



Anleitungen

SANtricity 11.6

NetApp
February 12, 2024

Inhalt

- Anleitungen 1
 - Zeigen Sie lokale Benutzerrollen an 1
 - Passwörter ändern 1
 - Ändern Sie die Einstellungen für das lokale Benutzerpasswort 2
 - Verzeichnisserver hinzufügen 3
 - Bearbeiten Sie die Einstellungen des Verzeichnisseservers und die Rollenzuordnungen 8
 - Verzeichnisserver entfernen 11

Anleitungen

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 SANtricity 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 Zertifikatsverwaltung. 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 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 **Passwort ändern** steht zur Verfügung.

4. Wählen Sie **Passwort Ändern**.

Das Dialogfeld **Passwort 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 **Lokale Benutzerpassworteinstellungen** 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**.

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 SANtricity 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 **Directory Server hinzufügen** 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 kommasetrennte Liste ein. Der Domänenname wird in der Anmeldung (<i>username@Domain</i>) verwendet, um anzugeben, gegen welchen Verzeichnisservers sich authentifizieren soll.	Server-URL
Geben Sie die URL für den Zugriff auf den LDAP-Server in Form von ein <code>ldap[s]://host:port</code> .	Zertifikat hochladen (optional)

Einstellung	Beschreibung
<div data-bbox="245 394 302 453"></div> <p data-bbox="358 170 477 674">Dieses Feld wird nur angezeigt, wenn ein LDAPS-Protokoll im obigen Feld Server-URL angegeben wird.</p> <p data-bbox="212 726 509 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="529 159 818 191">Konto binden (optional)</p>
<p data-bbox="212 1150 509 1797">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.</p>	<p data-bbox="529 1150 834 1182">Bindepaswort (optional)</p>

Einstellung	Beschreibung
<div data-bbox="245 296 302 348"></div> <p data-bbox="362 170 480 443">Dieses Feld wird angezeigt, wenn Sie ein Bindungskonto eingeben.</p> <p data-bbox="214 520 423 617">Geben Sie das Passwort für das Bindekonto ein.</p>	<p data-bbox="529 159 1252 191">Testen Sie die Serververbindung, bevor Sie sie hinzufügen</p>
<p data-bbox="214 674 509 1524">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.</p>	<p data-bbox="529 674 915 705">Berechtigungs-Einstellungen</p>
<p data-bbox="214 1577 431 1608">Basis-DN suchen</p>	<p data-bbox="529 1577 1341 1640">Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise in Form von CN=Users, DC=copc, DC=local.</p>
<p data-bbox="214 1698 493 1730">Attribut Benutzername</p>	<p data-bbox="529 1698 1414 1761">Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: sAMAccountName.</p>
<p data-bbox="214 1820 444 1852">Gruppenattribut(e)</p>	<p data-bbox="529 1820 1446 1917">Geben Sie eine Liste der Gruppenattribute für den Benutzer ein, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: memberOf, managedObjects.</p>

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.	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 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 **Directory Server Settings** wird geöffnet.

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

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 (<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.	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=copc, 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.

Einstellung	Beschreibung
Zuordnungen	Gruppen-DN
Der Domain-Name für die LDAP-Benutzergruppe, die zugeordnet werden soll.	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 **Directory Server entfernen** wird geöffnet.

5. Typ `remove` Klicken Sie im Feld auf **Entfernen**.

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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.