Zugriffsmanagement

SANtricity 11.7

NetApp
February 12, 2024

Inhalt

Zugriffsmanagement 1
Zugriffsmanagement – Überblick 1
Konzepte 1
Lokale Benutzerrollen verwenden 5
Verzeichnisdienste verwenden 8
FAQs 17

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.

Weitere Informationen:

- "Funktionsweise von Access Management"
- "Terminologie für das Zugriffsmanagement"
- "Berechtigungen für zugeordnete Rollen"

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"

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 ersten Anmeldung wird der Benutzername verwendet `admin` Wird automatisch angezeigt und kann nicht geändert werden. Der `admin` Der 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.
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.
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` Der 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` Der 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.

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 Domänennamen des LDAP-Servers ein. Geben Sie für mehrere Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird in der Anmeldung (*username@Domain*) 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 ein `ldap[s]://**host**:*port*`.	Zertifikat hochladen (optional)

Einstellung	Beschreibung
Dieses Feld wird nur angezeigt, wenn ein LDAPS-Protokoll im obigen Feld Server-URL angegeben wird. 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.	Konto binden (optional)
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 Bindebenutzer beispielsweise „bind-Konto“ heißt, können Sie einen Wert wie eingeben `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Bindepasswort (optional)

Einstellung	Beschreibung
Dieses Feld wird angezeigt, wenn Sie ein Bindungskonto eingeben. Geben Sie das Passwort für das Bindekonto ein.	Testen Sie die Serververbindung, bevor Sie sie hinzufügen
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. 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.	**Berechtigungseinstellungen**
Basis-DN suchen	Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise in Form von `CN=Users, DC=cpoc, DC=local`.
Attribut Benutzername	Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: `sAMAccountName`.

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

4. Klicken Sie auf die Registerkarte **Rollenzuordnung**.
5. 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 zu 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: \.[]{}()<>*+-=!?^	Rollen

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

6. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.
7. 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 Verzeichnisservers 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 kommagetrennte Liste ein. Der Domänenname wird in der Anmeldung (*username@Domain*) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.	Server-URL
Die URL für den Zugriff auf den LDAP-Server in Form von `ldap[s]://host:port`.	Konto binden (optional)
Das schreibgeschützte Benutzerkonto für Suchabfragen am LDAP-Server und für die Suche in den Gruppen.	Bindepasswort (optional)
Das Kennwort für das Bindekonto. (Dieses Feld wird angezeigt, wenn ein Bindekonto eingegeben wird.)	Testen Sie vor dem Speichern die Serververbindung

Einstellung	Beschreibung
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.	**Berechtigungseinstellungen**
Basis-DN suchen	Der LDAP-Kontext für die Suche nach Benutzern, in der Regel in Form von `CN=Users, DC=cpoc, DC=local`.
Attribut Benutzername	Das Attribut, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: `sAMAccountName`.
Gruppenattribut(e)	Eine Liste der Gruppenattribute für den Benutzer, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf, managedObjects`.

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: \.[]{}()<>*+-=!?^	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. Typ `remove` Klicken Sie im Feld auf **Entfernen**.

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

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.

Was muss ich vor dem Hinzufügen eines Verzeichnisservers 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.

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.