FAQs

SANtricity software

NetApp
June 16, 2025

This PDF was generated from https://docs.netapp.com/de-de/e-series-santricity/um-certificates/why-cant-i-log-in-unified.html on June 16, 2025. Always check docs.netapp.com for the latest.

Inhalt

FAQs . . . 1
- Warum kann ich mich nicht anmelden? . . . 1
- Was muss ich vor dem Hinzufügen eines Verzeichnisservers wissen? . . . 1
- Was muss ich über die Zuordnung von Speicher-Array-Rollen wissen? . . . 1
  - SAML . . . 2
- Was muss ich vor der Konfiguration und Aktivierung von SAML wissen? . . . 2
  - Anforderungen . . . 2
  - Einschränkungen . . . 3
- Welche lokalen Benutzer gibt es? . . . 3

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 entgangen 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.

Copyright-Informationen

Copyright © 2025 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 IRGENDEINER 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.