Richten Sie einen SMB-Server in einer Active Directory-Domäne ein

ONTAP 9

NetApp
April 24, 2024

Inhalt

Richten Sie einen SMB-Server in einer Active Directory-Domäne ein

Zeitdienste konfigurieren

Bevor Sie einen SMB-Server in einem Active Domain-Controller erstellen, müssen Sie sicherstellen, dass die Clusterzeit und die Zeit auf den Domänencontrollern der Domäne, zu der der SMB-Server gehört, innerhalb von fünf Minuten übereinstimmen.

Über diese Aufgabe

Sie sollten Cluster-NTP-Dienste so konfigurieren, dass sie dieselben NTP-Server für die Zeitsynchronisierung verwenden, die die Active Directory-Domäne verwendet.

Ab ONTAP 9.5 können Sie Ihren NTP-Server mit symmetrischer Authentifizierung einrichten.

Schritte

1. Konfigurieren Sie Zeitdienste mithilfe von `cluster time-service ntp server create` Befehl.
   - Geben Sie den folgenden Befehl ein, um Zeitdienste ohne symmetrische Authentifizierung zu konfigurieren: `cluster time-service ntp server create -server server_ip_address`
   - Geben Sie den folgenden Befehl ein, um Zeitdienste mit symmetrischer Authentifizierung zu konfigurieren: `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. Überprüfen Sie, ob Zeitdienste ordnungsgemäß eingerichtet sind, indem Sie den verwenden `cluster time-service ntp server show` Befehl.

   `cluster time-service ntp server show`

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

Befehle für das Managen der symmetrischen Authentifizierung auf NTP-Servern

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

Hier…	Befehl
Konfigurieren Sie einen NTP-Server ohne symmetrische Authentifizierung	`cluster time-service ntp server create -server server_name`
Konfigurieren Sie einen NTP-Server mit symmetrischer Authentifizierung	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Symmetrische Authentifizierung für einen vorhandenen NTP-Server aktivieren ein vorhandener NTP-Server kann angepasst 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`
Konfigurieren Sie einen freigegebenen NTP-Schlüssel	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Freigegebene Schlüssel werden durch eine ID bezeichnet. Die ID, der Typ und der Wert müssen auf dem Node und dem NTP-Server identisch sein
Konfigurieren Sie einen NTP-Server mit einer unbekannten Schlüssel-ID	`cluster time-service ntp server create -server server_name -key-id key_id`
Konfigurieren Sie einen Server mit einer Schlüssel-ID, die nicht auf dem NTP-Server konfiguriert ist.	`cluster time-service ntp server create -server server_name -key-id key_id` Die Schlüssel-ID, der Typ und der Wert müssen identisch mit der auf dem NTP-Server konfigurierten Schlüssel-ID, dem Typ und dem Wert sein.
Deaktivieren Sie die symmetrische Authentifizierung	`cluster time-service ntp server modify -server server_name -authentication disabled`

Erstellen Sie einen SMB-Server in einer Active Directory-Domäne

Sie können das verwenden `vserver cifs create` Befehl zum Erstellen eines SMB-Servers auf der SVM und zur Angabe der Active Directory-Domäne (AD), der sie angehört.

Bevor Sie beginnen

Die SVM und die LIFs, die Sie zur Bedienung von Daten verwenden, müssen konfiguriert worden sein, um das

SMB-Protokoll zu unterstützen. Die LIFs müssen in der Lage sein, eine Verbindung zu den DNS-Servern herzustellen, die auf der SVM konfiguriert sind, und zu einem AD-Domänencontroller der Domäne, mit dem Sie dem SMB-Server beitreten möchten.

Jeder Benutzer, der zum Erstellen von Computerkonten in der AD-Domäne autorisiert ist, zu der Sie dem SMB-Server beitreten, kann den SMB-Server auf der SVM erstellen. Dies kann auch Benutzer aus anderen Domänen umfassen.

Ab ONTAP 9.7 kann Ihr AD-Administrator Ihnen einen URI zu einer Keytab-Datei als Alternative zur Bereitstellung eines Namens und Kennworts für ein privilegiertes Windows-Konto zur Verfügung stellen. Wenn Sie den URI erhalten, geben Sie ihn in das ein `-keytab-uri` Parameter mit `vserver cifs` Befehle.

Über diese Aufgabe

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

- Sie müssen den vollständig qualifizierten Domänennamen (FQDN) verwenden, wenn Sie die Domäne angeben.
- Die Standardeinstellung besteht darin, das SMB-Serverrechnerkonto dem Objekt Active Directory CN=Computer hinzuzufügen.
- Sie können den SMB-Server mit der zu einer anderen Organisationseinheit (OU) hinzufügen `-ou` Option.
- Sie können optional eine kommagetrennte Liste mit einem oder mehreren NetBIOS-Aliasen (bis zu 200) für den SMB-Server hinzufügen.

  Das Konfigurieren von NetBIOS-Aliase für einen SMB-Server kann nützlich sein, wenn Sie Daten von anderen Dateiservern auf den SMB-Server konsolidieren und den SMB-Server auf die Namen der ursprünglichen Server reagieren möchten.

Der `vserver cifs` Man-Pages enthalten zusätzliche optionale Parameter und Benennungsanforderungen.

> Ab ONTAP 9.1 können Sie SMB Version 2.0 aktivieren, um eine Verbindung zu einem Domain Controller (DC) herzustellen. Wenn Sie SMB 1.0 auf Domänencontrollern deaktiviert haben, ist dies erforderlich. Ab ONTAP 9.2 ist SMB 2.0 standardmäßig aktiviert.

Ab ONTAP 9.8 können Sie festlegen, dass Verbindungen zu Domänencontrollern verschlüsselt werden. ONTAP erfordert Verschlüsselung für Domain Controller-Kommunikation, wenn der `-encryption-required -for-dc-connection` Die Option ist auf festgelegt `true`; Die Standardeinstellung ist `false`. Wenn die Option eingestellt ist, wird nur das SMB3-Protokoll für ONTAP-DC-Verbindungen verwendet, da Verschlüsselung nur von SMB3 unterstützt wird. .

"SMB-Management" Enthält weitere Informationen zu SMB-Serverkonfigurationsoptionen.

Schritte

1. Vergewissern Sie sich, dass SMB für Ihr Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist in enthalten "ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

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

2. Erstellen Sie den SMB-Server in einer AD-Domäne: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri`

`{(ftp|http)://hostname|IP_address}][-comment text]`

Beim Beitritt zu einer Domäne kann dieser Befehl einige Minuten dauern.

Mit dem folgenden Befehl wird der SMB-Server „`smb_server01`“ in der Domäne „`example.com`":“ erstellt

```
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. Überprüfen Sie die SMB-Serverkonfiguration mit `vserver cifs show` Befehl.

   In diesem Beispiel zeigt die Befehlsausgabe an, dass ein SMB-Server mit dem Namen „`SMB_SERVER01`“ auf 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: -
```

4. Aktivieren Sie bei Bedarf die verschlüsselte Kommunikation mit dem Domain Controller (ONTAP 9.8 und höher): `vserver cifs security modify -vserver svm_name -encryption-required-for -dc-connection true`

Beispiele

Mit dem folgenden Befehl wird ein SMB-Server mit dem Namen „`smb_server02`“ auf SVM vs2.example.com in der Domäne „`example.com`""“ erstellt. Das Maschinenkonto 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
```

Mit dem folgenden Befehl kann ein Benutzer aus einer anderen Domäne, in diesem Fall ein Administrator einer vertrauenswürdigen Domäne, einen SMB-Server mit dem Namen „`smb_server03`“ auf SVM vs3.example.com erstellen. Der `-domain` Option gibt den Namen der Home-Domain an (angegeben in der DNS-Konfiguration), in der der SMB-Server erstellt werden soll. Der `username` Option gibt den Administrator der vertrauenswürdigen Domäne an.

- Home Domain: example.com
- Vertrauenswürdige Domäne: 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 die SMB-Authentifizierung

Ab ONTAP 9.7 unterstützt ONTAP die SVM-Authentifizierung mit Active Directory (AD) Servern unter Verwendung von Keytab-Dateien. AD-Administratoren erzeugen eine Keytab-Datei und stellen sie ONTAP-Administratoren als einheitliche Ressourcen-ID (URI) zur Verfügung, die bei der Bereitstellung bereitgestellt wird `vserver cifs` Befehle erfordern eine Kerberos-Authentifizierung mit der AD-Domäne.

AD-Administratoren können die Keytab-Dateien mit dem Standard-Windows-Server erstellen `ktpass` Befehl. Der Befehl sollte in der primären Domäne ausgeführt werden, in der eine Authentifizierung erforderlich ist. Der `ktpass` Der Befehl kann verwendet werden, um Keytab-Dateien nur für primäre Domain-Benutzer zu generieren; Schlüssel, die mit vertrauenswürdigen Domain-Benutzern generiert werden, werden nicht unterstützt.

Keytab-Dateien werden für bestimmte ONTAP Admin-Benutzer generiert. Solange sich das Passwort des Admin-Benutzers nicht ändert, ändern sich die für den jeweiligen Verschlüsselungstyp und die Domäne generierten Schlüssel nicht. Daher ist immer dann eine neue Keytab-Datei erforderlich, wenn 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 der höchste Verschlüsselungstyp und sollte verwendet werden, wenn diese auf dem ONTAP-System aktiviert ist.

Keytab-Dateien können entweder durch Angabe des Admin-Passworts oder durch die Verwendung eines zufällig generierten Passworts generiert werden. Allerdings kann zu einem bestimmten Zeitpunkt nur eine Kennwortoption verwendet werden, da ein privater Schlüssel, der für den Admin-Benutzer spezifisch ist, auf dem AD-Server zum Entschlüsseln der Schlüssel in der Keytab-Datei benötigt wird. Jede Änderung des privaten Schlüssels für einen bestimmten Administrator wird die Keytab-Datei ungültig.