アクセス管理
SANtricity software

NetApp
August 22, 2025

目次

アクセス管理

アクセス管理の概要

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。
- 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：

- "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、[アクセス管理]ページで設定できます。

詳細：

- "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の設定"

概念

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機能します。

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。

   初回ログイン時は、ユーザ名が `admin`自動的に表示され、変更することはできません。`admin`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。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。
   - ローカルユーザーの役割-- 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、設定は必要ありません。
   - 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、LDAPユーザをローカルユーザロールにマッピングします。
   - *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. 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。ログイン中、システムは次のバックグラウンドタスクを実行します。
   - ユーザアカウントに対してユーザ名とパスワードを認証します。
   - 割り当てられたロールに基づいてユーザの権限を決定します。
   - 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

機能にアクセスできるかどうかは、ユーザに割り当てられたロールによって異なります。ロールには次のようなものがあります。

- * 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。

使用できない機能は淡色表示されるか、ユーザインターフェイスに表示されません。

アクセス管理の用語

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	製品説明
Active Directory	Active Directory（AD）は、Windowsドメインネットワーク用にLDAPを使用するMicrosoftのディレクトリサービスです。
バインド	バインド操作は、ディレクトリサーバに対してクライアントを認証するために使用されます。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。
カリフォルニア州	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ドキュメント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、この情報を証明（署名）する信頼されたエンティティのIDが含まれています。
LDAP	Lightweight Directory Access Protocol（LDAP）は、分散されたディレクトリ情報サービスにアクセスして管理するための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を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、個 々 のユーザのロールに基づいてコンピュータリソースまたはネットワークリソースへのアクセスを制御する方法です。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では多要素認証が可能で、ユーザはIDを証明するために2つ以上の項目（パスワードやフィンガープリントなど）を指定する必要があります。ストレージア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	Web Services Proxyは標準のHTTPSメカニズムを介したアクセスを提供し、管理者がストレージアレイの管理サービスを設定できるようにします。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されたユーザが含まれます。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。

各ロールは、次のタスクへのアクセスをユーザに提供します。

- * 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。

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、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には、管理者は次の操作を実行します。

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`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

2. 管理者が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、変更できません。
3. 必要に応じて、管理者は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。
- ユーザがパスワードなしでログインできるようにします。

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、設定は次のように機能します。

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`ユーザには、システム内のすべての機能へのフルアクセス権が付与されます。

2. LDAPサーバの設定を入力します。設定には、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は、LDAPサーバとWeb Services Proxyがインストールされているホスト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ると、管理者は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定義されており、変更することはできません。
5. LDAPサーバとWeb Services Proxyの間の接続をテストします。
6. ユーザは、自分に割り当てられた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します。
- ディレクトリサーバを削除します。
- 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。
- ユーザがパスワードなしでログインできるようにします。

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機能します。

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。

この `admin`ユーザには、System Managerのすべての機能に対するフルアクセスが付与されます。

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の間に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. ストレージアレイのロールを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。このテストでは、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. Unified Managerで、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。

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

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ア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ア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たログイン

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の表示

[ローカルユーザーの役割]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。

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。

タスクの内容

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のみです。

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。

ローカルユーザプロファイルのパスワードの変更

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。

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。

タスクの内容

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（[設定の表示/編集]）以上にする必要があります。
- パスワードは大文字と小文字が区別されます。
- 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注意してください。
- セキュリティを強化するために、15文字以上の英数字を使用し、パスワードを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の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際に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。

ローカルユーザのパスワード設定の変更

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に必要な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。

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。

タスクの内容

ローカルユーザパスワードの最小文字数を設定する際は、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文字に設定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に対してパスワードの最小文字数を設定するには、[Require all local user passwords to be at least]チェックボックスをオンにし、スピンボックスで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

ディレクトリサーバの追加

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。次に、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。

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をローカルマシンにインストールする必要があります。

タスクの内容

ディレクトリサーバの追加は、2つの手順で行います。最初にドメイン名と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は、認証用のCA証明書もアップロードする必要があります（標準の署名機関によって署名されている場合）。バインドアカウントのクレデンシャルがある場合は、ユーザ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	製品説明
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（*username@domain*）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をの形式で入力し`ldap[s]://**host**:*port*`ます。	証明書のアップロード（オプション）
このフィールドは、上記の[Server URL]フィールドで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。 [**Browse**]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。	バインドアカウント（オプション）

設定	製品説明
LDAPサーバに対する検索クエリおよびグループ内の検索に使用する読み取り専用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」の場合は、などの値を入力します `CN=bindacct,CN=Users,DC=cpoc,DC=local`。	バインドパスワード（オプション）
このフィールドは、バインドアカウントを入力すると表示されます。 バインドアカウントのパスワードを入力します。	追加する前にサーバ接続をテストする
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。 このチェックボックスを選択してテストに失敗した場合、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

設定	製品説明
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。

フィールドの詳細

設定	製品説明
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ています。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。\.[]{}()<>*+-=!?^$	
役割	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1つ選択します。このグループに含めるロールをそれぞれ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。 • * 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。

6. 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。
7. マッピングが終了したら、*追加*をクリックします。

   システムによって検証が実行され、ストレージアレイとLDAPサーバが通信できるかどうかが確認されます。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の設定とロールマッピングの編集

アクセス管理でディレクトリサーバをすでに設定している場合は、その設定をいつでも変更できます。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。

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を定義する必要があります。

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	製品説明
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（*username*@*domain*）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（の形式）`ldap[s]://host:port`。	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およびグループ内の検索に使用する読み取り専用ユーザアカウント。	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すると表示されます）。	保存する前にサーバ接続をテストする
システムがLDAPサーバ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選択してテストに失敗した場合、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	製品説明
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=cpoc, DC=local`
ユーザ名属性	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	ユーザのグループ属性のリスト。グループとロールのマッピングに使用されます。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	製品説明
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ています。これらの特殊正規表現文字が正規表現パターンに含まれていない場合は、バックスラッシュ（\）でエスケープする必要があります。 \.[]{}()<>*+-=！？^$	
役割	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それぞれ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。 • * 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。

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。現在のユーザーセッションのみが保持されます。

ディレクトリサーバの削除

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]ページで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たあとに古いサーバを削除する場合に実行できます。

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。

タスクの内容

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。現在のユーザー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. フィールドにと入力し `remove`、*[削除]*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

SAMLの設定

アクセス管理用の認証を設定するには、ストレージアレイに組み込みのSecurity Assertion Markup Language（SAML）機能を使用できます。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。

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。
- ストレージア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。

タスクの内容

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。多要素認証を提供し、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IdPを設定できます。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が設定されている場合、ストレージアレイは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とストレージア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。次に、IdPのユーザエンティティをストレージア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。SAMLをあとで無効にすると、ディレクトリサービスの設定は以前の設定に戻ります。

*編集と無効化。*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。

SAML認証の設定は複数の手順で構成されます。

手順**1**：**IdP**のメタデータファイルをアップロードする

ストレージアレイに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。

   [Import Identity Provider File]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とストレージアレイの間の信頼関係を確立するには、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、IdPがサービスプロバイダと通信できるように、コントローラのドメイン名やIPアドレスなどの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。ファイルが保存されている場所をメモします。

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ア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。

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	製品説明
マッピング	ユーザ属性
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ています。(\`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。\.[]{}()<>*+-=!?^$	
役割	フィールド内をクリックし、属性にマッピングするストレージアレイのロールを1つ選択します。含めるロールをそれぞれ個別に選択する必要があります。MonitorロールはUnified Managerにログインするために必要な他のロールと一緒に指定する必要があります。少なくとも1つのグループにはSecurity Adminロールも必要です。 各ロールの権限は次のとおりです。 • * 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。

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。

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ア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。

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

1. [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開きます。

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は、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かった場合は、エラーメッセージと詳細情報が表示されます。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、前の手順で説明しています。

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。

*編集と無効化。*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。

手順

1. [* SAML]タブで、[SAMLを有効にする]リンクを選択します。

   [SAMLの有効化の確認]ダイアログボックスが開きます。

2. と入力し `enable`、*[有効化]*をクリックします。
3. SSOログインテスト用の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ロールマッピングの変更

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

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	製品説明
マッピング	ユーザ属性
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。	役割

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。現在のユーザー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のエクスポート

必要に応じて、ストレージア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。

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。

タスクの内容

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。

[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。

   ファイルが保存されている場所をメモします。

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。

FAQ

ログインできないのはなぜですか？

ログイン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、次のいずれかの理由で発生する可能性があります。

- 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。
- Privilegesが不十分です。
- ログインに何度も失敗したため、ロックアウトモードがトリガーされました。10分待ってから再ログインしてください。
- SAML認証が有効になりました。ブラウザの表示を更新してログインします。

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をローカルマシンにインストールする必要があります。

ストレージアレイのロールに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。

- 管理者がディレクトリサービスでユーザーグループを定義しました。
- 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がわかっている必要があります。正規表現がサポートされています。(`\`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を設定して有効にするときは、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

開始する前に、次のこと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きます。

- 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。
- ストレージア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いることを確認してください。

- 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。（SAMLを有効にする前にSSOログインのテストも実行されます）。
- 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またはディレクトリサービス）が自動的にリストアされます。
- 現在ユーザ認証用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が設定されている場合、次のクライアントはストレージアレイ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たログイン

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ており、特定の権限が含まれています。

ローカルユーザは次のとおりです。

- **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

商標に関する情報