



概念

SANtricity 11.8

NetApp
December 16, 2024

目次

概念	1
アクセス管理の仕組み	1
アクセス管理の用語	2
マッピングされたロールの権限	3
ローカルユーザロールを使用したアクセス管理	3
ディレクトリサービスを使用したアクセス管理	4
SAMLを使用したアクセス管理	5

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でユーザ認証を確立します。

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

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。

期間	製品説明
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。
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、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 *--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で適用される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。

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で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ィールで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

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権を有し、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権については、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。