



# アクセス管理

## SANtricity 11.5

NetApp  
February 12, 2024

# 目次

アクセス管理 .....	1
概念 .....	1
方法 .....	7
よくある質問です .....	28

# アクセス管理

## 概念

### アクセス管理の仕組み

アクセス管理は、SANtricity System Managerでユーザ認証を確立する手段の1つです。ユーザは割り当てられたクレデンシャルを使用してシステムにログインする必要があります。

アクセス管理の設定およびユーザ認証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System 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

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。ストレージアレイ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。これはロールベースアクセス制御 (RBAC) 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--ストレージアレイに適用される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プロファイルと、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、ストレージアレイに組み込まれている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アレイの間の通信を確立し、ストレージア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. ユーザにSystem Managerのログインクレデンシャルを渡します。
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。



認証がSAMLとシングルサインオン (SSO) で管理されている場合は、System Managerのログインダイアログが省略されることがあります。

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タスクにユーザがアクセスできるようになります。
- インターフェイスの右上にユーザ名が表示されます。

## System Managerで実行できるタスク

タスクへのアクセス権は、ユーザに割り当てられている次のロールによって異なります。

- \* Storage admin \*--ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。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、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMBOL）のオン/オフの切り替え機能。
- \* Support admin \*--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。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。

使用できないタスクは、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。たとえば、Monitorロールを持つユーザは、ボリュームに関するすべての情報を表示できますが、そのボリュームを変更するための機能にはアクセスできません。[サービスのコピー]や[ワークロードへの追加]などの機能のタブはグレー表示され、[設定の表示/編集]のみが使用できます。

## SANtricity Storage Managerへのユーザアクセス

ローカルユーザロールとディレクトリサービスが設定されている場合は、Enterprise Management Window (EMW) で次のいずれかの機能を実行する前に、クレデンシャルを入力する必要があります。

- ストレージアレイの名前を変更しています
- コントローラファームウェアをアップグレード中です
- ストレージアレイ構成をロードしています
- スクリプトを実行する
- 未使用のセッションがタイムアウトしたときにアクティブな処理を実行しようとしています

ストレージアレイにSAMLが設定されている場合、ユーザはEMWを使用してそのアレイのストレージを検出または管理することはできません。

## アクセス管理の用語

ストレージアレイ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。

期間	説明
できます	<p>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。</p>
証明書	<p>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。</p>
IdP	<p>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。</p>
LDAP	<p>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。</p>
RBAC	<p>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。ストレージレイにはRBACが適用され、事前定義されたロールが用意されています。</p>
SAML	<p>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みのSAML機能は、SAML2.0のアイデンティティアサーション、認証、および許可に準拠しています。</p>
SP	<p>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。</p>

期間	説明
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。

## マッピングされたロールの権限

ストレージアレイに組み込みの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プロファイルが含まれています。各ロールには、SANtricity System 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。

ユーザプロファイルとマッピングされたロールには、どちらかのSystem Managerのユーザインターフェイスで設定（Access Management > ローカルユーザロール）のメニューからアクセスできます。

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 \*--ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。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、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMBOL）のオン/オフの切り替え機能。
- \* Support admin \*--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。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。

ユーザに特定のタスクに対する権限がない場合、そのタスクはグレー表示されるか、ユーザインターフェイスに表示されません。

## ローカルユーザロールを使用したアクセス管理

管理者は、ストレージアレイに組み込みのロールベースアクセス制御（RBAC）機能をアクセス管理に使用できます。これらの機能のことを「ローカルユーザロール」と呼びます。

### 設定ワークフロー

ローカルユーザロールはストレージアレイに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SANtricity System 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。

## ディレクトリサービスを使用したアクセス管理

管理者は、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）をアクセス管理に使用できます。

### 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SANtricity System 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サーバとストレージレイ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、ユーザグループをストレージレイの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サーバとストレージレイ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。

## 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ィールでSystem 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、System 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、ストレージア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。通信を設定するには、System Managerを使用して、各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。その後、IdPシステムからそれらの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. ストレージアレイのルールをIdPで定義されているユーザ属性にマッピングします。これを行うには、管理者はSystem 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、ストレージアレイと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. System Managerから、ストレージアレイの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。

- 新しいル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、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

## 方法

### ローカルユーザロールを表示します

[ローカルユーザーの役割]タブでは、ユーザープロファイルとデフォルトの役割のマッピングを表示できます。これらのマッピングは、ストレージレイに適用されたロールベースアクセス制御 (RBAC) 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

ユーザプロファイル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. メニューを選択します。Settings [Access Management]。
2. [ローカルユーザー役割\* (Local User Roles \*) ]タブを選択します。

ユーザプロファイルが表に表示されます。

- \* Root admin \*(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。このユーザプロファイルにはすべてのロールが含まれています。
- \* Storage admin \* (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。このユーザプロファイルには、Storage Admin、Support Admin、Monitorの各ロールが含まれています。
- \* Security admin \* (security) --アクセス管理、証明書管理、セキュリティ有効ドライブ機能など、セキュリティ構成を担当するユーザー。このユーザプロファイルには、Security AdminとMonitorの各ロールが含まれています。
- \* Support admin\*(support)--ハードウェアリソース'障害データ'ファームウェアのアップグレードを担当するユーザーこのユーザプロファイルには、Support AdminとMonitorの各ロールが含まれています。
- **Monitor**(モニタ)--システムへの読み取り専用アクセス権を持つユーザ。このユーザプロファイルには、Monitorロールのみが含まれています。

## パスワードを変更します

アクセス管理で各ユーザプロファイル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。



System Managerでパスワードを変更すると、コマンドラインインターフェイス (CLI) のパスワードも変更されます。また、パスワードは、ユーザのアクティブなセッションを終了するために原因を変更します。

手順

1. メニューを選択します。Settings [Access Management]。
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\* (Change Password \*) 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の最低文字数が設定されていない場合は、選択したユーザがパスワードを入力しないとストレージレイにアクセスできないようにするオプションのチェックボックスをオンにし、そのユーザの新しいパスワードを入力します。
6. ローカル管理者パスワードを入力し、\* Change \*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。

ローカルユーザパスワードの設定を変更します

ストレージレイで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ストレージレイ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ストレージレイ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. メニューを選択します。Settings [Access Management]。
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」 ボタンを選択します。

[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ストレージレイ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少なくとも必要とする」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オンにしてから、スピンド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。

## ディレクトリサーバを追加します

アクセス管理用に認証を設定するには、ストレージレイとLDAPサーバの間の通信を確立し、LDAPユーザグループをレイの事前定義された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LDAP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ストレージレイの事前定義されたロールにマッピングします。



手順でLDAPサーバを追加すると、従来の管理インターフェイスは無効になります。従来の管理インターフェイス (SYMbol) は、ストレージレイと管理クライアントの間の通信に使用される方法です。無効にすると、ストレージレイと管理クライアントはより安全な通信方法 (HTTPS経由のREST API) を使用します。

#### 手順

1. メニューを選択します。Settings [Access Management]。
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
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。	サーバURL
LDAPサーバにアクセスするためのURLを' <i>ldap[s]://host:port</i> 'の形式で入力します	証明書のアップロード（オプション）
<div data-bbox="245 716 302 772" style="border: 1px solid black; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin-bottom: 10px;"> <span style="font-size: 18px; color: blue;">i</span> </div> <p>このフィールドは、上記のサーバURLフィールドにLDAPS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> <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）
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=c poc、DC=local」などと入力します。	バインドパスワード（オプション）
<div data-bbox="245 1373 302 1430" style="border: 1px solid black; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin-bottom: 10px;"> <span style="font-size: 18px; color: blue;">i</span> </div> <p>このフィールドは、上記のバインドアカウントを入力した場合に表示されます。</p> <p>バインドアカウントのパスワードを入力します。</p>	追加する前にサーバ接続をテストします

設定	説明
入力したLDAPサーバの設定でストレージアレイ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。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。	権限の設定
検索ベースDN	ユーザーを検索するLDAPコンテキストを入力します通常は'CN=Users'DC=copc'DC=local'の形式で入力します
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`

- [ロールマッピング]タブをクリックします。
- 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。

#### 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ユーザグループの識別名 (DN) 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ロールがないユーザの場合、System Managerは正常に動作しません。

- 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。
- 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。

## ディレクトリサーバ設定とロールマッピングを編集します

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. メニューを選択します。Settings [Access Management]。
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。

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せん。	サーバURL
LDAPサーバにアクセスするためのURL。形式は「 <i>ldap[s]://host:port</i> 」です。	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せん)。	保存する前にサーバ接続をテストします

設定	説明
ストレージレイがLDAPサーバの設定と通信できることを確認します。テストは、ダイアログボックスの下部にある「保存」をクリックすると実行されます。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
検索ベースDN	ユーザを検索するLDAPコンテキスト。通常は「CN=Users」、DC=copc、DC=local」の形式で入力します。
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。

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。	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ロールがないユーザの場合、System Managerは正常に動作しません。

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ストレージレイ間の接続を解除するために、アクセス管理ページからサーバ情報を削除できます。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. メニューを選択します。Settings [Access Management]。
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。

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使用するように設定されている状況でSAMLを有効にした場合、System 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
- 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
- 手順3：ロールをマッピングする
- 手順4：SSOログインをテストする
- 手順5：SAMLを有効にする

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、System ManagerにIdPのメタデータをインポートします。

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。
- 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を同期しておきます（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、System 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

このタスクでは、IdPのメタデータファイルをSystem Managerにアップロードします。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。コントローラが2台ある場合でも、アップロードするメタデータファイルはストレージレイに対して1つだけです。

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。

作業を開始する前に

- ストレージレイの各コントローラのIPアドレスまたはドメイン名を確認しておきます。

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（コントローラごとに1ファイル）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間の信頼関係を確立し、許可要求を処理するために必要になります。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。

サービスプロバイダファイルのエクスポート\*ダイアログが開きます。

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。ストレージレイにコントローラが2台ある場合は、2台目のコントローラの Controller B \*フィールドでこの手順を繰り返します。

Export（エクスポート）をクリックすると、サービスプロバイダ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、エクスポートしたサービスプロバイダのメタデータファイルを探します。

コントローラごとにXML形式のファイルが1つあります。

4. IdPサーバで、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の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

System Managerに対する許可とアクセスをユーザに提供するには、IdPユーザ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System Managerにインポートしておきます。
- 各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IdPシステムにインポートして信頼関係を確立しておきます。

このタスクについて

このタスクでは、System Managerを使用してIdP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. System Managerのロールをマッピングするためのリンクをクリックします。

[役割マッピング (\* 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。	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ロールがないユーザの場合、System Managerは正常に動作しません。

3. 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。

4. 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System Managerにインポートしておきます。
- 各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IdPシステムにインポートして信頼関係を確立しておきます。

手順

1. [Test SSO Login\*]リンクを選択します。

SSOクレデンシャルの入力を求めるダイアログが表示されます。

2. 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。

ログインのテスト中にダイアログが開きます。

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のアドレスが正しいこと。

#### 手順5：SAMLを有効にする

最後の手順として、SAMLユーザ認証を有効にします。

作業を開始する前に

- IdPのメタデータファイルをSystem Managerにインポートしておきます。
- 各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IdPシステムにインポートして信頼関係を確立しておきます。
- 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。

このタスクについて

このタスクでは、ユーザ認証のSAMLの設定を終了する方法について説明します。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。



- 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 \*]ダイアログが開きます。

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。

#### SAMLの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。

[役割マッピング (\* 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とき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、System 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ロールがないユーザの場合、System Managerは正常に動作しません。

5. オプション： 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。

## SAML サービスプロバイダ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のメタデータをエクスポートし

て、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することができます。

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。
- 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 (コントローラごとに1ファイル) 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間の信頼関係を確立し、認証要求を処理するために必要になります。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。

サービスプロバイダファイルのエクスポート\*ダイアログが開きます。

4. 各コントローラについて、\* Export (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。



各コントローラの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、エクスポートしたサービスプロバイダのメタデータファイルを探します。

コントローラごとにXML形式のファイルが1つあります。

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、ファイルからコントローラの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。

監査ログアクティビティを表示します

Security Admin権限を持つユーザは、監査ログを表示して、ユーザによる操作、認証エラー、無効なログインの試行、およびユーザセッションの期間を監視できます。

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。

手順

1. メニューを選択します。Settings [Access Management]。

2. [監査ログ]タブを選択します。




\*監査ログ\*アクティビティは表形式で表示されます。この表には、次の情報列が含まれます。

- 日付/時刻--ストレージレイがイベントを検出した日時 (GMT) のタイムスタンプ
- ユーザー名--イベントに関連付けられたユーザー名。ストレージレイに対して認証されていない操作が実行された場合は、「N/A」と表示されます。内部プロキシまたはその他のメカニズムによって、認証されていないアクションがトリガーされることがあります。
- ステータスコード--操作のHTTPステータスコード(200、400など)およびイベントに関連する説明テキスト。
- **URL**アクセス--完全なURL (ホストを含む)とクエリ文字列。
- クライアント**IP**アドレス--イベントに関連付けられたクライアントのIPアドレス。
- **Source**--イベントに関連付けられたログインソース。System Manager、CLI、Webサービス、またはサポートシェルがあります。

3. [監査ログ]ページの選択項目を使用して、イベントを表示および管理します。



## 選択の詳細

選択 (Selection)	説明
イベントを表示する期間を選択...	表示されるイベントを日付範囲（過去24時間、過去7日間、過去30日間、またはカスタムの日付範囲）で限定します。
フィルタ	表示されるイベントをフィールドに入力した文字で限定します。単語の完全一致には引用符("")を使用し、1つ以上の単語を返すには「」または「」を入力します。単語を省略するにはダッシュ(--)を入力します。
更新	最新のイベントにページを更新するには、「更新」を選択します。
設定の表示/編集	[表示/設定の編集] を選択すると、ログに記録するフルログポリシーとアクションのレベルを指定できるダイアログボックスが開きます。
イベントを削除します	「削除」を選択すると、ページから古いイベントを削除できるダイアログボックスが開きます。
列の表示/非表示を切り替えます	<p>[列を表示/非表示 (* Show/Hide * Column) ]アイコンをクリックします  をクリックして、表に表示する列を追加で選択します。その他の列には、次のもの</p> <ul style="list-style-type: none"> <li>• メソッド-- HTTPメソッド(POST、GET、削除など)。</li> <li>• <b>CLI</b>コマンド実行-- Secure CLI要求に対して実行されるCLIコマンド(文法)。</li> <li>• <b>CLI</b>戻りステータス-- CLIステータスコードまたはクライアントからの入力ファイルの要求。</li> <li>• *SYMBOL手順*--実行されたSYMBOL手順。</li> <li>• *SSH Event Type*-- Secure Shell (SSH)イベントのタイプ(ログイン、ログアウト、login_failなど)</li> <li>• *SSHセッションPID*-- SSHセッションのプロセスID番号。</li> <li>• <b>SSH</b>セッション期間--ユーザーがログインした秒数</li> </ul>
列フィルタを切り替えます	[切り替え* (Toggle *) ]アイコンをクリックします  をクリックすると、各列のフィルタリングフィールドが開きます。表示されるイベントを特定の文字で限定するには、列フィールドにその文字を入力します。フィルタリングフィールドを閉じるには、アイコンをもう一度クリックします。
変更を元に戻します	[元に戻す (Undo) ]アイコンをクリックします  をクリックすると、テーブルがデフォルトの設定に戻ります。
エクスポート (Export)	[Export]をクリックして、テーブルデータをカンマ区切り値 (CSV) ファイルに保存します。

## 監査ログポリシーを定義する

上書きポリシーや監査ログに記録するイベントのタイプを変更することができます。

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。

このタスクについて

このタスクでは、監査ログの設定を変更する方法について説明します。古いイベントの上書きに関するポリシーや記録するイベントタイプに関するポリシーなどが含まれます。

手順

1. メニューを選択します。Settings [Access Management]。
2. [監査ログ]タブを選択します。
3. 「表示/設定の編集」を選択します。

[**Audit Log Settings** (監査ログ設定)]ダイアログボックスが開きます。

4. 上書きポリシーや記録するイベントのタイプを変更します。

設定	説明
<p>上書きポリシー</p>	<p>最大容量に達したときに古いイベントを上書きするポリシーを指定します。</p> <ul style="list-style-type: none"> <li>• 監査ログがいっぱいになったらイベントを古いものから上書きする-監査ログが50、000レコードに達したときに古いイベントを上書きします。</li> <li>• 監査ログのイベントを手動で削除する必要があります-イベントが自動的に削除されないように指定します。設定した割合に達した場合、しきい値の警告が表示されます。イベントは手動で削除する必要があります。</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> 上書きポリシーを無効にした場合、監査ログのエントリが上限に達すると、Security Adminの権限がないユーザによるSystem Managerへのアクセスは拒否されます。Security Adminの権限がないユーザが再びシステムにアクセスできるようにするには、Security Adminルールが割り当てられているユーザが古いイベントレコードを削除する必要があります。</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> 上書きポリシーは、監査ログをsyslogサーバにアーカイブするように設定されている場合は適用されません。</p> </div>
<p>ログに記録するアクションのレベル</p>	<p>ログに記録するイベントのタイプを指定します。</p> <ul style="list-style-type: none"> <li>• 変更イベントのみを記録する--ユーザーの操作によってシステムに変更が発生するイベントのみを記録します</li> <li>• すべての変更イベントと読み取り専用イベントを記録する--情報の読み取りまたはダウンロードを伴うユーザー操作を含むすべてのイベントを記録します</li> </ul>

5. [ 保存 ( Save ) ] をクリックします。

## 監査ログからイベントを削除します

監査ログの古いイベントをクリアすることができます。これにより、イベントの検索が容易になります。削除時に古いイベントをCSV（カンマ区切り値）ファイルに保存することもできます。

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。

このタスクについて

このタスクでは、監査ログから古いイベントを削除する方法について説明します。

手順

1. メニューを選択します。Settings [Access Management]。
2. [監査ログ]タブを選択します。
3. 「\* 削除」を選択します。

[監査ログの削除]ダイアログボックスが開きます。

4. 削除する古いイベントの数を選択または入力します。
5. 削除したイベントをCSVファイルにエクスポートする場合は、チェックボックスを選択したままにします（推奨）。次の手順で\*削除\*をクリックすると、ファイル名と場所の入力を求められます。イベントをCSVファイルに保存しない場合は、チェックボックスをクリックして選択を解除します。
6. [削除（Delete）]をクリックします。

確認のダイアログボックスが開きます。

7. フィールドに「delete」と入力し、「\* Delete \*」をクリックします。

最も古いイベントは監査ログページから削除されます。

## 監査ログ用のsyslogサーバを設定します

監査ログを外部のsyslogサーバにアーカイブする場合は、そのサーバとストレージアレイの間の通信を設定できます。接続が確立されると、監査ログは自動的にsyslogサーバに保存されます。

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。
- syslogサーバのアドレス、プロトコル、およびポート番号を確認しておく必要があります。サーバアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- サーバがセキュアなプロトコル（TLSなど）を使用している場合は、ローカルシステムに認証局（CA）証明書が配置されている必要があります。CA証明書がWebサイトの所有者を識別することにより、サーバとクライアントの間のセキュアな接続が確立さ

## 手順

1. メニューを選択します。Settings [Access Management]。
2. 監査ログ\*タブで、\* syslogサーバーの設定\*を選択します。

[Configure Syslog Servers]ダイアログボックスが開きます。

3. [追加 (Add) ]をクリックします。

[Add Syslog Server\*]ダイアログボックスが開きます。

4. サーバーの情報を入力し、\*追加\*をクリックします。
  - サーバアドレス—完全修飾ドメイン名'IPv4アドレス'またはIPv6アドレスを入力します
  - Protocol --ドロップダウンリストからプロトコル(TLS、UDP、TCPなど)を選択します。
  - 証明書のアップロード (オプション) -- TLSプロトコルを選択し、署名済みCA証明書をまだアップロードしていない場合は、参照をクリックして証明書ファイルをアップロードします。監査ログは、信頼された証明書がないとsyslogサーバにアーカイブされません。



あとで証明書が無効になると、TLSハンドシェイクは失敗します。その結果、監査ログにエラーメッセージが記録され、syslogサーバにメッセージが送信されなくなります。この問題を解決するには、syslogサーバで証明書を修正してから、メニューの[設定]、[監査ログ]、[ syslogサーバの設定]、[すべてテスト]の順に選択します。

- ポート-- syslog受信機のポート番号を入力します[Add]をクリックすると、[Configure Syslog Servers]\*ダイアログボックスが開き、設定したsyslogサーバがページに表示されます。

5. ストレージレイとのサーバ接続をテストするには、「\*すべてテスト」を選択します。

## 結果

設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。

## 監査ログレコード用のsyslogサーバ設定の編集

監査ログのアーカイブに使用するsyslogサーバの設定を変更したり、サーバ用の新しい認証局 (CA) 証明書をアップロードしたりできます。

### 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。
- syslogサーバのアドレス、プロトコル、およびポート番号を確認しておく必要があります。サーバアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- 新しいCA証明書をアップロードする場合は、ローカルシステムに証明書がある必要があります。

## 手順

1. メニューを選択します。Settings [Access Management]。
2. 監査ログ\*タブで、\* syslogサーバーの設定\*を選択します。

設定されているsyslogサーバがページに表示されます。

3. サーバ情報を編集するには、サーバ名の右側にある\* Edit \* (鉛筆) アイコンを選択し、次のフィールドで必要な変更を行います。
  - サーバアドレス—完全修飾ドメイン名'IPv4アドレス'またはIPv6アドレスを入力します
  - Protocol --ドロップダウンリストからプロトコル(TLS、UDP、TCPなど)を選択します。
  - ポート-- syslog受信機のポート番号を入力します
4. (UDPまたはTCPから) プロトコルをセキュアTLSプロトコルに変更した場合は、[Import Trusted Certificate]をクリックしてCA証明書をアップロードします。
5. ストレージアレイとの新しい接続をテストするには、「\*すべてテスト」を選択します。

## 結果

設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。

## よくある質問です

### ログインできないのはなぜですか？

System Managerにログインする際にエラーが表示される場合は、次の問題がないか確認してください。

System Managerのログインエラーは、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。
- ディレクトリサーバ（設定されている場合）が使用できない可能性があります。その場合は、ローカルユーザロールでログインしてみてください。
- 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。
- ロックアウト状態がトリガーされ、監査ログがいっぱいになった可能性があります。アクセス管理に移動し、監査ログから古いイベントを削除します。
- 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。

ミラーリングタスク用のリモートストレージアレイでログインエラーが発生する場合は、次のいずれかが原因の可能性あります。

- 入力したパスワードが正しくありません。
- 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。
- コントローラで使用されているクライアント接続が最大数に達している。複数のユーザまたはクライアントをチェックしてください。

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、次の要件を満たしていることを確認してください。

- 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、次のガイドラインを確認してください。

ストレージレイに搭載されたロールベースアクセス制御（RBAC）機能には次のロールがあります。

- \* Storage admin \*--ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。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、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMBOL）のオン/オフの切り替え機能。
- \* Support admin \*--ストレージレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。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。

## 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。
- Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

## SAML

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。
- Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System

Managerは正常に動作しません。

この変更の影響を受ける外部管理ツールはどれですか。

管理インターフェイスを切り替える、認証方式にSAMLを使用する、などの特定の変更をSystem Managerで行うと、一部の外部ツールや機能が使用できなくなることがあります。

管理インターフェイス

SANtricity SMI-S ProviderやOnCommand Insight (OCI) などの従来の管理インターフェイス (SYMBOL) と直接通信するツールは、レガシー管理インターフェイスの設定が有効になっていないかぎり機能しません。この設定が無効な場合、従来のCLIコマンドを使用したりミラーリング処理を実行したりすることはできません。

詳細については、テクニカルサポートにお問い合わせください。

### SAML 認証

SAMLが有効な場合、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

詳細については、テクニカルサポートにお問い合わせください。

**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を同期しておきます (NTPサーバを使用するかコントローラのクロック)



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、System 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。
- ストレージレイの各コントローラの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

## 監査ログにはどのようなタイプのイベントが記録されますか？

監査ログには、変更イベント、または変更イベントと読み取り専用イベントの両方を記録できます。

ポリシー設定に応じて、次のタイプのイベントが表示されます。

- 変更イベント--ストレージのプロビジョニングなど、システムへの変更を含む、System Manager内からのユーザーアクション。
- 変更イベントおよび読み取り専用イベント--システムへの変更を伴うユーザー操作、およびボリューム割り当ての表示やダウンロードなどの情報を含むイベント。

## syslogサーバを設定するときは、どのような点に注意する必要がありますか？

監査ログは外部syslogサーバにアーカイブできます。

syslogサーバを設定する際は、次のガイドラインに注意してください。

- サーバのアドレス、プロトコル、ポート番号を確認しておきます。サーバアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。

- サーバがセキュアなプロトコル（TLSなど）を使用している場合は、ローカルシステムに認証局（CA）証明書が配置されている必要があります。CA証明書がWebサイトの所有者を識別することにより、サーバとクライアントの間のセキュアな接続が確立さ
- 設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。
- \*Overwrite Policy\*設定（View/Edit Settingsで利用可能）は、ログがsyslogサーバ設定でどのように管理されるかに影響しません。
- 監査ログは、RFC 5424のメッセージ形式に従います。

**syslog**サーバが監査ログを受信しなくなりました。どうすればよいですか？

syslogサーバにTLSプロトコルを設定している場合、何らかの理由で証明書が無効になるとサーバはメッセージを受信できなくなります。無効な証明書に関するエラーメッセージが監査ログに記録されます。

この問題を解決するには、syslogサーバの証明書を修正する必要があります。有効な証明書チェーンが確立されたら、メニューに移動します。Settings [Audit Log]> Configure Syslog Servers > Test All]。

## 著作権に関する情報

Copyright © 2024 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。