



Zugriffsmanagement

SANtricity 11.8

NetApp
January 31, 2025

Inhalt

- Zugriffsmanagement 1
 - Zugriffsmanagement – Überblick 1
 - Konzepte 1
 - Lokale Benutzerrollen verwenden 7
 - Verzeichnisdienste verwenden 9
 - Verwenden Sie SAML 19
 - FAQs 25

Zugriffsmanagement

Zugriffsmanagement – Überblick

Bei Access Management handelt es sich um eine Methode zur Konfiguration der Benutzerauthentifizierung in Unified Manager.

Welche Authentifizierungsmethoden sind verfügbar?

Folgende Authentifizierungsmethoden sind verfügbar:

- **Lokale Benutzerrollen** — Authentifizierung wird über RBAC-Funktionen (rollenbasierte Zugriffssteuerung) verwaltet. Lokale Benutzerrollen umfassen vordefinierte Benutzerprofile und Rollen mit spezifischen Zugriffsberechtigungen.
- **Directory Services** — die Authentifizierung wird über einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst verwaltet, z. B. über Microsoft Active Directory.
- **SAML** — Authentifizierung wird über einen Identitäts-Provider (IdP) mit SAML 2.0 verwaltet.

Weitere Informationen:

- ["Funktionsweise von Access Management"](#)
- ["Terminologie für das Zugriffsmanagement"](#)
- ["Berechtigungen für zugeordnete Rollen"](#)
- ["SAML"](#)

Wie konfiguriere ich Access Management?

Die SANtricity-Software ist für die Verwendung lokaler Benutzerrollen vorkonfiguriert. Wenn Sie LDAP verwenden möchten, können Sie es auf der Seite Zugriffsverwaltung konfigurieren.

Weitere Informationen:

- ["Zugriffsverwaltung mit lokalen Benutzerrollen"](#)
- ["Zugriffsmanagement mit Verzeichnisdiensten"](#)
- ["SAML konfigurieren"](#)

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.
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.

Laufzeit	Beschreibung
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 Dienst Anbietern

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

Lokale Benutzerrollen verwenden

Zeigen Sie lokale Benutzerrollen an

Auf der Registerkarte Lokale Benutzerrollen können Sie die Zuordnungen der Benutzer zu den Standardrollen anzeigen. Diese Zuordnungen sind Teil der RBAC (rollenbasierte Zugriffssteuerung), die im Web Services Proxy für Unified Manager durchgesetzt wird.

Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Über diese Aufgabe

Die Benutzer und Zuordnungen können nicht geändert werden. Es können nur Passwörter geändert werden.

Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.

Die Benutzer sind in der Tabelle aufgeführt:

- **Admin** — Super-Administrator, der Zugriff auf alle Funktionen im System hat. Dieser Benutzer enthält alle Rollen.
- **Storage** — der Administrator, der für die gesamte Storage-Bereitstellung verantwortlich ist. Dieser Benutzer umfasst die folgenden Rollen: Storage-Administrator, Support-Administrator und Monitor.
- **Sicherheit** — der für die Sicherheitskonfiguration verantwortliche Benutzer, einschließlich Zugriffsverwaltung und Zertifikatverwaltung. Dieser Benutzer umfasst die folgenden Rollen: Security Admin und Monitor.
- **Support** — der Benutzer, der für Hardware-Ressourcen, Ausfalldaten und Firmware-Upgrades verantwortlich ist. Dieser Benutzer enthält die folgenden Rollen: Unterstützen Sie Admin und Monitor.
- **Monitor** — ein Benutzer mit schreibgeschütztem Zugriff auf das System. Dieser Benutzer enthält nur die Rolle „Monitor“.
- **rw** (lesen/schreiben) — dieser Benutzer enthält die folgenden Rollen: Speicheradministrator, Supportadministrator und Monitor.

- **Ro** (schreibgeschützt) — dieser Benutzer enthält nur die Rolle Monitor.

Passwörter für lokale Benutzerprofile ändern

Sie können die Benutzerpasswörter für jeden Benutzer in der Zugriffsverwaltung ändern.

Bevor Sie beginnen

- Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.
- Sie müssen das lokale Administratorkennwort kennen.

Über diese Aufgabe

Beachten Sie bei der Auswahl eines Passworts die folgenden Richtlinien:

- Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Einstellung für ein Mindestpasswort erfüllen oder überschreiten (unter „Einstellungen anzeigen/bearbeiten“).
- Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.
- Nachgestellte Leerzeichen werden nicht aus Kennwörtern entfernt, wenn sie gesetzt sind. Achten Sie darauf, Leerzeichen einzugeben, wenn diese im Passwort enthalten waren.
- Um die Sicherheit zu erhöhen, verwenden Sie mindestens 15 alphanumerische Zeichen, und ändern Sie das Passwort häufig.

Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
3. Wählen Sie einen Benutzer aus der Tabelle aus.

Die Schaltfläche Kennwort ändern steht zur Verfügung.

4. Wählen Sie **Passwort Ändern**.

Das Dialogfeld Kennwort ändern wird geöffnet.

5. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt ist, können Sie das Kontrollkästchen aktivieren, damit der Benutzer ein Passwort für den Zugriff auf das System eingeben muss.
6. Geben Sie das neue Kennwort für den ausgewählten Benutzer in die beiden Felder ein.
7. Geben Sie Ihr lokales Administratorpasswort ein, um diesen Vorgang zu bestätigen, und klicken Sie dann auf **Ändern**.

Ergebnisse

Wenn der Benutzer derzeit angemeldet ist, wird die aktive Sitzung des Benutzers durch die Kennwortänderung beendet.

Ändern Sie die Einstellungen für das lokale Benutzerpasswort

Sie können die erforderliche Mindestlänge für alle neuen oder aktualisierten lokalen Benutzerpasswörter festlegen. Außerdem können lokale Benutzer ohne Eingabe eines Kennworts auf das System zugreifen.

Bevor Sie beginnen

Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.

Über diese Aufgabe

Beachten Sie die folgenden Richtlinien, wenn Sie die Mindestlänge für lokale Benutzerpasswörter festlegen:

- Die Einstellung von Änderungen hat keine Auswirkung auf vorhandene lokale Benutzerpasswörter.
- Die Mindestlänge für lokale Benutzerpasswörter muss zwischen 0 und 30 Zeichen liegen.
- Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Mindestlängeneinstellung erfüllen oder überschreiten.
- Legen Sie keine Mindestlänge für das Passwort fest, wenn lokale Benutzer ohne Eingabe eines Kennworts auf das System zugreifen möchten.

Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
3. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

Das Dialogfeld Einstellungen für das lokale Benutzerpasswort wird geöffnet.

4. Führen Sie einen der folgenden Schritte aus:
 - Um lokalen Benutzern den Zugriff auf das System zu ermöglichen *ohne* ein Passwort einzugeben, deaktivieren Sie das Kontrollkästchen „Alle lokalen Benutzerpasswörter müssen mindestens sein“.
 - Um eine Mindestkennwortlänge für alle lokalen Benutzerpasswörter festzulegen, aktivieren Sie das Kontrollkästchen „Alle lokalen Benutzerpasswörter müssen mindestens sein“. Verwenden Sie dann das Spinner-Feld, um die erforderliche Mindestlänge für alle lokalen Benutzerpasswörter festzulegen.

Neue lokale Benutzerpasswörter müssen die aktuelle Einstellung erfüllen oder überschreiten.

5. Klicken Sie Auf **Speichern**.

Verzeichnisdienste verwenden

Verzeichnisserver hinzufügen

Um die Authentifizierung für die Zugriffsverwaltung zu konfigurieren, stellen Sie eine Kommunikation zwischen einem LDAP-Server und dem Host her, auf dem der Web Services Proxy für Unified Manager ausgeführt wird. Anschließend ordnen Sie die LDAP-Benutzergruppen den lokalen Benutzerrollen zu.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
- LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich Domänenname, Server-URL und optional Benutzername und Kennwort für das Bindekonto.
- Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette des LDAP-Servers auf Ihrem lokalen Computer installiert sein.

Über diese Aufgabe

Das Hinzufügen eines Verzeichnisservers ist ein zweistufiger Prozess. Geben Sie zuerst den Domain-Namen und die URL ein. Wenn Ihr Server ein sicheres Protokoll verwendet, müssen Sie auch ein CA-Zertifikat zur Authentifizierung hochladen, wenn es von einer nicht standardmäßigen Signierungsbehörde signiert ist. Wenn Sie über Anmeldedaten für ein Bindekonto verfügen, können Sie auch Ihren Benutzernamen und Ihr Kennwort eingeben. Als Nächstes werden die Benutzergruppen des LDAP-Servers lokalen Benutzerrollen zugeordnet.

Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie auf der Registerkarte **Directory Services** die Option **Add Directory Server** aus.

Das Dialogfeld Add Directory Server wird geöffnet.

3. Geben Sie auf der Registerkarte **Server-Einstellungen** die Anmeldeinformationen für den LDAP-Server ein.

Felddetails

Einstellung	Beschreibung
Konfigurationseinstellungen	Domäne(en)
Geben Sie den Domännennamen des LDAP-Servers ein. Geben Sie für mehrere Domänen die Domänen in eine kommasetrennte Liste ein. Der Domänenname wird in der Anmeldung (<i>username@Domain</i>) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.	Server-URL
Geben Sie die URL für den Zugriff auf den LDAP-Server in Form von <code>`ldap[s]://host:*port`</code> ein.	Zertifikat hochladen (optional)

Einstellung	Beschreibung
<div data-bbox="245 394 302 453" style="border: 1px solid black; border-radius: 50%; width: 20px; height: 20px; display: flex; align-items: center; justify-content: center; margin-bottom: 10px;"> i </div> <p data-bbox="358 170 480 674">Dieses Feld wird nur angezeigt, wenn ein LDAPS-Protokoll im obigen Feld Server-URL angegeben wird.</p> <p data-bbox="212 726 513 1094">Klicken Sie auf Durchsuchen und wählen Sie ein CA-Zertifikat zum Hochladen aus. Dies ist das vertrauenswürdige Zertifikat oder die Zertifikatskette, die für die Authentifizierung des LDAP-Servers verwendet wird.</p>	<p data-bbox="529 159 821 191">Konto binden (optional)</p>
<p data-bbox="212 1150 513 1766">Geben Sie ein schreibgeschütztes Benutzerkonto ein, um Suchanfragen auf dem LDAP-Server und für die Suche in den Gruppen durchzuführen. Geben Sie den Kontonamen im LDAP-Format ein. Wenn der BIND-Benutzer beispielsweise "bindact" heißt, können Sie einen Wert wie eingeben <code>CN=bindacct,CN=Users,DC=cpoc,DC=local</code>.</p>	<p data-bbox="529 1150 837 1182">Bindepasswort (optional)</p>

Einstellung	Beschreibung
<div style="display: flex; align-items: center;">  <div style="border-left: 1px solid black; padding-left: 10px;"> <p>Dieses Feld wird angezeigt, wenn Sie ein Bindungskonto eingeben.</p> </div> </div> <p>Geben Sie das Passwort für das Bindekonto ein.</p>	<p>Testen Sie die Serververbindung, bevor Sie sie hinzufügen</p>
<p>Aktivieren Sie dieses Kontrollkästchen, wenn Sie sicherstellen möchten, dass das System mit der eingegebenen LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt, nachdem Sie unten im Dialogfeld auf Hinzufügen geklickt haben.</p> <p>Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht hinzugefügt. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration hinzuzufügen.</p>	<p>Berechtigungseinstellungen</p>
<p>Basis-DN suchen</p>	<p>Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise in Form von CN=Users, DC=cpoc, DC=local.</p>
<p>Attribut Benutzername</p>	<p>Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID gebunden ist. Zum Beispiel: sAMAccountName.</p>

Einstellung	Beschreibung
Gruppenattribut(e)	Geben Sie eine Liste der Gruppenattribute für den Benutzer ein, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Zum Beispiel: <code>memberOf, managedObjects</code> .

- Klicken Sie auf die Registerkarte **Rollenzuordnung**.
- Weisen Sie den vordefinierten Rollen LDAP-Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

Felddetails

Einstellung	Beschreibung
Zuordnungen	Gruppen-DN
Geben Sie den Group Distinguished Name (DN) für die zugeordnete LDAP-Benutzergruppe an. Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich (\) entgangen werden, wenn sie nicht Teil eines regulären Ausdrucksmusters sind: <code>\.[]{}()<>*+ -= !? ^</code>	Rollen



Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich.

- Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.
- Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf **Hinzufügen**.

Das System führt eine Validierung durch und stellt sicher, dass das Speicher-Array und der LDAP-Server kommunizieren können. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die im Dialogfeld eingegebenen Anmeldeinformationen, und geben Sie die Informationen ggf. erneut ein.

Bearbeiten Sie die Einstellungen des Verzeichnisseservers und die Rollenzuordnungen

Wenn Sie zuvor einen Verzeichnisserver in der Zugriffsverwaltung konfiguriert haben, können Sie dessen Einstellungen jederzeit ändern. Zu den Einstellungen gehören die Informationen zur Serververbindung und die Zuordnungen von Gruppen zu Rollen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Ein Verzeichnisserver muss definiert werden.

Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Directory Services** aus.
3. Wenn mehr als ein Server definiert ist, wählen Sie den Server aus der Tabelle aus, den Sie bearbeiten möchten.
4. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

Das Dialogfeld Verzeichnisservereinstellungen wird geöffnet.

5. Ändern Sie auf der Registerkarte **Server-Einstellungen** die gewünschten Einstellungen.

Felddetails

Einstellung	Beschreibung
Konfigurationseinstellungen	Domäne(en)
Der/die Domänenname(n) des/der LDAP-Server(e). Geben Sie für mehrere Domänen die Domänen in eine kommasetrennte Liste ein. Der Domänenname wird in der Anmeldung (<i>username@Domain</i>) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.	Server-URL
Die URL für den Zugriff auf den LDAP-Server in Form von <code>ldap[s]://host:port</code> .	Konto binden (optional)
Das schreibgeschützte Benutzerkonto für Suchabfragen am LDAP-Server und für die Suche in den Gruppen.	Bindepaswort (optional)
Das Kennwort für das Bindekonto. (Dieses Feld wird angezeigt, wenn ein Bindekonto eingegeben wird.)	Testen Sie vor dem Speichern die Serververbindung

Einstellung	Beschreibung
<p>Überprüft, ob das System mit der LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt nach dem Klicken auf Speichern. Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht geändert. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration erneut zu bearbeiten.</p>	<p>Berechtigungseinstellungen</p>
<p>Basis-DN suchen</p>	<p>Der LDAP-Kontext, um nach Benutzern zu suchen, normalerweise in Form von CN=Users, DC=cpoc, DC=local.</p>
<p>Attribut Benutzername</p>	<p>Das Attribut, das zur Authentifizierung an die Benutzer-ID gebunden ist. Zum Beispiel: sAMAccountName.</p>
<p>Gruppenattribut(e)</p>	<p>Eine Liste der Gruppenattribute für den Benutzer, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Zum Beispiel: memberOf, managedObjects.</p>

6. Ändern Sie auf der Registerkarte **Rollenzuordnung** die gewünschte Zuordnung.

Felddetails

Einstellung	Beschreibung
Zuordnungen	Gruppen-DN
Der Domain-Name für die LDAP-Benutzergruppe, die zugeordnet werden soll. Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich (\) entgangen werden, wenn sie nicht Teil eines regulären Ausdrucksmusters sind: <code>\.[]{}()<>*+.=!/?^</code>	Rollen



Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich.

7. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.
8. Klicken Sie Auf **Speichern**.

Ergebnisse

Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

Verzeichnisserver entfernen

Um die Verbindung zwischen einem Verzeichnisserver und dem Web Services Proxy zu unterbrechen, können Sie die Serverinformationen von der Seite Zugriffsverwaltung entfernen. Sie möchten diese Aufgabe möglicherweise ausführen, wenn Sie einen neuen Server konfiguriert haben und den alten dann entfernen möchten.

Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Über diese Aufgabe

Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Directory Services** aus.
3. Wählen Sie in der Liste den Verzeichnisserver aus, den Sie löschen möchten.
4. Klicken Sie Auf **Entfernen**.

Das Dialogfeld Verzeichnisserver entfernen wird geöffnet.

5. Geben Sie das Feld ein `remove`, und klicken Sie dann auf **Entfernen**.

Die Konfigurationseinstellungen des Verzeichnisseservers, die Berechtigungseinstellungen und Rollenzuordnungen werden entfernt. Benutzer können sich nicht mehr mit Anmeldeinformationen von diesem Server anmelden.

Verwenden Sie SAML

SAML konfigurieren

Zum Konfigurieren der Authentifizierung für das Zugriffsmanagement können Sie die im Speicher-Array integrierten SAML-Funktionen (Security Assertion Markup Language) verwenden. Mit dieser Konfiguration wird eine Verbindung zwischen einem Identitätsanbieter und dem Speicheranbieter hergestellt.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Sie müssen die IP-Adresse oder den Domännennamen des Controllers im Speicher-Array kennen.
- Ein IdP-Administrator hat ein IdP-System konfiguriert.
- Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
- Ein Administrator hat sichergestellt, dass der IdP-Server und die Controller-Uhr synchronisiert werden (entweder über einen NTP-Server oder durch Anpassung der Controller-Uhreinstellungen).
- Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, das für den Zugriff auf Unified Manager verwendet wird.

Über diese Aufgabe

Ein Identitäts-Provider (IdP) ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert und festgestellt werden können, ob dieser Benutzer erfolgreich authentifiziert wurde. Der IdP kann so konfiguriert werden, dass er Multi-Faktor-Authentifizierung bietet und eine beliebige Benutzerdatenbank, wie z. B. Active Directory, verwendet. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich. Ein Service-Provider (SP) ist ein System, das die Benutzerauthentifizierung und den Zugriff steuert. Wenn Access Management mit SAML konfiguriert ist, fungiert das Storage-Array als Dienstanbieter für die Anforderung der Authentifizierung vom Identity Provider. Um eine Verbindung zwischen dem IdP und dem Storage-Array herzustellen, teilen Sie Metadatendateien zwischen diesen beiden Einheiten gemeinsam. Als Nächstes ordnen Sie die IdP-Benutzereinheiten den Storage-Array-Rollen zu. Und schließlich testen Sie die Verbindung und SSO-Anmeldedaten, bevor Sie SAML aktivieren.



SAML und Directory Services. Wenn Sie SAML aktivieren, wenn die Verzeichnisdienste als Authentifizierungsmethode konfiguriert sind, ersetzt SAML die Verzeichnisdienste in Unified Manager. Wenn Sie SAML später deaktivieren, wird die Konfiguration der Verzeichnisdienste wieder in die vorherige Konfiguration zurückgeführt.



Bearbeiten und Deaktivieren. 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.

Die Konfiguration der SAML-Authentifizierung erfolgt in mehreren Schritten.

Schritt 1: Laden Sie die IdP-Metadatendatei hoch

Um IdP-Verbindungsinformationen für das Storage-Array bereitzustellen, importieren Sie IdP-Metadaten in Unified Manager. Das IdP-System benötigt diese Metadaten, um Authentifizierungsanforderungen an die richtige URL weiterzuleiten und die erhaltenen Antworten zu validieren.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **SAML**.

Auf der Seite wird eine Übersicht der Konfigurationsschritte angezeigt.

3. Klicken Sie auf den Link * Import Identity Provider (IdP) file*.

Das Dialogfeld „Datei des Identitätsanbieters importieren“ wird geöffnet.

4. Klicken Sie auf **Durchsuchen**, um die IdP-Metadatendatei auszuwählen und auf Ihr lokales System hochzuladen.

Nach der Auswahl der Datei wird die IdP-Entity-ID angezeigt.

5. Klicken Sie Auf **Import**.

Schritt 2: Exportieren Sie die Dateien des Dienstanbieters

Um eine Vertrauensbeziehung zwischen dem IdP und dem Storage-Array herzustellen, importieren Sie die Metadaten des Service-Providers in das IdP. Das IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zum Controller herzustellen und Autorisierungsanforderungen zu verarbeiten. Die Datei enthält Informationen wie den Domännennamen oder die IP-Adresse des Controllers, sodass das IdP mit den Service-Providern kommunizieren kann.

Schritte

1. Klicken Sie auf den Link **Export Service Provider Files**.

Das Dialogfeld Dateien des Dienstanbieters exportieren wird geöffnet.

2. Geben Sie die Controller-IP-Adresse oder den DNS-Namen in das Feld **Controller A** ein, und klicken Sie dann auf **Exportieren**, um die Metadatendatei auf Ihrem lokalen System zu speichern.

Nachdem Sie auf **Export** geklickt haben, werden die Metadaten des Dienstanbieters auf Ihr lokales System heruntergeladen. Notieren Sie sich, wo die Datei gespeichert ist.

3. Suchen Sie vom lokalen System aus die XML-formatierte Service Provider-Metadatendatei, die Sie exportiert haben.
4. Importieren Sie vom IdP-Server die Metadatendatei des Dienstansbieters, um die Vertrauensbeziehung herzustellen. Sie können die Datei entweder direkt importieren oder die Controller-Informationen manuell aus der Datei eingeben.

Schritt 3: Rollen zuordnen

Um Benutzern die Autorisierung und den Zugriff auf Unified Manager zu ermöglichen, müssen Sie die IdP-Benutzerattribute und Gruppenmitgliedschaften den vordefinierten Rollen des Speicherarrays zuordnen.

Bevor Sie beginnen

- Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften im IdP-System konfiguriert.
- Die IdP-Metadatendatei wird in Unified Manager importiert.
- Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für den Controller in das IdP-System importiert.

Schritte

1. Klicken Sie auf den Link für **Mapping Unified Manager-Rollen**.

Das Dialogfeld Rollenzuordnung wird geöffnet.

2. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

Felddetails

Einstellung	Beschreibung
Zuordnungen	Benutzerattribut
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-Gruppe an.	Attributwert
Geben Sie den Attributwert für die zugeordnete Gruppe an. Reguläre Ausdrücke werden unterstützt. Diese Sonderzeichen mit regulären Ausdrücken müssen mit einem umgekehrten Schrägstrich versehen werden(\, wenn sie nicht Teil eines regulären Ausdrucksmusters sind: <code>\.[]{}()<>*+ -=! ? ^</code>	Rollen



Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Unified Manager funktioniert für keinen Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.

3. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.



Rollenzuordnungen können geändert werden, nachdem SAML aktiviert ist.

4. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf **Speichern**.

Schritt 4: SSO-Anmeldung testen

Um sicherzustellen, dass das IdP-System und das Speicherarray kommunizieren können, können Sie optional eine SSO-Anmeldung testen. Dieser Test wird auch während des letzten Schritts zur Aktivierung von SAML durchgeführt.

Bevor Sie beginnen

- Die IdP-Metadatendatei wird in Unified Manager importiert.
- Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für den Controller in das IdP-System importiert.

Schritte

1. Klicken Sie auf den Link **SSO-Login testen**.

Zum Eingeben von SSO-Anmeldedaten wird ein Dialogfeld geöffnet.

2. Geben Sie die Anmeldeinformationen für einen Benutzer mit Sicherheitsadministratorrechten und Überwachungsberechtigungen ein.

Ein Dialogfeld wird geöffnet, während das System die Anmeldung testet.

3. Suchen Sie nach einer Meldung für den erfolgreichen Test. Wenn der Test erfolgreich abgeschlossen wurde, fahren Sie mit dem nächsten Schritt zur Aktivierung von SAML fort.

Wenn der Test nicht erfolgreich abgeschlossen wird, wird eine Fehlermeldung mit weiteren Informationen angezeigt. Stellen Sie sicher, dass:

- Der Benutzer gehört zu einer Gruppe mit Berechtigungen für Security Admin und Monitor.
- Die Metadaten, die Sie für den IdP-Server hochgeladen haben, sind korrekt.
- Die Controller-Adresse in den SP-Metadatendateien ist korrekt.

Schritt 5: SAML aktivieren

Der letzte Schritt besteht darin, die SAML-Konfiguration für die Benutzerauthentifizierung abzuschließen. Während dieses Prozesses werden Sie vom System auch aufgefordert, eine SSO-Anmeldung zu testen. Der SSO-Anmelde-Test wird im vorherigen Schritt beschrieben.

Bevor Sie beginnen

- Die IdP-Metadatendatei wird in Unified Manager importiert.
- Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für den Controller in das IdP-System importiert.
- Mindestens ein Monitor und eine Sicherheitsadministratorzuordnung sind konfiguriert.



Bearbeiten und Deaktivieren. 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.

Schritte

1. Wählen Sie auf der Registerkarte **SAML** den Link **SAML aktivieren**.

Das Dialogfeld SAML aktivieren bestätigen wird geöffnet.

2. Geben Sie, ein `enable` und klicken Sie dann auf **enable**.
3. Geben Sie die Benutzeranmeldeinformationen für einen SSO-Anmeldetest ein.

Ergebnisse

Nachdem das System SAML aktiviert hat, werden alle aktiven Sitzungen beendet und die Authentifizierung von Benutzern über SAML beginnt.

SAML-Rollenzuordnungen ändern

Wenn Sie zuvor SAML für Access Management konfiguriert haben, können Sie die Rollenzuordnungen zwischen den IdP-Gruppen und den vordefinierten Rollen des Speicherarrays ändern.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften im IdP-System konfiguriert.
- SAML wurde konfiguriert und aktiviert.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **SAML**.
3. Wählen Sie **Rollenzuordnung**.

Das Dialogfeld Rollenzuordnung wird geöffnet.

4. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.



Achten Sie darauf, dass Sie Ihre Berechtigungen nicht entfernen, während SAML aktiviert ist, sonst verlieren Sie den Zugriff auf Unified Manager.

Felddetails

Einstellung	Beschreibung
Zuordnungen	Benutzerattribut
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-Gruppe an.	Attributwert
Geben Sie den Attributwert für die zu zugeordnete Gruppe an.	Rollen



Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Unified Manager funktioniert für keinen Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.

5. Klicken Sie optional auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.

6. Klicken Sie Auf **Speichern**.

Ergebnisse

Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

Exportieren Sie SAML-Dienstanbieter-Dateien

Bei Bedarf können Sie Service-Provider-Metadaten für das Speicher-Array exportieren und die Datei erneut in das Identity Provider (IdP)-System importieren.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- SAML wurde konfiguriert und aktiviert.

Über diese Aufgabe

In dieser Aufgabe exportieren Sie Metadaten vom Controller. Das IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zum Controller herzustellen und Authentifizierungsanforderungen zu verarbeiten. Die Datei enthält Informationen wie den Domännennamen des Controllers oder die IP-Adresse, die das IdP zum Senden von Anforderungen verwenden kann.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **SAML**.
3. Wählen Sie **Export**.

Das Dialogfeld Dateien des Dienstanbieters exportieren wird geöffnet.

4. Klicken Sie auf **Export**, um die Metadatendatei auf Ihrem lokalen System zu speichern.



Das Feld für den Domännennamen ist schreibgeschützt.

Notieren Sie sich, wo die Datei gespeichert ist.

5. Suchen Sie vom lokalen System aus die XML-formatierte Service Provider-Metadatendatei, die Sie exportiert haben.
6. Importieren Sie vom IdP-Server die Metadatendatei des Dienstanbieters. Sie können die Datei entweder direkt importieren oder die Controller-Informationen manuell eingeben.
7. Klicken Sie Auf **Schließen**.

FAQs

Warum kann ich mich nicht anmelden?

Wenn Sie bei der Anmeldung einen Fehler erhalten, überprüfen Sie diese möglichen Ursachen.

Aus einem der folgenden Gründe können Anmeldefehler auftreten:

- Sie haben einen falschen Benutzernamen oder ein falsches Passwort eingegeben.
- Sie verfügen über unzureichende Berechtigungen.
- Sie haben mehrmals versucht, sich erfolglos anzumelden, was den Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, bis Sie sich erneut anmelden können.
- SAML-Authentifizierung ist aktiviert. Aktualisieren Sie Ihren Browser, um sich anzumelden.

Was muss ich vor dem Hinzufügen eines Verzeichnisseservers wissen?

Bevor Sie einen Verzeichnisserver in Access Management hinzufügen, müssen Sie bestimmte Anforderungen erfüllen.

- Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
- LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich Domänenname, Server-URL und optional Benutzername und Kennwort für das Bindekonto.
- Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette des LDAP-Servers auf Ihrem lokalen Computer installiert sein.

Was muss ich über die Zuordnung von Speicher-Array-Rollen wissen?

Überprüfen Sie die Richtlinien, bevor Sie Gruppen zu Rollen zuordnen.

Die RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen folgende Rollen:

- **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.



Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich.

Wenn Sie einen LDAP-Server (Lightweight Directory Access Protocol) und Verzeichnisdienste verwenden, stellen Sie sicher, dass:

- Ein Administrator hat im Verzeichnisdienst Benutzergruppen definiert.
- Sie kennen die Gruppen-Domain-Namen für die LDAP-Benutzergruppen.

SAML

Wenn Sie die im Speicher-Array integrierten SAML-Funktionen (Security Assertion Markup Language) verwenden, stellen Sie sicher, dass:

- Ein IdP-Administrator (Identity Provider) hat im IdP-System Benutzerattribute und Gruppenmitgliedschaften konfiguriert.
- Sie kennen die Namen der Gruppenmitgliedschaft.

- Sie kennen den Attributwert für die zu zugeordnete Gruppe. Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich enthoben werden(\, wenn sie nicht Teil eines regulären Ausdrucksmusters sind:

```
\ . [ ] { } ( ) < > * + - = ! ? ^ $ |
```

- Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Unified Manager funktioniert für keinen Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.

Was muss ich vor der Konfiguration und Aktivierung von SAML wissen?

Bevor Sie die SAML-Funktionen (Security Assertion Markup Language) für die Authentifizierung konfigurieren und aktivieren, müssen Sie sicherstellen, dass Sie die folgenden Anforderungen erfüllen und SAML-Einschränkungen verstehen.

Anforderungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- Ein Identitäts-Provider (IdP) ist in Ihrem Netzwerk konfiguriert. Ein IdP ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert werden und festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich.
- Ein IdP-Administrator hat Benutzerattribute und Gruppen im IdP-System konfiguriert.
- Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
- Ein Administrator hat sichergestellt, dass der IdP-Server und die Controller-Uhr synchronisiert werden (entweder über einen NTP-Server oder durch Anpassung der Controller-Uhreinrichtungen).
- Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, auf dem der Zugriff auf Unified Manager erfolgt.
- Sie kennen die IP-Adresse oder den Domain-Namen des Controllers im Speicher-Array.

Einschränkungen

Zusätzlich zu den oben genannten Anforderungen sollten Sie sich mit den folgenden Einschränkungen vertraut machen:

- 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. Es wird empfohlen, die SSO-Anmeldungen zu testen, bevor Sie SAML im letzten Konfigurationsschritt aktivieren. (Das System führt auch einen SSO-Anmeldetest vor Aktivierung von SAML durch.)
- Wenn Sie SAML zukünftig deaktivieren, stellt das System automatisch die vorherige Konfiguration wieder her (lokale Benutzerrollen und/oder Verzeichnisdienste).
- Wenn Verzeichnisdienste derzeit für die Benutzerauthentifizierung konfiguriert sind, überschreibt SAML diese Konfiguration.
- Wenn SAML konfiguriert ist, können die folgenden Clients nicht auf Speicher-Array-Ressourcen 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

Welche lokalen Benutzer gibt es?

Lokale Benutzer sind im System vordefiniert und enthalten bestimmte Berechtigungen.

Zu den lokalen Benutzern gehören:

- **Admin** — Super-Administrator, der Zugriff auf alle Funktionen im System hat. Dieser Benutzer enthält alle Rollen. Das Passwort muss bei der ersten Anmeldung festgelegt werden.
- **Storage** — der Administrator, der für die gesamte Storage-Bereitstellung verantwortlich ist. Dieser Benutzer umfasst die folgenden Rollen: Storage-Administrator, Support-Administrator und Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **Sicherheit** — der für die Sicherheitskonfiguration verantwortliche Benutzer, einschließlich Zugriffsverwaltung und Zertifikatverwaltung. Dieser Benutzer umfasst die folgenden Rollen: Security Admin und Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **Support** — der Benutzer, der für Hardware-Ressourcen, Ausfalldaten und Firmware-Upgrades verantwortlich ist. Dieser Benutzer enthält die folgenden Rollen: Unterstützen Sie Admin und Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **Monitor** — ein Benutzer mit schreibgeschütztem Zugriff auf das System. Dieser Benutzer enthält nur die Rolle „Monitor“. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **rw** (lesen/schreiben) — dieser Benutzer enthält die folgenden Rollen: Speicheradministrator, Supportadministrator und Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **Ro** (schreibgeschützt) — dieser Benutzer enthält nur die Rolle Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.