設定SMB存取SVM

ONTAP 9

NetApp
February 12, 2026

目錄

設定SMB存取SVM . . . 1
- 設定 SMB 存取 ONTAP SVM . . . 1
- 建立 ONTAP SVM 以提供 SMB 資料存取 . . . 1
- 確認 ONTAP SVM 上已啟用 SMB 傳輸協定 . . . 2
- 開啟 ONTAP SVM 根 Volume 的 SMB 匯出原則 . . . 3
- 建立 ONTAP SMB 生命 . . . 4
- 啟用 DNS 以進行 ONTAP SMB 主機名稱解析 . . . 8
- 在Active Directory網域中設定SMB伺服器 . . . 9
  - 為 SMB 伺服器設定 ONTAP 時間服務 . . . 9
  - 用於管理 NTP 伺服器上對稱驗證的 ONTAP 命令 . . . 10
  - 在 ONTAP Active Directory 網域中建立 SMB 伺服器 . . . 11
  - 為 ONTAP SMB 驗證建立 Keytab 檔案 . . . 13
- 在工作群組中設定SMB伺服器 . . . 14
  - 瞭解 ONTAP 工作群組中的 SMB 伺服器組態 . . . 14
  - 在具有指定工作群組的 ONTAP SVM 上建立 SMB 伺服器 . . . 14
  - 建立本機 ONTAP SMB 使用者帳戶 . . . 15
  - 建立本機 ONTAP SMB 群組 . . . 17
  - 管理本機 ONTAP SMB 群組成員資格 . . . 18
- 驗證啟用的 ONTAP SMB 版本 . . . 19
- 對應 DNS 伺服器上的 ONTAP SMB 伺服器 . . . 20

設定SMB存取SVM

設定 SMB 存取 ONTAP SVM

如果您尚未設定SVM進行SMB用戶端存取、則必須建立並設定新的SVM、或是設定現有的SVM。設定SMB需要開啟SVM根磁碟區存取、建立SMB伺服器、建立LIF、啟用主機名稱解析、設定名稱服務、以及視需要進行、 啟用Kerberos安全性。

建立 ONTAP SVM 以提供 SMB 資料存取

如果叢集中尚未至少有一個 SVM 可提供 SMB 用戶端的資料存取、則必須建立一個 SVM 。

開始之前

- 從 ONTAP 9.13.1 開始，您可以設定儲存 VM 的最大容量。您也可以在 SVM 接近臨界值容量層級時設定警示。如需更多資訊、請參閱 管理 SVM 容量。

步驟

1. 建立SVM： `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*
   - 使用的 NTFS 設定 `-rootvolume-security-style` 選項。
   - 使用預設的 C.UTF-8 `-language` 選項。
   - 。 `ipspace` 設定為選用項目。
2. 驗證新建立的SVM的組態和狀態： `vserver show -vserver` *`vserver_name`*
   - 。 `Allowed Protocols` 欄位必須包含 CIFS 。您可以稍後再編輯此清單。
   - 。 `Vserver Operational State` 欄位必須顯示 `running` 州/省。如果顯示 `initializing` 狀態、表示有些中繼作業（例如建立根磁碟區）失敗、您必須刪除 SVM 並重新建立它。

範例

下列命令會建立 SVM 、以便在 IPspace 中存取資料 `ipspaceA`：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

下列命令顯示 SVM 是以 1 GB 的根磁碟區所建立、而且是自動啟動且位於中 `running` 州/省。根磁碟區具有預設的匯出原則、不含任何規則、因此根磁碟區在建立時不會匯出。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

從 ONTAP 9.13.1 開始，您可以設定調適性 QoS 原則群組範本，將處理量下限套用至 SVM 中的磁碟區。您只能在建立 SVM 之後套用此原則。若要深入瞭解此程序，請參閱設定調適性原則群組範本。

確認 ONTAP SVM 上已啟用 SMB 傳輸協定

在 SVM 上設定和使用 SMB 之前、您必須先確認已啟用傳輸協定。

關於這項工作

這通常是在 SVM 設定期間完成、但如果您在設定期間未啟用傳輸協定、您可以稍後使用加以啟用 `vserver add-protocols` 命令。

一旦建立LIF、您就無法從其新增或移除通訊協定。

您也可以使用停用 SVM 上的通訊協定 `vserver remove-protocols` 命令。

步驟

1. 檢查SVM目前啟用和停用的傳輸協定： `vserver show -vserver vserver_name -protocols`

您也可以使用 `vserver show-protocols` 用於檢視叢集中所有 SVM 上目前啟用的通訊協定的命令。

2. 如有必要、請啟用或停用傳輸協定：
   - 若要啟用 SMB 傳輸協定： `vserver add-protocols -vserver vserver_name -protocols cifs`
   - 若要停用通訊協定： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. 確認已啟用和停用的傳輸協定已正確更新： `vserver show -vserver vserver_name -protocols`

範例

下列命令顯示名為VS1的SVM上目前啟用和停用（允許和不允許）的傳輸協定：

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

下列命令可透過新增來存取 SMB `cifs` 到名為 VS1 的 SVM 上已啟用的通訊協定清單：

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

開啟 ONTAP SVM 根 Volume 的 SMB 匯出原則

SVM 根 Volume 的預設匯出原則必須包含一條規則、以允許所有用戶端透過 SMB 開啟存取。如果沒有這種規則、所有 SMB 用戶端都會被拒絕存取 SVM 及其磁碟區。

關於這項工作

建立新的SVM時、會自動為SVM的根Volume建立預設匯出原則（稱為預設）。您必須先為預設匯出原則建立一或多個規則、用戶端才能存取SVM上的資料。

您應該確認所有SMB存取都是在預設匯出原則中開啟、之後再建立個別磁碟區或qtree的自訂匯出原則、以限制個別磁碟區的存取。

步驟

1. 如果您使用現有的SVM、請檢查預設的根Volume匯出原則： `vserver export-policy rule show`

   命令輸出應類似下列內容：

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

如果存在允許開啟存取的規則、則此工作即告完成。如果沒有、請繼續下一步。

2. 建立SVM根磁碟區的匯出規則： `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. 使用驗證規則建立 `vserver export-policy rule show` 命令。

結果

任何 SMB 用戶端現在都可以存取 SVM 上建立的任何 Volume 或 qtree 。

建立 ONTAP SMB 生命

LIF是與實體或邏輯連接埠相關聯的IP位址。如果元件發生故障、LIF可能會容錯移轉至不同的實體連接埠、或移轉至不同的實體連接埠、進而繼續與網路通訊。

開始之前

- 基礎實體或邏輯網路連接埠必須設定為管理 `up`狀態。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

  子網路包含屬於同一第3層子網路的IP位址集區。它們是使用建立的 `network subnet create` 命令。

  如"指令參考資料ONTAP"需詳細 `network subnet create`資訊，請參閱。

- 指定LIF處理之流量類型的機制已變更。對於僅適用於更新版本的版本、LIF會使用角色來指定其處理的流量類型。ONTAP從ONTAP Sf6開始、I生命 就會使用服務原則來指定處理的流量類型。

關於這項工作

- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- 如果叢集中有大量的生命、您可以使用來驗證叢集上支援的 LIF 容量 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show`

命令（進階權限層級）。

如"指令參考資料ONTAP"需詳細 `network interface`資訊，請參閱。

- 從ONTAP NetApp 9.7開始、如果相同子網路中的SVM已存在其他LIF、您就不需要指定LIF的主連接埠。在相同的廣播網域中、系統會自動在指定的主節點上選擇隨機連接埠、如同在同一個子網路中設定的其他LIF。ONTAP

步驟

1. 建立LIF：

```
network interface create -vserver vserver_name -lif lif_name -role data -data
-protocol cifs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

《》第9.5版及更早版本* ONTAP
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

版本**9.6**及更新版本 ONTAP
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

  - 。 `-role` 使用服務原則建立 LIF 時不需要參數（從 ONTAP 9.6 開始）。
  - 。 `-data-protocol` 使用服務原則建立 LIF 時不需要參數（從 ONTAP 9.6 開始）。使用 ONTAP 9.5 或更早版本時 `-data-protocol` 必須在建立 LIF 時指定參數、而且必須在稍後修改、才能銷毀及重新建立資料 LIF 。
  - `-home-node` 是 LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。

    您也可以指定 LIF 是否應該使用自動還原至主節點和主連接埠 `-auto-revert` 選項。
  - `-home-port` 是 LIF 在時傳回的實體或邏輯連接埠 `network interface revert` 命令會在LIF上執行。
  - 您可以使用指定 IP 位址 `-address` 和 `-netmask` 或是您可以使用從子網路進行分配 `-subnet_name` 選項。
  - 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
  - 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。在中深入瞭解 `network route create`並建立 SVM 內的靜態路由"指令參考資

料ONTAP"。

- 適用於 `-firewall-policy` 選項、請使用相同的預設值 `data` 成為 LIF 角色。

  如果需要、您可以稍後建立並新增自訂防火牆原則。

  > 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- `-auto-revert` 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下自動還原至其主節點。預設設定為 `false`**但您可以將其設定為** `false` 視環境中的網路管理原則而定。

2. 確認LIF已成功建立：

   ```
   network interface show
   ```

3. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	`network ping`
IPv6位址	`network ping6`

範例

下列命令會建立 LIF 並使用指定 IP 位址和網路遮罩值 `-address` 和 `-netmask` 參數：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

下列命令會建立LIF、並從指定的子網路（名為client1_sub）指派IP位址和網路遮罩值：

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

下列命令顯示叢集1中的所有LIF。資料生命週期1和資料傳輸3均設定為使用IPv4位址、而資料傳輸4則設定為使用IPv6位址：

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

下列命令顯示如何建立指派給的 NAS 資料 LIF `default-data-files` 服務原則：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

相關資訊

- "網路ping"
- "網路介面回復"

啟用 DNS 以進行 ONTAP SMB 主機名稱解析

您可以使用 `vserver services name-service dns`命令在 SVM 上啟用 DNS ，並將其設定為使用 DNS 進行主機名稱解析。使用外部DNS伺服器解析主機名稱。如"指令參考資料ONTAP"需詳細 `vserver services name-service dns`資訊，請參閱。

開始之前

站台範圍的DNS伺服器必須可供主機名稱查詢。

您應該設定多個DNS伺服器、以避免單點故障。如果您只輸入一個 DNS 伺服器名稱，則命令會 `vserver services name-service dns create`發出警告。如"指令參考資料ONTAP"需詳細 `vserver services name-service dns create`資訊，請參閱。

關於這項工作

深入瞭解 "在 SVM 上設定動態 DNS"。

步驟

1. 在SVM上啟用DNS： `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   下列命令可啟用SVM VS1上的外部DNS伺服器：

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   ◦ `vserver services name-service dns create` 如果 ONTAP 無法連絡名稱伺服器、命令會執行自動組態驗證、並回報錯誤訊息。

2. 使用顯示 DNS 網域組態 `vserver services name-service dns show` 命令。

   下列命令會顯示叢集中所有SVM的DNS組態：

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   下列命令會顯示SVM VS1的詳細DNS組態資訊：

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 使用驗證名稱伺服器的狀態 `vserver services name-service dns check` 命令。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver            Name Server     Status       Status Details
---------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

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`
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。

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。
- 您可以選擇使用將 SMB 伺服器新增至不同的組織單位（ OU ） `-ou` 選項。
- 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。

在工作群組中設定SMB伺服器

瞭解 ONTAP 工作群組中的 SMB 伺服器組態

將SMB伺服器設定為工作群組的成員包括建立SMB伺服器、然後建立本機使用者和群組。

當Microsoft Active Directory網域基礎架構無法使用時、您可以在工作群組中設定SMB伺服器。

工作群組模式中的SMB伺服器僅支援NTLM驗證、不支援Kerberos驗證。

在具有指定工作群組的 ONTAP SVM 上建立 SMB 伺服器

您可以使用 `vserver cifs create` 命令在 SVM 上建立 SMB 伺服器、並指定其所屬的工作群組。

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。

關於這項工作

工作群組模式的SMB伺服器不支援下列SMB功能：

- SMB3見證傳輸協定
- SMB3 CA共用
- SQL over SMB
- 資料夾重新導向
- 漫遊設定檔
- 群組原則物件（GPO）
- Volume Snapshot服務（VSS）

如需更多 `vserver cifs`"指令參考資料ONTAP"資訊，以及選用的組態參數和命名需求，請參閱。

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. 在工作群組中建立 SMB 伺服器： `vserver cifs create -vserver vserver_name -cifs -server cifs_server_name -workgroup workgroup_name [-comment text]`

   下列命令會在工作群組「workgroup 01」中建立SMB伺服器「'shMB_server01」：

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

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

   在下列範例中、命令輸出顯示在工作群組「workgroup 01」的SVM vs1.example.com上建立了名為「shmb_server01」的SMB伺服器：

   ```
   cluster1::> vserver cifs show -vserver vs0

                                           Vserver: vs1.example.com
                         CIFS Server NetBIOS Name: SMB_SERVER01
                     NetBIOS Domain/Workgroup Name: workgroup01
                       Fully Qualified Domain Name: -
                               Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                    Workgroup Name: workgroup01
                                Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                            CIFS Server Description:
                            List of NetBIOS Aliases: -
   ```

完成後

對於工作群組中的CIFS伺服器、您必須在SVM上建立本機使用者及選擇性的本機群組。

相關資訊

"中小企業管理"

建立本機 **ONTAP SMB** 使用者帳戶

您可以建立本機使用者帳戶、以便透過SMB連線授權存取SVM中所含的資料。您也可以在建立SMB工作階段時、使用本機使用者帳戶進行驗證。

關於這項工作

建立SVM時、預設會啟用本機使用者功能。

建立本機使用者帳戶時、您必須指定使用者名稱、並指定要與帳戶建立關聯的SVM。

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 users-and-groups local-user`資訊，請參閱。

步驟

1. 建立本機使用者： `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   下列選用參數可能很有用：

   - `-full-name`

     使用者的全名。

   - `-description`

     本機使用者的說明。

   - `-is-account-disabled {true|false}`

     指定使用者帳戶是啟用還是停用。如果未指定此參數、則預設為啟用使用者帳戶。

   命令會提示輸入本機使用者的密碼。

2. 輸入本機使用者的密碼、然後確認密碼。
3. 確認已成功建立使用者： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

範例

以下範例建立一個本機使用者「'Smb_server01\sue」、全名為「'Shue Chang'」、與SVM vs1.example.com相關聯：

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator              Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

建立本機 ONTAP SMB 群組

您可以建立本機群組、以便透過SMB連線授權存取與SVM相關的資料。您也可以指派權限來定義群組成員擁有的使用者權限或功能。

關於這項工作

建立SVM時、預設會啟用本機群組功能。

當您建立本機群組時、必須為群組指定名稱、而且必須指定要與群組建立關聯的SVM。您可以使用或不使用本機網域名稱來指定群組名稱、也可以選擇性地指定本機群組的說明。您無法將本機群組新增至其他本機群組。

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 users-and-groups local-group`資訊，請參閱。

步驟

1. 建立本機群組： `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   下列選用參數可能很有用：

   - `-description`

     本機群組的說明。

2. 確認已成功建立群組： `vserver cifs users-and-groups local-group show -vserver vserver_name`

範例

下列範例建立與SVM VS1相關的本機群組「'Smb_server01\Engineering」：

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                     Description
---------------- ------------------------------ ------------------------------
vs1.example.com  BUILTIN\Administrators         Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators       Backup Operators group
vs1.example.com  BUILTIN\Power Users            Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                  All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

完成後

您必須將成員新增至新群組。

管理本機 ONTAP SMB 群組成員資格

您可以新增及移除本機或網域使用者、或新增及移除網域群組、來管理本機群組成員資格。如果您想要根據群組中的存取控制來控制資料存取、或是想要使用者擁有與該群組相關的權限、這很有用。

關於這項工作

如果您不再希望本機使用者、網域使用者或網域群組擁有根據群組成員資格而設定的存取權限或權限、您可以從群組中移除成員。

將成員新增至本機群組時、必須謹記下列事項：

- 您無法將使用者新增至特殊的_Everyon__群組。
- 您無法將本機群組新增至其他本機群組。
- 若要將網域使用者或群組新增至本機群組、ONTAP 則必須能夠將名稱解析為SID。

從本機群組中移除成員時、必須謹記下列事項：

- 您無法從特殊的_Everyon__群組中移除成員。
- 若要從本機群組中移除成員、ONTAP 則必須能夠將成員的名稱解析為一個SID。

步驟

1. 新增成員至群組或從群組中移除成員。
   - 新增成員： `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     您可以指定要新增至指定本機群組的本機使用者、網域使用者或網域群組的以逗號分隔的清單。
   - 移除成員： `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     您可以指定要從指定本機群組中移除的本機使用者、網域使用者或網域群組的以逗號分隔的清單。

範例

以下範例將本機使用者「'Smb_server01\sue」新增至SVM vs1.example.com上的本機群組「'Smb_server01\Engineering」：

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

以下範例將本機使用者「'MB_server01\sue」和「'MB_server01\James」從SVM vs1.example.com上的本機群組「'MB_server01\Engineering」中移除：

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

驗證啟用的 ONTAP SMB 版本

您的版本支援的版本取決於預設啟用哪些SMB版本、以便與用戶端和網域控制器連線。ONTAP您應該確認SMB伺服器是否支援您環境中所需的用戶端和功能。

關於這項工作

若要與用戶端和網域控制器連線、您應該盡可能啟用SMB 2.0和更新版本。基於安全考量、您應該避免使用SMB 1.0、如果您已確認環境中不需要SMB 1.0、則應該停用SMB 1.0。

從功能更新9.3開始ONTAP 、它在新的SVM上預設為停用。

> 如果 `-smb1-enabled-for-dc-connections` 設為 `false` 而 `-smb1-enabled` 設為 `true`，ONTAP 拒絕 SMB 1.0 連線做為用戶端，但會繼續接受傳入 SMB 1.0 連線做為伺服器。

"中小企業管理" 包含支援的SMB版本和功能的詳細資料。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 確認啟用哪些 SMB 版本：

   ```
   vserver cifs options show
   ```

   您可以向下捲動清單、檢視啟用用戶端連線的SMB版本、如果您要在AD網域中設定SMB伺服器、以進行AD網域連線。

3. 視需要啟用或停用用戶端連線的SMB傳輸協定：

   - 若要啟用 SMB 版本：

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     true
     ```

     的可能值 `smb_version`：

     - `-smb1-enabled`
     - `-smb2-enabled`

- `-smb3-enabled`
- `-smb31-enabled`

  下列命令可在 SVM vs1.example.com 上啟用 SMB 3.1 ： `cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true`

◦ 若要停用 SMB 版本：

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. 如果SMB伺服器位於Active Directory網域中、請視需要啟用或停用SMB傳輸協定以進行DC連線：
   ◦ 若要啟用 SMB 版本：

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   ◦ 若要停用 SMB 版本：

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. 返回管理權限層級：

```
set -privilege admin
```

對應 DNS 伺服器上的 ONTAP SMB 伺服器

您站台的DNS伺服器必須有一個項目、將SMB伺服器名稱和任何NetBios別名指向資料LIF的IP位址、以便Windows使用者將磁碟機對應至SMB伺服器名稱。

開始之前

您必須擁有站台DNS伺服器的管理存取權。如果您沒有管理存取權、則必須要求DNS管理員執行此工作。

關於這項工作

如果您使用SMB伺服器名稱的NetBios別名、最好為每個別名建立DNS伺服器進入點。

步驟

1. 登入DNS伺服器。
2. 建立轉送（A -位址記錄）和反轉（PTL -指標記錄）查詢項目、將SMB伺服器名稱對應至資料LIF的IP位址。

3. 如果您使用的是NetBios別名、請建立別名標準名稱（CNAME資源記錄）查詢項目、將每個別名對應至SMB伺服器資料LIF的IP位址。

結果

在整個網路傳播對應之後、Windows使用者可以將磁碟機對應到SMB伺服器名稱或其NetBios別名。