在Active Directory網域中設定SMB伺服器

ONTAP 9

NetApp
March 03, 2026

目錄

在Active Directory網域中設定SMB伺服器

為 SMB 伺服器設定 ONTAP 時間服務

在Active Domain控制器中建立SMB伺服器之前、您必須確保SMB伺服器所屬網域的網域控制器上的叢集時間和時間、在五分鐘內相符。

關於這項工作

您應該設定叢集 NTP 服務以使用與 Active Directory 網域相同的 NTP 伺服器進行同步。

從功能完善的9.5開始ONTAP 、您可以使用對稱驗證來設定NTP伺服器。

步驟

1. 使用設定時間服務 `cluster time-service ntp server create` 命令。
   - 若要在不使用對稱驗證的情況下設定時間服務、請輸入下列命令： `cluster time-service ntp server create -server server_ip_address`
   - 若要使用對稱驗證來設定時間服務、請輸入下列命令： `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. 使用確認時間服務已正確設定 `cluster time-service ntp server show` 命令。

   `cluster time-service ntp server show`

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

相關資訊

- "叢集時間服務 NTP"

用於管理 NTP 伺服器上對稱驗證的 ONTAP 命令

從推出支援的版本號為《支援網路時間傳輸協定》（NTP）第3版。ONTAPNTPv3包含使用SHA-1金鑰的對稱驗證、可提高網路安全性。

若要這麼做...	使用此命令...
設定NTP伺服器而不進行對稱驗證	`cluster time-service ntp server create -server server_name`

若要這麼做...	使用此命令...
設定採用對稱驗證的NTP伺服器	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
啟用現有NTP伺服器的對稱驗證您可以修改現有NTP伺服器、藉由新增所需的金鑰ID來啟用驗證。	`cluster time-service ntp server modify -server server_name -key-id key_id`
設定共用的NTP金鑰	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 共用金鑰是由ID所指。節點和NTP伺服器上的ID、其類型和值必須相同
使用未知的金鑰ID設定NTP伺服器	`cluster time-service ntp server create -server server_name -key-id key_id`
在NTP伺服器上設定未設定金鑰ID的伺服器。	`cluster time-service ntp server create -server server_name -key-id key_id` 金鑰ID、類型和值必須與NTP伺服器上設定的金鑰ID、類型和值相同。
停用對稱驗證	`cluster time-service ntp server modify -server server_name -authentication disabled`

相關資訊

- "叢集時間服務 NTP"

在 ONTAP Active Directory 網域中建立 SMB 伺服器

您可以使用 `vserver cifs create` 命令在 SVM 上建立 SMB 伺服器、並指定其所屬的 Active Directory （ AD ）網域。

開始之前

您用來提供資料的SVM和LIF必須設定為允許SMB傳輸協定。生命期必須能夠連線到SVM上設定的DNS伺服器、以及要加入SMB伺服器之網域的AD網域控制器。

任何有權在您要加入SMB伺服器的AD網域中建立機器帳戶的使用者、都可以在SVM上建立SMB伺服器。這可能包括來自其他網域的使用者。

若要建立 SMB 伺服器、您需要對組織單元（ OU ）擁有以下最低權限：

- 建立電腦物件

- 刪除電腦物件
- 重設密碼
- 讀取和寫入帳戶限制
- 已驗證寫入 DNS 主機名稱
- 已驗證寫入服務主體名稱
- 讀取 msDS-SupportedEncryptedTypes
- 寫入 msDS-SupportedEncryptedTypes

從ONTAP 功能更新9.7開始、AD管理員可以提供Keytab檔案的URI、作為提供權限Windows帳戶名稱和密碼的替代方案。當您收到 URI 時、請將其加入 `-keytab-uri` 參數 `vserver cifs` 命令。

關於這項工作

在活動目錄網域中建立SMB伺服器時：

- 指定網域時、您必須使用完整網域名稱（FQDN）。
- 預設設定是將SMB伺服器機器帳戶新增至Active Directory CN=電腦物件。
- 您可以使用 `-ou` 選項將 SMB 伺服器新增至不同的 OU。
- 您可以選擇性地為SMB伺服器新增一個或多個NetBios別名（最多200個）的以逗號分隔的清單。

  當您將其他檔案伺服器的資料整合到SMB伺服器、並希望SMB伺服器回應原始伺服器的名稱時、設定SMB伺服器的NetBios別名很有用。

如需更多"指令參考資料ONTAP"資訊，以及選用參數和命名需求的詳細 `vserver cifs`資訊，請參閱。

從ONTAP 功能表9.8開始、您可以指定要加密網域控制器的連線。ONTAP 需要加密網域控制站通訊 `-encryption-required-for-dc-connection` 選項設定為 `true`；預設值為 `false`。設定此選項時、只有SMb3傳輸協定會用於ONTAP-DC連線、因為只有SMb3才支援加密。。

"中小企業管理" 包含SMB伺服器組態選項的詳細資訊。

步驟

1. 驗證叢集上是否已授權 SMB ： `system license show -package cifs`

   SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。

   如果SMB伺服器僅用於驗證、則不需要CIFS授權。

2. 在 AD 網域中建立 SMB 伺服器： `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]`

   加入網域時、此命令可能需要幾分鐘的時間才能完成。

   下列命令會在網域「example.com`":」中建立SMB伺服器「'shMB_server01」

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

下列命令會在「mydomain.com`"」網域中建立SMB伺服器「'shMB_server02」、並使用ONTAP Keytab檔案驗證該管理員：

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

3. 使用驗證 SMB 伺服器組態 `vserver cifs show` 命令。

在此範例中、命令輸出顯示在SVM vs1.example.com上建立名為「smb_server01」的SMB伺服器、並加入「example.com`"網域」。

```
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. 如有需要、請啟用與網域控制器（ ONTAP 9.8 及更新版本）的加密通訊： `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

範例

下列命令會在「example.com`"網域」的SVM vs2.example.com上建立名為「shmb_server02」的SMB伺服器。機器帳戶是在「'ou=eng,ou=corp,d=exam,dc=exam,d=com'」容器中建立。SMB伺服器會被指派一個NetBios別名。

```
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
```

下列命令可讓來自不同網域的使用者（在此情況下為信任網域的系統管理員）在SVM vs3.example.com上建立名為「sMB _server03」的SMB伺服器。。 `-domain` 選項指定您要在其中建立 SMB 伺服器的主網域名稱（在 DNS 組態中指定）。。 `username` 選項指定信任網域的系統管理員。

- 主網域：example.com
- 信任的網域：trust.lab.com
- 信任網域的使用者名稱：Administrator 1

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

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

為 ONTAP SMB 驗證建立 Keytab 檔案

從支援SVM 9.7開始ONTAP 、ONTAP 使用Keytab檔案、透過Active Directory（AD）伺服器支援SVM驗證。AD 系統管理員會產生 Keytab 檔案、並將其提供給 ONTAP 系統管理員、做為統一的資源識別元（ URI ） `vserver cifs` 命令需要使用 AD 網域進行 Kerberos 驗證。

AD 管理員可以使用標準 Windows Server 建立 Keytab 檔案 `ktpass` 命令。命令應在需要驗證的主要網域上執行。。 `ktpass` 命令僅可用於為主要網域使用者產生 Keytab 檔案；不支援使用信任網域使用者所產生的金鑰。

Keytab檔案是針對特定ONTAP 的資訊管理員使用者所產生。只要管理員使用者的密碼未變更、針對特定加密類型和網域所產生的金鑰就不會變更。因此、每當管理員使用者的密碼變更時、都需要新的Keytab檔案。

支援下列加密類型：

- AES256-SHA1
- 德斯CBC-MD5

  不支援DES-CBC-CRC加密類型。ONTAP

- RC4-HMAC

ES256是最高的加密類型、如果在ONTAP 支援的系統上啟用、就應該使用。

您可以指定管理密碼或使用隨機產生的密碼來產生Keytab檔案。不過、在任何指定時間、只能使用一個密碼選項、因為AD伺服器需要專屬的管理使用者私密金鑰、才能解密Keytab檔案中的金鑰。對特定管理員的私密金鑰進行任何變更、都會使Keytab檔案失效。