# Konzepte

SANtricity 11.8

NetApp
January 31, 2025

# Inhalt

# Konzepte

## Funktionsweise von Access Management

Verwenden Sie Access Management, um die Benutzerauthentifizierung in Unified Manager einzurichten.

### Konfigurationsworkflow

Die Zugriffsmanagement-Konfiguration funktioniert wie folgt:

1. Ein Administrator meldet sich bei Unified Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren enthält.

   Bei der erstmaligen Anmeldung wird der Benutzername `admin` automatisch angezeigt und kann nicht geändert werden. Der `admin` Benutzer hat vollen Zugriff auf alle Funktionen im System. Das Passwort muss bei der ersten Anmeldung festgelegt werden.

2. Der Administrator navigiert zur Zugriffsverwaltung in der Benutzeroberfläche, die vorkonfigurierte lokale Benutzerrollen enthält. Diese Rollen sind eine Implementierung von RBAC-Funktionen (rollenbasierte Zugriffssteuerung).
3. Der Administrator konfiguriert eine oder mehrere der folgenden Authentifizierungsmethoden:
   - **Lokale Benutzerrollen** — Authentifizierung wird über RBAC-Funktionen verwaltet. Lokale Benutzerrollen umfassen vordefinierte Benutzer und Rollen mit bestimmten Zugriffsberechtigungen. Administratoren können diese lokalen Benutzerrollen als einzige Authentifizierungsmethode verwenden oder in Kombination mit einem Verzeichnisdienst verwenden. Es ist keine Konfiguration erforderlich – abgesehen von der Festlegung von Passwörtern für die Benutzer.
   - **Directory Services** — die Authentifizierung wird über einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst verwaltet, z. B. über Microsoft Active Directory. Ein Administrator stellt eine Verbindung zum LDAP-Server her und ordnet die LDAP-Benutzer den lokalen Benutzerrollen zu.
   - **SAML** — Authentifizierung wird über einen Identitäts-Provider (IdP) mit der Security Assertion Markup Language (SAML) 2.0 verwaltet. Ein Administrator stellt die Verbindung zwischen dem IdP-System und dem Storage-Array her und ordnet anschließend die IdP-Benutzer den im Storage-Array eingebetteten lokalen Benutzerrollen zu.
4. Der Administrator stellt Benutzern die Anmeldeinformationen für Unified Manager zur Verfügung.
5. Benutzer melden sich beim System an, indem sie ihre Anmeldedaten eingeben. Während der Anmeldung führt das System die folgenden Hintergrundaufgaben aus:
   - Authentifiziert Benutzernamen und Kennwort anhand des Benutzerkontos.
   - Legt die Berechtigungen des Benutzers basierend auf den zugewiesenen Rollen fest.
   - Bietet dem Benutzer Zugriff auf Funktionen in der Benutzeroberfläche.
   - Zeigt den Benutzernamen im oberen Banner an.

### Funktionen in Unified Manager verfügbar

Der Zugriff auf Funktionen hängt von den zugewiesenen Rollen eines Benutzers ab. Dazu gehören:

- **Storage Admin** — Vollständiger Lese-/Schreibzugriff auf Speicherobjekte auf den Arrays, aber kein Zugriff auf die Sicherheitskonfiguration.
- **Security Admin** — Zugriff auf die Sicherheitskonfiguration in Access Management und Certificate Management.
- **Support Admin** — Zugriff auf alle Hardware-Ressourcen auf Speicher-Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
- **Monitor** — schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Eine nicht verfügbare Funktion ist entweder ausgegraut oder wird in der Benutzeroberfläche nicht angezeigt.

# Terminologie für das Zugriffsmanagement

Erfahren Sie, wie die Bedingungen für das Zugriffsmanagement für Unified Manager gelten.

| Laufzeit | Beschreibung |
|---|---|
| Active Directory | Active Directory (AD) ist ein Microsoft-Verzeichnisdienst, der LDAP für Windows-Domänennetzwerke verwendet. |
| Verbindlich | Bindevorgänge werden zur Authentifizierung von Clients auf dem Verzeichnisserver verwendet. Binding erfordert in der Regel Konto- und Kennwortanmeldeinformationen, aber einige Server erlauben anonyme Bindevorgänge. |
| CA | Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer, die sichere Verbindungen zwischen Clients und Servern ermöglichen. |
| Zertifikat | Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet). |
| LDAP | Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisinformationsdienste und die Wartung. Mit diesem Protokoll können viele verschiedene Anwendungen und Dienste eine Verbindung zum LDAP-Server zur Überprüfung von Benutzern herstellen. |
| RBAC | Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ist eine Methode zur Regulierung des Zugriffs auf Computer- oder Netzwerkressourcen, basierend auf den Rollen einzelner Benutzer. Unified Manager enthält vordefinierte Rollen. |

| Laufzeit | Beschreibung |
| --- | --- |
| SAML | Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für die Authentifizierung und Autorisierung zwischen zwei Einheiten. SAML ermöglicht Multi-Faktor-Authentifizierung, bei der Benutzer zwei oder mehr Elemente zur Identitätsnachweise bereitstellen müssen (z. B. ein Passwort und ein Fingerabdruck). Die in das Storage Array integrierte SAML-Funktion ist mit SAML2.0 zur Identitätsprüfung, Authentifizierung und Autorisierung kompatibel. |
| SSO | Bei Single Sign On (SSO) handelt es sich um einen Authentifizierungsservice, mit dem ein Satz an Anmeldeinformationen auf mehrere Anwendungen zugreifen kann. |
| Web Services Proxy | Der Web Services Proxy, der Zugriff über HTTPS-Standardmechanismen bereitstellt, ermöglicht Administratoren die Konfiguration von Managementservices für Speicher-Arrays. Der Proxy kann auf Windows- oder Linux-Hosts installiert werden. Die Unified Manager-Schnittstelle ist mit dem Web Services Proxy verfügbar. |

# Berechtigungen für zugeordnete Rollen

Die RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen vordefinierte Benutzer, wobei eine oder mehrere Rollen zugewiesen sind. Jede Rolle umfasst Berechtigungen für den Zugriff auf Aufgaben in Unified Manager.

Die Rollen ermöglichen Benutzern den Zugriff auf Aufgaben wie folgt:

- **Storage Admin** — Vollständiger Lese-/Schreibzugriff auf Speicherobjekte auf den Arrays, aber kein Zugriff auf die Sicherheitskonfiguration.
- **Security Admin** — Zugriff auf die Sicherheitskonfiguration in Access Management und Certificate Management.
- **Support Admin** — Zugriff auf alle Hardware-Ressourcen auf Speicher-Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
- **Monitor** — schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Wenn ein Benutzer über keine Berechtigungen für eine bestimmte Funktion verfügt, ist diese Funktion entweder zur Auswahl nicht verfügbar oder wird nicht in der Benutzeroberfläche angezeigt.

# Zugriffsverwaltung mit lokalen Benutzerrollen

Administratoren können RBAC-Funktionen (rollenbasierte Zugriffssteuerung) nutzen, die in Unified Manager durchgesetzt werden. Diese Funktionen werden als „lokale Benutzerrollen“ bezeichnet.

## Konfigurationsworkflow

Lokale Benutzerrollen sind im System vorkonfiguriert. Um lokale Benutzerrollen für die Authentifizierung zu

verwenden, können Administratoren Folgendes tun:

1. Ein Administrator meldet sich bei Unified Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren enthält.

   Der `admin` Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Ein Administrator überprüft die Benutzerprofile, die vordefiniert sind und nicht geändert werden können.
3. Optional weist der Administrator jedem Benutzerprofil neue Passwörter zu.
4. Benutzer melden sich mit ihren zugewiesenen Anmeldedaten am System an.

### Vereinfachtes

Bei der Verwendung von nur lokalen Benutzerrollen für die Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben ausführen:

- Passwörter ändern.
- Legen Sie eine Mindestlänge für Passwörter fest.
- Benutzern erlauben, sich ohne Passwörter anzumelden.

# Zugriffsmanagement mit Verzeichnisdiensten

Administratoren können einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst wie Microsoft Active Directory verwenden.

### Konfigurationsworkflow

Wenn ein LDAP-Server und ein Verzeichnisdienst im Netzwerk verwendet werden, funktioniert die Konfiguration wie folgt:

1. Ein Administrator meldet sich bei Unified Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren enthält.

   Der `admin` Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Der Administrator gibt die Konfigurationseinstellungen für den LDAP-Server ein. Zu den Einstellungen gehören der Domain-Name, die URL und die Bind-Kontoinformationen.
3. Wenn der LDAP-Server ein sicheres Protokoll (LDAPS) verwendet, lädt der Administrator eine Zertifikatskette für die Authentifizierung zwischen dem LDAP-Server und dem Hostsystem, auf dem der Web Services Proxy installiert ist, hoch.
4. Nachdem die Serververbindung hergestellt wurde, ordnet der Administrator die Benutzergruppen den lokalen Benutzerrollen zu. Diese Rollen sind vordefiniert und können nicht geändert werden.
5. Der Administrator testet die Verbindung zwischen dem LDAP-Server und dem Web Services Proxy.
6. Benutzer melden sich mit ihren zugewiesenen LDAP/Directory Services-Anmeldedaten am System an.

### Vereinfachtes

Bei der Verwendung von Verzeichnisdiensten zur Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben ausführen:

- Fügen Sie einen Verzeichnisserver hinzu.
- Bearbeiten der Einstellungen des Verzeichnisservers.
- Zuordnen von LDAP-Benutzern zu lokalen Benutzerrollen.
- Entfernen Sie einen Verzeichnisserver.
- Passwörter ändern.
- Legen Sie eine Mindestlänge für Passwörter fest.
- Benutzern erlauben, sich ohne Passwörter anzumelden.

# Zugriffsmanagement mit SAML

Für die Zugriffsverwaltung können Administratoren die in das Array integrierten Funktionen der Security Assertion Markup Language (SAML) 2.0 verwenden.

### Konfigurationsworkflow

Die SAML-Konfiguration funktioniert wie folgt:

1. Ein Administrator meldet sich bei Unified Manager mit einem Benutzerprofil an, das Sicherheitsadministratorberechtigungen enthält.

   Der `admin` Benutzer hat vollen Zugriff auf alle Funktionen im System Manager.

2. Der Administrator wechselt zur Registerkarte **SAML** unter Zugriffsverwaltung.
3. Ein Administrator konfiguriert die Kommunikation mit dem Identity Provider (IdP). Ein IdP ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert werden und festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Um die Kommunikation mit dem Speicher-Array zu konfigurieren, lädt der Administrator die IdP-Metadatendatei vom IdP-System herunter und lädt die Datei dann mithilfe von Unified Manager auf das Speicher-Array hoch.
4. Ein Administrator stellt eine Vertrauensbeziehung zwischen dem Dienstanbieter und dem IdP her. Ein Dienstanbieter steuert die Benutzerautorisierung. In diesem Fall fungiert der Controller im Speicher-Array als Service Provider. Zum Konfigurieren der Kommunikation verwendet der Administrator Unified Manager, um eine Service Provider-Metadatendatei für den Controller zu exportieren. Vom IdP-System importiert der Administrator dann die Metadatendatei in das IdP.

   Administratoren sollten außerdem sicherstellen, dass das IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.

5. Der Administrator ordnet die Rollen des Storage-Arrays den in IdP definierten Benutzerattributen zu. Dazu verwendet der Administrator Unified Manager zum Erstellen der Zuordnungen.
6. Der Administrator testet die SSO-Anmeldung an der IdP-URL. Dieser Test stellt sicher, dass das Storage-Array und das IdP kommunizieren können.

Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

7. Über Unified Manager aktiviert der Administrator SAML für das Storage-Array.
8. Benutzer melden sich mit ihren SSO-Anmeldedaten am System an.

## Vereinfachtes

Bei der Verwendung von SAML zur Authentifizierung können Administratoren die folgenden Managementaufgaben ausführen:

- Neue Rollenzuordnungen ändern oder erstellen
- Exportieren Sie die Dateien von Dienstanbietern

## Zugriffsbeschränkungen

Wenn SAML aktiviert ist, können Benutzer Speicher für dieses Array nicht über die vorhandene Storage Manager-Schnittstelle ermitteln oder verwalten.

Außerdem können die folgenden Clients nicht auf Services und Ressourcen des Speicherarrays zugreifen:

- Enterprise Management-Fenster (EMW)
- Befehlszeilenschnittstelle (CLI)
- Software Developer Kits (SDK)-Clients
- In-Band-Clients
- REST-API-Clients für die HTTP-Standardauthentifizierung
- Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an