Kerberos mit NFS für hohe Sicherheit verwenden

ONTAP 9

NetApp
September 30, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nfs-config/kerberos-nfs-strong-security-concept.html on September 30, 2026. Always check docs.netapp.com for the latest.

Inhalt

Kerberos mit NFS für hohe Sicherheit verwenden . . . 1
Informationen zur Verwendung von Kerberos mit ONTAP NFS für eine starke Authentifizierung . . . 1
UNIX-Berechtigungen für NFS-Kerberos-Konfigurationen auf ONTAP SVMs überprüfen . . . 2
Erstellen von NFS Kerberos Realm-Konfigurationen auf ONTAP SVMs . . . 3
NFS-Kerberos zulässige Verschlüsselungstypen für ONTAP SVMs konfigurieren . . . 4
NFS Kerberos auf ONTAP LIFs aktivieren . . . 6

Kerberos mit NFS für hohe Sicherheit verwenden

Informationen zur Verwendung von Kerberos mit ONTAP NFS für eine starke Authentifizierung

Wenn Kerberos in Ihrer Umgebung für die starke Authentifizierung verwendet wird, ist eine Zusammenarbeit mit Ihrem Kerberos-Administrator erforderlich, um die Anforderungen und geeigneten Speichersystemkonfigurationen zu bestimmen und anschließend die SVM als Kerberos-Client zu aktivieren.

Ihre Umgebung sollte die folgenden Richtlinien erfüllen:

- Die Standortbereitstellung sollte den Best Practices für die Konfiguration von Kerberos-Server und -Client entsprechen, bevor Kerberos für ONTAP konfiguriert wird.
- Wenn möglich, sollte NFSv4 oder höher verwendet werden, falls eine Kerberos-Authentifizierung erforderlich ist.

  NFSv3 kann mit Kerberos verwendet werden. Die vollen Sicherheitsvorteile von Kerberos kommen jedoch nur in ONTAP Deployments von NFSv4 oder höher vollständig zum Tragen.

- Um redundanten Serverzugriff zu fördern, sollte Kerberos auf mehreren Daten-LIFs auf mehreren Knoten im Cluster unter Verwendung desselben SPN aktiviert werden.
- Wenn Kerberos auf der SVM aktiviert ist, muss je nach Konfiguration Ihres NFS-Clients eine der folgenden Sicherheitsmethoden in den Exportrichtlinien für Volumes oder qtrees angegeben werden.
  - `krb5` (Kerberos v5-Protokoll)
  - `krb5i` (Kerberos v5-Protokoll mit Integritätsprüfung mittels Prüfsummen)
  - `krb5p` (Kerberos v5-Protokoll mit Datenschutzdienst)

Zusätzlich zum Kerberos-Server und den Clients müssen die folgenden externen Dienste für ONTAP konfiguriert werden, damit Kerberos unterstützt wird:

- Verzeichnisdienst

  In Ihrer Umgebung sollte ein sicherer Verzeichnisdienst wie Active Directory oder OpenLDAP verwendet werden, der für die Nutzung von LDAP über SSL/TLS konfiguriert ist. NIS sollte nicht verwendet werden, da dessen Anfragen im Klartext gesendet werden und daher nicht sicher sind.

- NTP

  Sie benötigen einen funktionierenden Zeitserver, auf dem NTP ausgeführt wird. Dies ist notwendig, um einen Fehler bei der Kerberos-Authentifizierung aufgrund von Zeitabweichungen zu verhindern.

- Domainnamensauflösung (DNS)

  Jeder UNIX-Client und jede SVM-LIF muss über einen gültigen Service Record (SRV) verfügen, der beim KDC in den Forward- und Reverse-Lookup-Zonen registriert ist. Alle Teilnehmer müssen über DNS auflösbar sein.

UNIX-Berechtigungen für NFS-Kerberos-Konfigurationen auf ONTAP SVMs überprüfen

Kerberos erfordert, dass bestimmte UNIX-Berechtigungen für das SVM Root-Volume sowie für lokale Benutzer und Gruppen festgelegt sind.

Schritte

1. Die relevanten Berechtigungen für das SVM-Root-Volume werden angezeigt:

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   Das Root-Volume der SVM muss folgende Konfiguration aufweisen:

Name…	Einstellung…
UID	Root-Benutzer oder ID 0
GID	Root-Benutzer oder ID 0
UNIX-Berechtigungen	755

   Falls diese Werte nicht angezeigt werden, kann der `volume modify` Befehl zur Aktualisierung verwendet werden.

2. Lokale UNIX-Benutzer werden angezeigt:

   `vserver services name-service unix-user show -vserver vserver_name`

   Die SVM muss über die folgenden UNIX-Benutzer verfügen:

Benutzername	Benutzer-ID	Primäre Gruppen-ID	Kommentar
NFS	500	0	Erforderlich für die GSS INIT-Phase. Die erste Komponente des NFS-Client-Benutzer-SPN wird als Benutzer verwendet. Der NFS-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX-Namenszuordnung für den SPN des NFS-Client-Benutzers existiert.
root	0	0	Für das Mounten erforderlich.

   Falls diese Werte nicht angezeigt werden, kann der `vserver services name-service unix-user modify` Befehl verwendet werden, um sie zu aktualisieren.

3. Lokale UNIX-Gruppen werden angezeigt:

   `vserver services name-service unix-group show -vserver vserver _name`

   Die SVM muss mit den folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Daemon	1
root	0

   Falls diese Werte nicht angezeigt werden, kann der `vserver services name-service unix-group modify` Befehl verwendet werden, um sie zu aktualisieren.

Erstellen von NFS Kerberos Realm-Konfigurationen auf ONTAP SVMs

Damit ONTAP auf externe Kerberos-Server in Ihrer Umgebung zugreifen kann, müssen Sie die SVM zunächst für die Verwendung eines vorhandenen Kerberos-Realms konfigurieren. Dazu benötigen Sie die Konfigurationswerte für den Kerberos-KDC-Server und verwenden dann den `vserver nfs kerberos realm create` Befehl, um die Kerberos-Realm-Konfiguration auf einer SVM zu erstellen.

Bevor Sie beginnen

Der Clusteradministrator sollte NTP auf dem Speichersystem, dem Client und dem KDC-Server konfiguriert haben, um Authentifizierungsprobleme zu vermeiden. Zeitunterschiede zwischen Client und Server (Uhrzeitabweichung) sind eine häufige Ursache für Authentifizierungsfehler.

Schritte

1. Mit dem Kerberos-Administrator kann bestimmt werden, welche geeigneten Konfigurationswerte für den `vserver nfs kerberos realm create` Befehl bereitzustellen sind.
2. Erstellen einer Kerberos Realm-Konfiguration auf der SVM:

   `vserver nfs kerberos realm create -vserver vserver_name -realm realm_name {AD_KDC_server_values |AD_KDC_server_values} -comment "text"`

3. Es wird überprüft, ob die Kerberos Realm-Konfiguration erfolgreich erstellt wurde:

   `vserver nfs kerberos realm show`

Beispiele

Der folgende Befehl erstellt eine NFS Kerberos Realm-Konfiguration für die SVM vs1, die einen Microsoft Active Directory Server als KDC-Server verwendet. Der Kerberos Realm ist AUTH.EXAMPLE.COM. Der Active Directory Server heißt ad-1 und hat die IP-Adresse 10.10.8.14. Die zulässige Zeitabweichung beträgt 300 Sekunden (Standardwert). Die IP-Adresse des KDC-Servers ist 10.10.8.14, und seine Portnummer ist 88 (Standardwert). Der Kommentar ist „Microsoft Kerberos config“.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
```

```
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

Der folgende Befehl erstellt eine NFS Kerberos Realm-Konfiguration für die SVM vs1, die einen MIT KDC verwendet. Das Kerberos Realm ist SECURITY.EXAMPLE.COM. Die zulässige Zeitabweichung beträgt 300 Sekunden. Die IP-Adresse des KDC-Servers ist 10.10.9.1, und seine Portnummer ist 88. Der KDC-Anbieter ist Other, um einen UNIX-Anbieter anzuzeigen. Die IP-Adresse des Administrationsservers ist 10.10.9.1, und seine Portnummer ist 749 (Standard). Die IP-Adresse des Passwortservers ist 10.10.9.1, und seine Portnummer ist 464 (Standard). "UNIX Kerberos config" ist der Kommentar.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

NFS-Kerberos zulässige Verschlüsselungstypen für ONTAP SVMs konfigurieren

Standardmäßig unterstützt ONTAP die folgenden Verschlüsselungstypen für NFS Kerberos: DES, 3DES, AES-128 und AES-256. Die zulässigen Verschlüsselungstypen können für jede SVM entsprechend den Sicherheitsanforderungen der jeweiligen Umgebung mit dem `vserver nfs modify` Befehl und dem `-permitted-enc-types` Parameter konfiguriert werden.

Über diese Aufgabe

Für größtmögliche Client-Kompatibilität unterstützt ONTAP standardmäßig sowohl die schwache DES- als auch die starke AES-Verschlüsselung. Das bedeutet beispielsweise, dass, wenn eine Erhöhung der Sicherheit gewünscht ist und die Umgebung dies unterstützt, mit diesem Verfahren DES und 3DES deaktiviert werden können und Clients ausschließlich AES-Verschlüsselung verwenden müssen.

Sie sollten die stärkste verfügbare Verschlüsselung verwenden. Für ONTAP ist das AES-256. Es sollte mit Ihrem KDC-Administrator bestätigt werden, dass diese Verschlüsselungsstufe in Ihrer Umgebung unterstützt wird.

- Das vollständige Aktivieren oder Deaktivieren von AES (sowohl AES-128 als auch AES-256) auf SVMs ist störend, da dabei die ursprüngliche DES-Principal-/Keytab-Datei zerstört wird, wodurch die Kerberos-Konfiguration auf allen LIFs für die SVM deaktiviert werden muss.

  Vor dieser Änderung sollte überprüft werden, ob NFS Clients auf der SVM nicht auf AES Verschlüsselung angewiesen sind.

- Das Aktivieren oder Deaktivieren von DES oder 3DES erfordert keine Änderungen an der Kerberos-Konfiguration auf LIFs.

Schritt

1. Den gewünschten zulässigen Verschlüsselungstyp aktivieren oder deaktivieren:

Wenn Sie aktivieren oder deaktivieren möchten…	**Folgen Sie diesen Schritten…**
DES oder 3DES	a. Die zulässigen Verschlüsselungstypen für NFS Kerberos der SVM konfigurieren: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Mehrere Verschlüsselungstypen durch ein Komma trennen. b. Es sollte überprüft werden, ob die Änderung erfolgreich war: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

AES-128 oder AES-256	a. Ermitteln, auf welcher SVM und LIF Kerberos aktiviert ist:
	`vserver nfs kerberos interface show`
	
	b. Kerberos auf allen LIFs der SVM deaktivieren, deren NFS Kerberos zulässigen Verschlüsselungstyp Sie ändern möchten:
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	
	c. Die zulässigen Verschlüsselungstypen für NFS Kerberos der SVM konfigurieren:
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	
	Mehrere Verschlüsselungstypen durch ein Komma trennen.
	
	d. Es sollte überprüft werden, ob die Änderung erfolgreich war:
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	
	e. Kerberos auf allen LIFs auf der SVM wieder aktivieren:
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	
	f. Es sollte überprüft werden, dass Kerberos auf allen LIFs aktiviert ist:
	`vserver nfs kerberos interface show`

NFS Kerberos auf ONTAP LIFs aktivieren

Sie können den `vserver nfs kerberos interface enable` Befehl verwenden, um Kerberos auf einer Daten-LIF zu aktivieren. Dadurch kann die SVM Kerberos-Sicherheitsdienste für NFS verwenden.

Über diese Aufgabe

Wenn Sie einen Active Directory KDC verwenden, müssen die ersten 15 Zeichen aller verwendeten SPNs innerhalb eines Realms oder einer Domäne über alle SVMs hinweg eindeutig sein.

Schritte

1. Die NFS-Kerberos-Konfiguration erstellen:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   ONTAP benötigt den geheimen Schlüssel für den SPN vom KDC, damit die Kerberos-Schnittstelle aktiviert werden kann.

   Bei Microsoft KDCs wird der KDC kontaktiert und über die CLI eine Benutzername- und Kennwortabfrage angezeigt, um den geheimen Schlüssel zu erhalten. Wenn der SPN in einer anderen Organisationseinheit (OU) des Kerberos-Bereichs erstellt werden soll, kann der optionale `-ou` Parameter angegeben werden.

   Für Nicht-Microsoft-KDCs kann der geheime Schlüssel auf eine von zwei Arten bezogen werden:

Wenn Sie…	**Dem Befehl ist außerdem der folgende Parameter hinzuzufügen…**
Die KDC-Administratoranmeldeinformationen sind erforderlich, um den Schlüssel direkt vom KDC abzurufen.	`-admin-username` *`kdc_admin_username`*
Sie besitzen nicht die KDC-Administratoranmeldeinformationen, haben aber eine Keytab-Datei vom KDC, die den Schlüssel enthält	`-keytab-uri` {ftp

2. Es sollte überprüft werden, ob Kerberos auf der LIF aktiviert ist:

   `vserver nfs kerberos-config show`

3. Schritte 1 und 2 werden wiederholt, um Kerberos auf mehreren LIFs zu aktivieren.

Beispiel

Der folgende Befehl erstellt und überprüft eine NFS-Kerberos-Konfiguration für die SVM mit dem Namen vs1 auf der logischen Schnittstelle ves03-d1 mit dem SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM in der OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
```

```
         Logical
Vserver  Interface Address       Kerberos  SPN
-------  --------- -------       --------- --------------------------------
vs0      ves01-a1
                   10.10.10.30   disabled  -
vs2      ves01-d1
                   10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Copyright-Informationen

Copyright © 2026 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.