概念
SANtricity 11.7

NetApp
February 12, 2024

目次

概念

アクセス管理の仕組み

アクセス管理を使用して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ァイルでUnified Managerにログインします。

   初回ログイン時のユーザ名 `admin` は自動的に表示され、変更できません。。 `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あります。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。
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。

アクセス管理の用語

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
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ア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、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。

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、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` ユーザには、システム内のすべての機能へのフルアクセス権があります。

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

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` ユーザには、システム内のすべての機能へのフルアクセス権があります。

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。

著作権に関する情報

商標に関する情報