDNS名を[\*コントローラA\*]フィールドに入力し、[\*エクスポート]をクリックしてメタデータファイルをローカルシステムに保存します。

「\* Export」をクリックすると、サービスプロバイダのメタデータがローカルシステムにダウンロードされます。ファイルの保存先をメモします。

3. ローカルシステムで、エクスポートしたXML形式のサービスプロバイダメタデータファイルを探します。
4. IdPサーバから、サービスプロバイダのメタデータファイルをインポートして信頼関係を確立します。ファイルを直接インポートすることも、ファイルからコントローラ情報を手動で入力することもできます。

## 手順3：ロールをマッピングする

Unified Managerへのアクセスをユーザに許可するには、IdPユーザの属性とグループメンバーシップをストレージレイの事前定義されたロールにマッピングする必要があります。

### 作業を開始する前に

- IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- IdPのメタデータファイルをUnified Managerにインポートします。
- コントローラのサービスプロバイダメタデータファイルが、信頼関係のIdPシステムにインポートされている。

### 手順

1. 「mapping Unified Manager \* roles」のリンクをクリックします。

ロールマッピング(Role Mapping)ダイアログボックスが開きます

2. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。

## フィールドの詳細

設定	説明
マッピング	ユーザー属性
マッピングするSAMLグループの属性 (「member of」など) を指定します。	属性値
マッピングするグループの属性値を指定します。正規表現がサポートされます。正規表現パターンの一部でない場合は、これらの特殊な正規表現文字をバックスラッシュ (「\」) でエスケープする必要があります	ロール



Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

- 必要に応じて、\*別のマッピングを追加\*をクリックして、グループとロールのマッピングをさらに入力します。



ロールのマッピングは、SAMLを有効にしたあとに変更できます。

- マッピングが終了したら、\*保存\*をクリックします。

### 手順4：SSOログインをテストする

IdPシステムとストレージレイが通信できることを確認するために、必要に応じてSSOログインをテストできます。このテストは、SAMLを有効にする最後の手順でも実行します。

作業を開始する前に

- IdPのメタデータファイルをUnified Managerにインポートします。
- コントローラのサービスプロバイダメタデータファイルが、信頼関係のIdPシステムにインポートされている。

手順

- [Test SSO Login\*]リンクを選択します。

SSOクレデンシャルを入力するためのダイアログボックスが表示されます。

- Security AdminとMonitorの両方の権限を持つユーザのログインクレデンシャルを入力します。

ログインのテストを実行している間、ダイアログボックスが開きます。

3. テストに成功したことを示すメッセージを確認します。テストに成功した場合は、SAMLを有効にする次の手順に進みます。

テストが正常に完了しない場合は、エラーメッセージに詳細が表示されます。次の点を確認してください。

- ユーザがSecurity AdminとMonitorの権限を持つグループに属していること。
- アップロードしたIdPサーバのメタデータが正しいこと。
- SPメタデータファイル内のコントローラアドレスが正しい。

#### 手順5：SAMLを有効にする

最後に、ユーザ認証用のSAMLの設定を完了します。このプロセスでは、SSOログインのテストも求められます。SSOログインのテストプロセスについては、前の手順で説明したとおりです。

作業を開始する前に

- IdPのメタデータファイルをUnified Managerにインポートします。
- コントローラのサービスプロバイダメタデータファイルが、信頼関係のIdPシステムにインポートされている。
- 少なくともMonitorロールとSecurity Adminロールを1つずつマッピングしておきます。



- SAMLを編集および無効化しています。\* SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

手順

1. [\* SAML]タブで、[SAMLを有効にする]リンクを選択します。

[Confirm Enable SAML (SAMLを有効にする)]ダイアログボックスが開きます。

2. 「enable」と入力し、「\* Enable」をクリックします。
3. SSOログインのテスト用にユーザクレデンシャルを入力します。

結果

SAMLが有効になると、アクティブなセッションはすべて終了され、SAMLを使用したユーザの認証が開始されます。

## SANtricity Unified Manager で SAML ロール マッピングを変更する

アクセス管理にSAMLを設定している場合、IdPグループとストレージレイの事前定義されたロールとの間のロールマッピングを変更できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

- IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- SAMLを設定して有効にします。

#### 手順

1. メニューを選択します。Settings [Access Management]。
2. SAML \*タブを選択します。
3. [役割のマッピング]を選択します。

ロールマッピング(Role Mapping)ダイアログボックスが開きます

4. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。



SAMLが有効になっている間は権限を削除しないように注意してください。削除すると、Unified Managerにアクセスできなくなります。

#### フィールドの詳細

設定	説明
マッピング	ユーザー属性
マッピングするSAMLグループの属性（「member of」などを指定します。	属性値
マッピングするグループの属性値を指定します。	ロール



Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

5. 必要に応じて、\* Add another mapping \*をクリックして、グループとロールのマッピングをさらに入力します。
6. [保存 ( Save ) ]をクリックします。

#### 結果

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザセッションのみが保持されます。

### SANtricity Unified ManagerでSAMLサービスプロバイダーファイルをエクスポートする

必要に応じて、ストレージレイのサービスプロバイダメタデータをエクスポートし、

そのファイルをアイデンティティプロバイダ (IdP) システムに再インポートできます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- SAMLを設定して有効にします。

このタスクについて

このタスクでは、コントローラからメタデータをエクスポートします。このメタデータは、IdPがコントローラとの信頼関係を確立し、認証要求を処理するために必要です。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPで要求の送信に使用できる情報が含まれています。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML \*タブを選択します。
3. 「書き出し」を選択します。

[Export Service Provider Files]ダイアログボックスが開きます。

4. [エクスポート]\*をクリックして、メタデータファイルをローカルシステムに保存します。



ドメイン名フィールドは読み取り専用です。

ファイルの保存先をメモします。

5. ローカルシステムで、エクスポートしたXML形式のサービスプロバイダメタデータファイルを探します。
6. IdPサーバから、サービスプロバイダのメタデータファイルをインポートします。ファイルを直接インポートすることも、コントローラ情報を手動で入力することもできます。
7. [\* 閉じる \*]をクリックします。

## SANtricity Unified Manager のユーザー アクセス管理に関する FAQ

この FAQ は、質問に対する簡単な回答を探している場合に役立ちます。

ログインできない理由は何ですか？

ログイン試行時にエラーが表示された場合は、次の原因を確認してください。

ログインエラーは、次のいずれかが原因の可能性あります。

- 入力したユーザ名またはパスワードが正しくありません。
- 必要な権限がありません。
- ログインが複数回失敗したために、ロックアウトモードがトリガーされました。10分待ってから再度ログインしてください。

- SAML認証が有効になりました。ログインするには、ブラウザをリフレッシュしてください。

ディレクトリサーバを追加するときは、どのような点に注意する必要がありますか？

アクセス管理でディレクトリサーバを追加する前に、一定の要件を満たす必要があります。

- ユーザグループがディレクトリサービスに定義されている必要があります。
- LDAPサーバのクレデンシャルを確認しておく必要があります。ドメイン名とサーバのURLのほか、必要に応じてバインドアカウントのユーザ名とパスワードも指定できます。
- セキュアなプロトコルを使用するLDAPSサーバの場合は、LDAPサーバの証明書チェーンがローカルマシンにインストールされている必要があります。

ストレージレイのロールをマッピングするときは、どのような点に注意する必要がありますか？

グループをロールにマッピングする前に、ガイドラインを確認してください。

RBAC（ロールベースアクセス制御）機能には次のロールがあります。

- \* Storage admin \*--アレイ上のストレージ・オブジェクトへの読み取り/書き込みのフル・アクセスを提供しますがセキュリティ構成へのアクセスはありません
- \* Security admin \*--アクセス管理と証明書管理のセキュリティ設定へのアクセス。
- \* Support admin \*--ストレージアレイ上のすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。
- \* Monitor \*--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。



Monitorロールは、管理者を含むすべてのユーザに必要です。

LDAP（Lightweight Directory Access Protocol）サーバとディレクトリサービスを使用する場合は、次の点を確認してください。

- ディレクトリサービスでユーザグループを定義しておきます。
- LDAPユーザグループのグループドメイン名を確認しておきます。

## SAML

ストレージアレイに組み込みのSecurity Assertion Markup Language（SAML）機能を使用する場合は、次の点を確認してください。

- アイデンティティプロバイダ（IdP）管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- グループメンバーシップ名を確認しておきます。
- マッピングするグループの属性値を確認しておきます。正規表現がサポートされます。正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュ（「\」）でエスケープする必要があります。

```
\. [ ] { } ( ) < > * + - = ! ? ^ $ |
```

- Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

## SAMLを設定および有効にするときは、どのような点に注意する必要がありますか？

認証のためにSecurity Assertion Markup Language (SAML) の機能を設定して有効にする前に、次の要件を満たしていることを確認し、SAMLの制限事項を理解しておきます。

### 要件

作業を開始する前に、次の点を確認してください。

- ネットワークにアイデンティティプロバイダ (IdP) を設定しておきます。IdPは、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するための外部システムです。IdPの保守はセキュリティチームが行います。
- IdP管理者が、IdPシステムでユーザ属性とユーザグループを設定しておく必要があります。
- IdP管理者が、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。
- IdPサーバとコントローラのクロックが同期されていることを確認しておきます (NTPサーバを使用するかコントローラのクロックの設定を調整します)。
- IdPのメタデータファイルをIdPシステムからダウンロードし、Unified Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。
- ストレージレイのコントローラのIPアドレスまたはドメイン名を確認しておきます。

### 制限事項

上記の要件に加えて、次の制限事項を理解しておく必要があります。

- SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。最後の設定手順でSAMLを有効にする前に、SSOログインをテストすることを推奨します。(SSOログインテストはSAMLが有効になる前にシステムでも実行されます)。
- あとでSAMLを無効にすると、以前の設定 (ローカルユーザロール、ディレクトリサービス、またはその両方) が自動的にリストアされます。
- 現在ユーザ認証にディレクトリサービスが設定されている場合は、SAMLによって上書きされます。
- SAMLを設定すると、次のクライアントがストレージレイリソースにアクセスできなくなります。
  - Enterprise Management Window (EMW)
  - コマンドラインインターフェイス (CLI)
  - ソフトウェア開発キット (SDK) クライアント
  - インバンドクライアント
  - HTTPベーシック認証REST APIクライアント

- 標準のREST APIエンドポイントを使用してログインします

## ローカルユーザとは何ですか？

ローカルユーザは、システムに事前に定義されたユーザで、特定の権限が含まれています。

ローカルユーザの例を次に示します。

- **admin**--システム内のすべての機能にアクセスできるスーパー管理者。このユーザにはすべてのロールが含まれています初回ログイン時にパスワードを設定する必要があります。
- **\* storage \***--すべてのストレージ・プロビジョニングを担当する管理者。このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- **\* security \***--アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザには、Security AdminとMonitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- **\* support \***--ハードウェアリソース、障害データ、ファームウェアアップグレードを担当するユーザー。このユーザには、Support AdminとMonitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- **\* monitor \***--システムへの読み取り専用アクセス権を持つユーザー。このユーザにはMonitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- **\* rw \***（読み取り/書き込み）-このユーザには、Storage Admin、Support Admin、Monitorのロールが含まれています。このアカウントは、パスワードが設定されるまで無効になります。
- **\* ro \***（読み取り専用）--このユーザーには、Monitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効になります。

## 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。