FAQs

SANtricity 11.8

NetApp
January 31, 2025

Inhalt

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 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.

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-Uhreinstellungen).
- 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.