Einen SMB Server in einer Active Directory Domäne einrichten

ONTAP 9

NetApp
September 25, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-config/configure-time-services-task.html on September 25, 2026. Always check docs.netapp.com for the latest.

Inhalt

Einen SMB Server in einer Active Directory Domäne einrichten 1
ONTAP Zeitdienste für SMB Server konfigurieren 1
ONTAP Befehle zur Verwaltung der symmetrischen Authentifizierung auf NTP-Servern 1
SMB-Server in einer ONTAP Active Directory-Domäne erstellen 2
Erstellen von Keytab-Dateien für ONTAP SMB-Authentifizierung 6

Einen SMB Server in einer Active Directory Domäne einrichten

ONTAP Zeitdienste für SMB Server konfigurieren

Bevor ein SMB-Server in einem Active Domain Controller erstellt wird, muss sichergestellt werden, dass die Clusterzeit und die Zeit auf den Domänencontrollern der Domäne, zu der der SMB-Server gehören wird, innerhalb von fünf Minuten übereinstimmen.

Über diese Aufgabe

Die Cluster-NTP-Dienste sind so zu konfigurieren, dass für die Synchronisierung dieselben NTP-Server wie von der Active Directory-Domäne verwendet werden.

Ab ONTAP 9.5 ist die Einrichtung Ihres NTP-Servers mit symmetrischer Authentifizierung möglich.

Schritte

1. Zeitdienste werden mithilfe des `cluster time-service ntp server create`Befehls konfiguriert.
   - Um Zeitdienste ohne symmetrische Authentifizierung zu konfigurieren, ist folgender Befehl einzugeben: `cluster time-service ntp server create -server server_ip_address`
   - Um Zeitdienste mit symmetrischer Authentifizierung zu konfigurieren, den folgenden Befehl eingeben: `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. Es kann überprüft werden, ob die Zeitdienste korrekt eingerichtet sind, indem der `cluster time-service ntp server show` Befehl verwendet wird.

   `cluster time-service ntp server show`

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

Verwandte Informationen

- "Cluster Zeitdienst NTP"

ONTAP Befehle zur Verwaltung der symmetrischen Authentifizierung auf NTP-Servern

Ab ONTAP 9.5 wird das Network Time Protocol (NTP) Version 3 unterstützt. NTPv3 beinhaltet eine symmetrische Authentifizierung mit SHA-1-Schlüsseln, was die Netzwerksicherheit erhöht.

Dazu …	Verwenden Sie diesen Befehl…
Konfiguration eines NTP-Servers ohne symmetrische Authentifizierung	`cluster time-service ntp server create -server server_name`
Einen NTP-Server mit symmetrischer Authentifizierung konfigurieren	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Symmetrische Authentifizierung für einen bestehenden NTP serverAn Server aktivieren. Ein bestehender NTP Server kann modifiziert werden, um die Authentifizierung durch Hinzufügen der erforderlichen Schlüssel-ID zu ermöglichen.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Einen gemeinsamen NTP-Schlüssel konfigurieren	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Gemeinsame Schlüssel werden über eine ID referenziert. Die ID, ihr Typ und ihr Wert müssen sowohl auf dem Knoten als auch auf dem NTP Server identisch sein.
Einen NTP-Server mit einer unbekannten Schlüssel-ID konfigurieren	`cluster time-service ntp server create -server server_name -key-id key_id`
Ein Server mit einer Schlüssel-ID, die auf dem NTP-Server nicht konfiguriert ist, wird konfiguriert.	`cluster time-service ntp server create -server server_name -key-id key_id` Die Schlüssel-ID, der Schlüsseltyp und der Schlüsselwert müssen mit der auf dem NTP-Server konfigurierten Schlüssel-ID, dem Schlüsseltyp und dem Schlüsselwert identisch sein.
Symmetrische Authentifizierung deaktivieren	`cluster time-service ntp server modify -server server_name -authentication disabled`

Verwandte Informationen

- "Cluster Zeitdienst NTP"

SMB-Server in einer ONTAP Active Directory-Domäne erstellen

Mit dem `vserver cifs create` Befehl lässt sich ein SMB-Server auf der SVM erstellen und die Active Directory (AD)-Domäne angeben, zu der er gehört.

Bevor Sie beginnen

Die von Ihnen zur Datenbereitstellung verwendeten SVM und LIFs müssen so konfiguriert sein, dass das SMB-Protokoll zugelassen ist. Die LIFs müssen eine Verbindung zu den auf der SVM konfigurierten DNS-Servern und zu einem AD-Domänencontroller der Domäne herstellen können, der der SMB-Server beitreten

soll.

Jeder Benutzer, der berechtigt ist, Computerkonten in der AD-Domäne zu erstellen, zu der Sie den SMB-Server hinzufügen, kann den SMB-Server auf der SVM erstellen. Dies kann auch Benutzer aus anderen Domänen umfassen.

Sie benötigen die folgenden Mindestberechtigungen für die Organisationseinheit (OU), um den SMB-Server zu erstellen:

- Computerobjekte erstellen
- Computerobjekte löschen
- Passwort zurücksetzen
- Lese- und Schreibbeschränkungen für Konten
- Validierter Schreibvorgang zum DNS-Hostnamen
- Validierte Schreibvorgänge für Service Principal Names
- Lesen Sie msDS-SupportedEncryptedTypes
- Schreiben Sie msDS-SupportedEncryptedTypes

Ab ONTAP 9.7 kann Ihnen Ihr AD-Administrator als Alternative zu einem Namen und Passwort für ein privilegiertes Windows-Konto eine URI zu einer Keytab-Datei bereitstellen. Nach Erhalt der URI ist diese im `-keytab-uri` Parameter mit den `vserver cifs` Befehlen anzugeben.

Über diese Aufgabe

Beim Erstellen eines SMB-Servers in einer Activity Directory-Domäne:

- Es ist erforderlich, den vollqualifizierten Domainnamen (FQDN) zu verwenden, wenn die Domäne angegeben wird.
- Standardmäßig wird das SMB-Server-Computerkonto dem Active Directory CN=Computer-Objekt hinzugefügt.
- Sie können wählen, den SMB-Server mithilfe der `-ou` Option einer anderen Organisationseinheit hinzuzufügen.
- Ab ONTAP 9.13.1 können Sie einen Standardstandort für den SMB-Server konfigurieren. ONTAP kann diesen Standort verwenden, wenn ein LIF keiner Standortmitgliedschaft angehört, und als Ausweichmöglichkeit, falls die Standortermittlung für eine vertrauenswürdige Domäne beim Auffinden von Domänencontrollern der vertrauenswürdigen Domäne fehlschlägt.
- Optional kann eine durch Kommas getrennte Liste von einem oder mehreren NetBIOS-Aliasen (bis zu 200) für den SMB-Server hinzugefügt werden.

  Die Konfiguration von NetBIOS-Aliasen für einen SMB-Server kann nützlich sein, wenn Daten von anderen Dateiservern auf den SMB-Server konsolidiert werden und der SMB-Server auf die Namen der ursprünglichen Server reagieren soll.

Weitere Informationen zu `vserver cifs` und optionalen Parametern sowie Namensanforderungen finden Sie in der "ONTAP-Befehlsreferenz".

Ab ONTAP 9.8 kann angegeben werden, dass Verbindungen zu Domänencontrollern verschlüsselt werden. ONTAP erfordert die Verschlüsselung der Kommunikation mit Domänencontrollern, wenn die `-encryption -required-for-dc-connection` Option auf `true` gesetzt ist; der Standardwert ist `false`. Wenn die Option gesetzt ist, wird für ONTAP DC-Verbindungen ausschließlich das SMB3-Protokoll verwendet, da

Verschlüsselung nur von SMB3 unterstützt wird. .

"SMB Management" enthält weitere Informationen zu den Konfigurationsoptionen des SMB-Servers.

Schritte

1. Es sollte überprüft werden, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. Erstellen des SMB-Servers in einer AD-Domäne: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-default-site site_name][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Beim Beitritt zu einer Domäne kann dieser Befehl mehrere Minuten in Anspruch nehmen.

   Der folgende Befehl erstellt den SMB-Server “smb_server01” in der Domäne “example.com”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   Der folgende Befehl erstellt den SMB-Server “smb_server02” in der Domäne “mydomain.com” und authentifiziert den ONTAP-Administrator mit einer Keytab-Datei:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Die SMB-Serverkonfiguration kann mit dem `vserver cifs show` Befehl überprüft werden.

   In diesem Beispiel zeigt die Befehlsausgabe, dass ein SMB-Server mit dem Namen “SMB_SERVER01” auf der SVM vs1.example.com erstellt und der Domäne “example.com” hinzugefügt wurde.

   ```
   cluster1::> vserver cifs show -vserver vs1

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                               Authentication Style: domain
                  CIFS Server Administrative Status: up
                            CIFS Server Description: -
   ```

```
                            List of NetBIOS Aliases: -
```

Ab ONTAP 9.13.1 wird der Standardstandort des SMB-Servers auch als Fallback verwendet, wenn ONTAP keine Standortinformationen für eine vertrauenswürdige Domäne ermitteln kann.

1. Bei Bedarf kann die verschlüsselte Kommunikation mit dem Domänencontroller aktiviert werden (ONTAP 9.8 und höher): `vserver cifs security modify -vserver svm_name -encryption-required -for-dc-connection true`

Beispiele

Der folgende Befehl erstellt einen SMB-Server mit dem Namen „smb_server02“ auf der SVM vs2.example.com in der Domäne „example.com“. Das Computerkonto wird im Container „OU=eng,OU=corp,DC=example,DC=com“ erstellt. Dem SMB-Server wird ein NetBIOS-Alias zugewiesen.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                      CIFS Server NetBIOS Name: SMB_SERVER02
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
               CIFS Server Administrative Status: up
                        CIFS Server Description: -
                        List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

Der folgende Befehl ermöglicht es einem Benutzer aus einer anderen Domäne, in diesem Fall einem Administrator einer vertrauenswürdigen Domäne, einen SMB-Server mit dem Namen „smb_server03“ auf der SVM vs3.example.com zu erstellen. Die `-domain` Option gibt den Namen der Heimatdomäne (in der DNS-Konfiguration festgelegt) an, in der der SMB-Server erstellt werden soll. Die `username` Option gibt den Administrator der vertrauenswürdigen Domäne an.

- Heimdomain: example.com
- Vertrauenswürdige Domain: trust.lab.com
- Benutzername für die vertrauenswürdige Domäne: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Erstellen von Keytab-Dateien für ONTAP SMB-Authentifizierung

Ab ONTAP 9.7 unterstützt ONTAP die SVM-Authentifizierung mit Active Directory (AD)-Servern mithilfe von Keytab-Dateien. AD-Administratoren erstellen eine Keytab-Datei und stellen sie ONTAP Administratoren als Uniform Resource Identifier (URI) zur Verfügung, der bereitgestellt wird, wenn `vserver cifs` Befehle eine Kerberos-Authentifizierung mit der AD-Domäne erfordern.

AD-Administratoren können die Keytab-Dateien mithilfe des Standardbefehls von Windows Server `ktpass` erstellen. Der Befehl sollte in der primären Domäne ausgeführt werden, in der Authentifizierung erforderlich ist. Der `ktpass` Befehl kann verwendet werden, um Keytab-Dateien nur für Benutzer der primären Domäne zu generieren; Schlüssel, die mit Benutzern vertrauenswürdiger Domänen generiert wurden, werden nicht unterstützt.

Keytab-Dateien werden für bestimmte ONTAP-Admin-Benutzer generiert. Solange sich das Passwort des Admin-Benutzers nicht ändert, bleiben die für den jeweiligen Verschlüsselungstyp und die jeweilige Domain generierten Schlüssel unverändert. Daher ist eine neue Keytab-Datei erforderlich, sobald das Passwort des Admin-Benutzers geändert wird.

Folgende Verschlüsselungstypen werden unterstützt:

- AES256-SHA1
- DES-CBC-MD5

  ⓘ ONTAP unterstützt den Verschlüsselungstyp DES-CBC-CRC nicht.

- RC4-HMAC

AES256 ist die höchste Verschlüsselungsstufe und sollte verwendet werden, wenn sie auf dem ONTAP System aktiviert ist.

Keytab-Dateien können entweder durch Angabe des Administratorpassworts oder durch Verwendung eines zufällig generierten Passworts erstellt werden. Es kann jedoch immer nur eine Passwortoption verwendet werden, da auf dem AD-Server ein dem Administrator zugeordneter privater Schlüssel benötigt wird, um die Schlüssel in der Keytab-Datei zu entschlüsseln. Jede Änderung des privaten Schlüssels eines bestimmten Administrators macht die Keytab-Datei ungültig.

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.