使用 CLI 設定 SMB

ONTAP 9

NetApp
April 24, 2024

目錄

使用 CLI 設定 SMB

使用 CLI 的 SMB 組態概觀

您可以使用ONTAP 支援功能支援功能支援支援功能、以設定SMB用戶端存取新磁碟區或新SVM或現有SVM中qtree中所含的檔案。

> *SMB*（伺服器訊息區塊）是指通用網際網路檔案系統（CIFS）傳輸協定的現代語言。您仍會在ONTAP VMware的指令行介面（CLI）和OnCommand VMware的管理工具中看到_CIFS_。

如果您想要以下列方式設定SMB對磁碟區或qtree的存取權、請使用下列程序：

- 您想要使用SMB第2版或更新版本。
- 您只想為SMB用戶端服務、而非NFS用戶端（而非多重傳輸協定組態）。
- NTFS 檔案權限將用於保護新磁碟區的安全。
- 您擁有叢集管理員權限、而非SVM管理員權限。

  建立SVM和LIF需要叢集管理員權限。SVM管理員權限足以執行其他SMB組態工作。

- 您想要使用CLI、而非System Manager或自動化指令碼工具。

  若要使用System Manager設定NAS多重傳輸協定存取、請參閱 "同時使用NFS和SMB為Windows和Linux配置NAS儲存設備"。

- 您想要使用最佳實務做法、而非探索每個可用選項。

  如需命令語法的詳細資料、請參閱CLI說明和ONTAP 支援手冊頁。

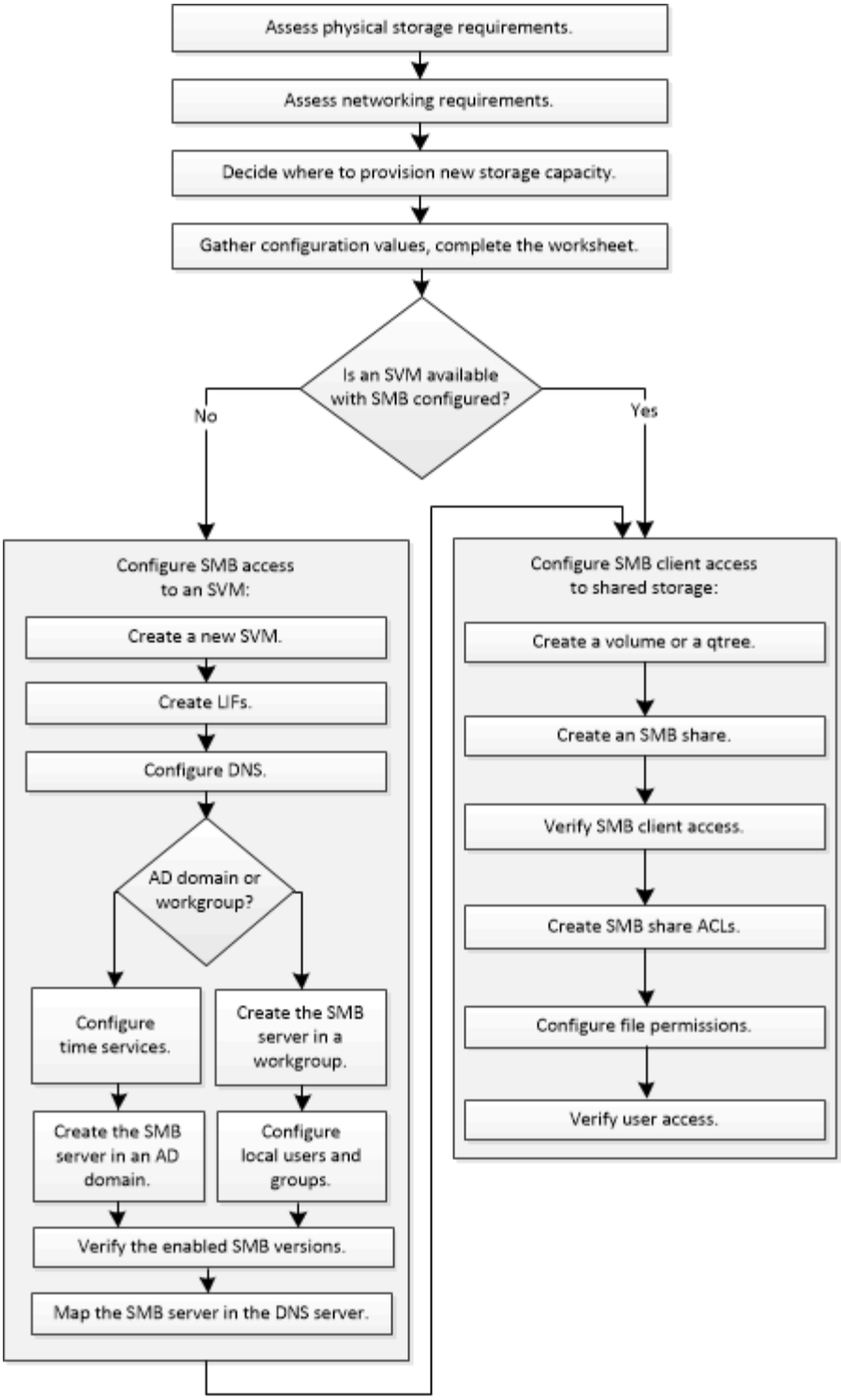
如果您想要瞭解ONTAP 有關各項功能的詳細資訊、請參閱 "SMB參考總覽"。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作…	請參閱…
重新設計的System Manager（ONTAP 提供更新版本的更新版本）	"使用SMB為Windows伺服器配置NAS儲存設備"
System Manager Classic（ONTAP 適用於更新版本的更新版本）	"SMB 組態概觀"

SMB 組態工作流程

設定SMB需要評估實體儲存設備和網路需求、然後選擇專屬於您目標的工作流程、設定SMB存取新的或現有的SVM、或將Volume或qtree新增至已完全設定為SMB存取的現有SVM。



準備

評估實體儲存需求

在為用戶端配置SMB儲存設備之前、您必須確保現有的集合體中有足夠的空間可容納新的磁碟區。如果沒有、您可以將磁碟新增至現有的Aggregate、或建立所需類型的新Aggregate。

步驟

1. 顯示現有Aggregate中的可用空間： `storage aggregate show`

   如果集合體有足夠的空間、請在工作表中記錄其名稱。

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 如果沒有具有足夠空間的集合體、請使用將磁碟新增至現有的集合體 `storage aggregate add-disks` 或使用建立新的 Aggregate `storage aggregate create` 命令。

評估網路需求

向用戶端提供SMB儲存設備之前、您必須確認網路設定正確、以符合SMB資源配置需求。

開始之前

必須設定下列叢集網路物件：

- 實體與邏輯連接埠
- 廣播網域
- 子網路（如有需要）
- IPspaces（視需要而定、除了預設IPspace）
- 容錯移轉群組（視需要、以及每個廣播網域的預設容錯移轉群組）
- 外部防火牆

步驟

1. 顯示可用的實體和虛擬連接埠： `network port show`
   - 如果可能、您應該使用資料網路速度最高的連接埠。
   - 資料網路中的所有元件必須具有相同的MTU設定、才能獲得最佳效能。

2. 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、請確認該子網路存在且有足夠的可用位址：`network subnet show`

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

3. 顯示可用的IPspaces： `network ipspace show`

   您可以使用預設IPspace或自訂IPspace。

4. 如果您要使用IPv6位址、請確認叢集上已啟用IPv6： `network options ipv6 show`

   如有需要、您可以使用啟用 IPv6 `network options ipv6 modify` 命令。

決定要在何處配置新的**SMB**儲存容量

在建立新的 SMB Volume 或 qtree 之前、您必須先決定要將它放在新的或現有的 SVM 中、以及 SVM 需要多少組態。此決定決定決定您的工作流程。

選擇

- 如果您想要在新的SVM上配置磁碟區或qtree、或是在已啟用SMB但尚未設定的現有SVM上配置、請完成「設定SMB存取SVM」和「將儲存容量新增至啟用SMB的SVM」中的步驟。

  設定SMB存取SVM

  設定SMB用戶端存取共享儲存設備

  如果符合下列任一項條件、您可以選擇建立新的SVM：

  - 您是第一次在叢集上啟用 SMB 。
  - 您在不想啟用 SMB 支援的叢集中有現有的 SVM 。
  - 叢集中有一個或多個啟用SMB的SVM、您需要下列其中一個連線：
    - 至不同的Active Directory樹系或工作群組。
    - 至隔離命名空間中的SMB伺服器（多租戶案例）。 您也應該選擇此選項、在已啟用 SMB 但尚未設定 SMB 的現有 SVM 上佈建儲存設備。如果您為SAN存取建立SVM、或是在建立SVM時未啟用任何傳輸協定、則可能會發生這種情況。

  在 SVM 上啟用 SMB 之後、請繼續配置 Volume 或 qtree 。

- 如果您想要在完全設定為SMB存取的現有SVM上配置磁碟區或qtree、請完成「將儲存容量新增至啟用SMB的SVM」中的步驟。

  設定SMB用戶端存取共享儲存設備

用於收集**SMB**組態資訊的工作表

SMB 組態工作表可讓您收集設定用戶端 SMB 存取所需的資訊。

您應該完成工作表的一或兩個區段、視您對儲存資源配置的決策而定：

- 如果您要設定SMB存取SVM、請完成這兩個部分。

  設定SMB存取SVM

  設定SMB用戶端存取共享儲存設備

- 如果您要將儲存容量新增至啟用 SMB 的 SVM 、則只需完成第二節。

  設定SMB用戶端存取共享儲存設備

命令手冊頁包含有關參數的詳細資料。

設定**SMB**存取**SVM**

*用於建立SVM*的參數

您可以將這些值提供給 `vserver create` 命令、如果您要建立新的 SVM 。

欄位	說明	您的價值
`-vserver`	您為新SVM提供的名稱、可以是完整網域名稱（FQDN）、也可以遵循另一種在叢集內強制執行唯一SVM名稱的慣例。	
`-aggregate`	叢集中有足夠空間容納新SMB儲存容量的集合體名稱。	
`-rootvolume`	您為SVM根磁碟區提供的唯一名稱。	
`-rootvolume-security-style`	使用 SVM 的 NTFS 安全樣式。	`ntfs`
`-language`	使用此工作流程中的預設語言設定。	`C.UTF-8`
`ipspace`	選用：IPspaces是SVM所在的不同IP位址空間。	

*用於建立LIF*的參數

您可以將這些值提供給 `network interface create` 建立生命時的命令。

欄位	說明	您的價值
`-lif`	您為新LIF提供的名稱。	
`-role`	在此工作流程中使用資料LIF角色。	`data`

欄位	說明	您的價值
`-data-protocol`	在此工作流程中、請僅使用 SMB 傳輸協定。	`cifs`
`-home-node`	LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。	
`-home-port`	LIF 在返回時傳回的連接埠或介面群組 `network interface revert` 命令會在LIF上執行。	
`-address`	叢集上的IPV4或IPv6位址、用於新LIF的資料存取。	
`-netmask`	LIF的網路遮罩和閘道。	
`-subnet`	IP位址集區。改用 `-address` 和 `-netmask` 自動指派位址和網路遮罩。	
`-firewall-policy`	在此工作流程中使用預設的資料防火牆原則。	`data`
`-auto-revert`	選用：指定資料LIF在啟動時或其他情況下是否自動還原至主節點。預設設定為 `false`。	

- DNS主機名稱解析參數*

您可以將這些值提供給 `vserver services name-service dns create` 設定 DNS 時的命令。

欄位	說明	您的價值
`-domains`	最多五個DNS網域名稱。	
`-name-servers`	每個DNS名稱伺服器最多三個IP位址。	

在**Active Directory**網域中設定**SMB**伺服器

時間服務組態的參數

您可以將這些值提供給 `cluster time-service ntp server create` 命令。

欄位	說明	您的價值
`-server`	Active Directory網域的NTP伺服器主機名稱或IP位址。	

在**Active Directory**網域中建立**SMB**伺服器的參數

您可以將這些值提供給 `vserver cifs create` 命令：建立新的 SMB 伺服器並指定網域資訊。

欄位	說明	您的價值
`-vserver`	要在其中建立SMB伺服器的SVM名稱。	
`-cifs-server`	SMB伺服器名稱（最多15個字元）。	
`-domain`	要與SMB伺服器建立關聯的Active Directory網域完整網域名稱（FQDN）。	
`-ou`	選用：Active Directory網域中與SMB伺服器相關聯的組織單位。依預設、此參數設為「CN=電腦」。	
`-netbios-aliases`	選用：NetBios別名清單、是SMB伺服器名稱的替代名稱。	
`-comment`	選用：伺服器的文字註解。瀏覽網路上的伺服器時、Windows用戶端可以看到此SMB伺服器說明。	

在工作群組中設定**SMB**伺服器

在工作群組中建立**SMB**伺服器的參數

您可以將這些值提供給 `vserver cifs create` 命令：當您建立新的 SMB 伺服器並指定支援的 SMB 版本時。

欄位	說明	您的價值
`-vserver`	要在其中建立SMB伺服器的SVM名稱。	
`-cifs-server`	SMB伺服器名稱（最多15個字元）。	

欄位	說明	您的價值
`-workgroup`	工作群組名稱（最多15個字元）。	
`-comment`	選用：伺服器的文字註解。瀏覽網路上的伺服器時、Windows用戶端可以看到此SMB伺服器說明。	

建立本機使用者的參數

您可以在使用建立本機使用者時提供這些值 `vserver cifs users-and-groups local-user create` 命令。工作群組中的SMB伺服器和AD網域中的選用伺服器都需要這些伺服器。

欄位	說明	您的價值
`-vserver`	要在其中建立本機使用者的SVM名稱。	
`-user-name`	本機使用者名稱（最多20個字元）。	
`-full-name`	選用：使用者的全名。如果全名包含空格、請將全名括在雙引號內。	
`-description`	選用：本機使用者的說明。如果說明包含空格、請將參數括在引號中。	
`-is-account-disabled`	選用：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。	

建立本機群組的參數

您可以在使用建立本機群組時提供這些值 `vserver cifs users-and-groups local-group create` 命令。對於AD網域和工作群組中的SMB伺服器而言、它們是選用的。

欄位	說明	您的價值
`-vserver`	要在其中建立本機群組的SVM名稱。	
`-group-name`	本機群組名稱（最多256個字元）。	
`-description`	選用：本機群組的說明。如果說明包含空格、請將參數括在引號中。	

將儲存容量新增至啟用 **SMB** 的 **SVM**

建立**Volume**的參數

您可以將這些值提供給 `volume create` 如果您要建立的是 Volume 而非 qtree 、則為命令。

欄位	說明	您的價值
`-vserver`	將裝載新磁碟區的新SVM或現有SVM名稱。	
`-volume`	您為新磁碟區提供的唯一描述性名稱。	
`-aggregate`	叢集中有足夠空間可容納新SMB Volume的集合體名稱。	
`-size`	您為新磁碟區大小所提供的整數。	
`-security-style`	此工作流程使用NTFS安全樣式。	`ntfs`
`-junction-path`	要掛載新磁碟區的根目錄（/）下的位置。	

用於建立**qtree**的參數

您可以將這些值提供給 `volume qtree create` 如果您要建立 qtree 而非 Volume 、請執行命令。

欄位	說明	您的價值
`-vserver`	包含qtree之磁碟區所在的SVM名稱。	
`-volume`	將包含新qtree的磁碟區名稱。	
`-qtree`	您為新qtree提供的唯一描述性名稱、64個字元或更少。	
`-qtree-path`	格式中的 qtree path 引數 `/vol/volume_name/qtree_name\>` 可以指定、而非將 Volume 和 qtree 指定為個別的引數。	

建立**SMB**共用的參數

您可以將這些值提供給 `vserver cifs share create` 命令。

欄位	說明	您的價值
`-vserver`	要在其中建立SMB共用區的SVM名稱。	
`-share-name`	您要建立的SMB共用區名稱（最多256個字元）。	
`-path`	SMB共用區路徑名稱（最多256個字元）。此路徑必須存在於磁碟區中、才能建立共用區。	
`-share-properties`	選用：共用內容清單。預設設定為 `oplocks`、 `browsable`、 `changenotify`和 `show-previous-versions`。	
`-comment`	選用：伺服器的文字註解（最多256個字元）。在網路上瀏覽時、Windows用戶端可以看到此SMB共用說明。	

建立**SMB**共用存取控制清單（**ACL**）的參數

您可以將這些值提供給 `vserver cifs share access-control create` 命令。

欄位	說明	您的價值
`-vserver`	要在其中建立SMB ACL的SVM名稱。	
`-share`	要在其中建立的SMB共用區名稱。	
`-user-group-type`	要新增至共用ACL的使用者或群組類型。預設類型為 `windows`	`windows`
`-user-or-group`	要新增至共用ACL的使用者或群組。如果您指定使用者名稱、則必須使用「domain\userName」格式來包含使用者的網域。	
`-permission`	指定使用者或群組的權限。	`[No_access
Read	Change	Full_Control]`

設定SMB存取SVM

設定SMB存取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SVM

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。如需詳細資訊、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 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**SVM**根磁碟區的匯出原則

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LIF

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已設定為系統管理 `up` 狀態。
- 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。

- 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）。
- 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。。 `network route create` 手冊頁包含在 SVM 中建立靜態路由的相關資訊。
- 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
```

啟用DNS進行主機名稱解析

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。

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。。 `vserver services name-service dns create` 如果只輸入一個 DNS 伺服器名稱、命令會發出警告。

關於這項工作

網路管理指南_包含在SVM上設定動態DNS的相關資訊。

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
   ```

   > 從 ONTAP 9.2 開始 `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` 命令可從 ONTAP 9.2 開始使用。

```
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

設定時間服務

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、使其使用與Active Directory網域相同的NTP伺服器進行時間同步。

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
```

用於管理**NTP**伺服器上對稱驗證的命令

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`

在**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。

。 `vserver cifs` 手冊頁包含其他選用參數和命名要求。

> 從ONTAP 推出支援支援功能的支援功能升級至支援功能的SMB 2.0版、即可連線至網域控制器（DC）。如果您已在網域控制器上停用SMB 1.0、就必須這麼做。從0：9.2開始ONTAP 、預設會啟用SMB 2.0。

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`

   隨附 SMB 授權 "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: . . .
```

建立用於**SMB**驗證的**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

在工作群組總覽中設定**SMB**伺服器

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。

在工作群組中建立**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）

。 `vserver cifs` 手冊頁包含其他選用的組態參數和命名需求。

步驟

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

   隨附 SMB 授權 "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。

- `vserver cifs users-and-groups local-user` 手冊頁包含有關可選參數和命名要求的詳細信息。

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。

- `vserver cifs users-and-groups local-group` 手冊頁包含有關可選參數和命名要求的詳細信息。

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**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。

在支援支援功能的支援中、預設會針對用戶端連線啟用SMB 2.0版及更新版本、但預設啟用的SMB 1.0版本則取決於您的版本。ONTAP ONTAP

- 從ONTAP SVM開始、即可停用SVM上的SMB 1.0。
  - `-smb1-enabled` 選項 `vserver cifs options modify` 命令可啟用或停用 SMB 1.0 。
- 從功能更新9.3開始ONTAP 、它在新的SVM上預設為停用。

如果您的SMB伺服器位於Active Directory（AD）網域中、您可以啟用SMB 2.0來連線至以ONTAP 支援功能9.1

開頭的網域控制器（DC）。如果您已在DC上停用SMB 1.0、就必須這麼做。從ONTAP 0：9.2開始、預設會啟用SMB 2.0以進行DC連線。

> 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
```

   - 若要停用 SMB 版本：

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

     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
```

1. 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
     ```

2. 返回管理權限層級：

   ```
   set -privilege admin
   ```

對應DNS伺服器上的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。

設定SMB用戶端存取共享儲存設備

設定SMB用戶端存取共享儲存設備

若要讓SMB用戶端存取SVM上的共享儲存設備、您必須建立一個Volume或qtree以提供儲存容器、然後建立或修改該容器的共用區。然後您可以設定共用和檔案權限、並測試用戶

端系統的存取。

開始之前

- 必須在 SVM 上完全設定 SMB 。
- 您名稱服務組態的任何更新都必須完成。
- 對Active Directory網域或工作群組組態的任何新增或修改都必須完成。

建立Volume或qtree儲存容器

建立Volume

您可以使用建立 Volume 並指定其連接點和其他屬性 `volume create` 命令。

關於這項工作

磁碟區必須包含_交會路徑_、才能讓用戶端使用其資料。您可以在建立新磁碟區時指定交會路徑。如果您在建立磁碟區時未指定連接路徑、則必須使用 _ 掛載 _ SVM 命名空間中的磁碟區 `volume mount` 命令。

開始之前

- 應設定並執行 SMB 。
- SVM 安全樣式必須是 NTFS 。
- 從 ONTAP 9.13.1 開始、您可以使用容量分析和活動追蹤功能來建立 Volume 。若要啟用容量或活動追蹤、請核發 `volume create` 命令 `-analytics-state` 或 `-activity-tracking-state` 設定為 `on`。

  若要深入瞭解容量分析和活動追蹤、請參閱 啟用檔案系統分析。

步驟

1. 建立具有交會點的Volume： `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path` *`junction_path`*]

   的選擇 `-junction-path` 以下是：

   - 直接位於根目錄下、例如 `/new_vol`

     您可以建立新磁碟區、並指定將其直接掛載到SVM根磁碟區。

   - 在現有目錄下、例如 `/existing_dir/new_vol`

     您可以建立新磁碟區、並指定將其掛載至現有磁碟區（在現有階層架構中）、以目錄形式表示。

   如果您想在新目錄中建立磁碟區（在新磁碟區下的新階層中）、例如：`/new_dir/new_vol`接著、您必須先建立與 SVM 根 Volume 相關的新父 Volume 。接著、您會在新父Volume（新目錄）的交會路徑中建立新的子Volume。

2. 確認已使用所需的交會點建立磁碟區： `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

範例

下列命令會在SVM vs1.example.com和Aggr1上建立名為user1的新磁碟區。新的 Volume 可在取得 `/users`。磁碟區大小為750 GB、磁碟區保證為磁碟區類型（預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                          Junction                 Junction
Vserver           Volume  Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1  true     /users          RW_volume
```

下列命令會在SVM上建立一個名為「'home4'」的新磁碟區：vs1.example.com`"和Aggr1'集合體。目錄 `/eng/` VS1 SVM 的命名空間已存在、新的 Volume 可從取得 `/eng/home`、成為的主目錄 `/eng/` 命名空間。磁碟區大小為 750 GB 、其磁碟區保證屬於類型 `volume` （預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                         Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

建立**qtree**

您可以建立 qtree 來包含資料、並使用來指定其內容 `volume qtree create` 命令。

開始之前

- SVM和將要包含新qtree的Volume必須已經存在。
- SVM安全樣式必須為NTFS、且SMB必須設定並執行。

步驟

1. 建立qtree： `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   您可以將 Volume 和 qtree 指定為個別的引數、或以格式指定 qtree 路徑引數 `/vol/volume_name/_qtree_name`。

2. 確認qtree是以所需的交會路徑建立： `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

範例

以下範例建立一個 qtree 、名稱為 qt01 、位於 SVM vs1.example.com 上、具有交會路徑 `/vol/data1`：

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                   Security Style: ntfs
                      Oplock Mode: enable
                 Unix Permissions: ---rwxr-xr-x
                         Qtree Id: 2
                     Qtree Status: normal
                    Export Policy: default
        Is Export Policy Inherited: true
```

建立SMB共用區的需求與考量

在建立SMB共用區之前、您必須先瞭解共用路徑和共用內容的需求、尤其是對於主目錄。

建立 SMB 共用需要指定目錄路徑結構（使用 `-path` 中的選項 `vserver cifs share create` 命令）。目錄路徑會對應到您在SVM命名空間中建立之磁碟區或qtree的交會路徑。建立共用區之前、目錄路徑和對應的交會路徑必須存在。

共用路徑有下列需求：

- 目錄路徑名稱最長可達255個字元。
- 如果路徑名稱中有空格、則必須將整個字串放在引號中（例如、 `"/new volume/mount here"`）。
- 如果是 UNC 路徑 (`\\servername\sharename\filepath`）共享區包含超過 256 個字元（不包括 UNC 路徑中的初始「」）、則 Windows 內容方塊中的 * 安全性 * 索引標籤無法使用。

  這是Windows用戶端問題、而非ONTAP 功能不均的問題。為避免此問題、請勿使用超過256個字元的UNC路徑建立共用。

共用內容預設值可以變更：

- 所有共用的預設初始屬性為 `oplocks`、 `browsable`、 `changenotify`和 `show-previous-versions`。
- 您可以在建立共用時指定共用內容。

不過、如果您在建立共用時確實指定共用內容、則不會使用預設值。如果您使用 `-share-properties` 參數建立共用時、您必須使用逗號分隔的清單、指定要套用至共用的所有共用屬性。

- 若要指定主目錄共用、請使用 `homedirectory` 屬性。

  此功能可讓您根據連線的使用者及一組變數、設定對應至不同目錄的共用區。您不需要為每個使用者建立個別的共用區、而是使用幾個主目錄參數來設定單一共用區、以定義使用者在入口點（共用區）及其主目錄（SVM上的目錄）之間的關係。

  > 您無法在建立共用之後新增或移除此內容。

主目錄共用具有下列需求：

- 在建立 SMB 主目錄之前、您必須使用新增至少一個主目錄搜尋路徑 `vserver cifs home-directory search-path add` 命令。
- 主目錄共用、由的值指定 `homedirectory` 在上 `-share-properties` 參數必須包含 `%w` （ Windows 使用者名稱）共用名稱中的動態變數。

  共用名稱也可以包含 `%d` （網域名稱）動態變數（例如、 `%d/%w`）或共享區名稱中的靜態部分（例如、`home1_%w`）。

- 如果系統管理員或使用者使用共用來連線至其他使用者的主目錄（使用的選項） `vserver cifs home-directory modify` 命令）、動態共用名稱模式必須在開頭加上代字符號 (~)。

"中小企業管理" 和 `vserver cifs share` 手冊頁包含其他資訊。

建立SMB共用區

您必須先建立SMB共用區、才能與SMB用戶端共用SMB伺服器的資料。建立共用時、您可以設定共用內容、例如將共用區指定為主目錄。您也可以設定選用的設定來自訂共用區。

開始之前

在建立共用之前、磁碟區或qtree的目錄路徑必須存在於SVM命名空間中。

關於這項工作

建立共用時、預設的共用 ACL （預設共用權限）為 `Everyone / Full Control`。在測試共用區的存取之後、您應該移除預設的共用ACL、並改用更安全的替代方法。

步驟

1. 如有必要、請建立共用的目錄路徑結構。

   - `vserver cifs share create` 命令會檢查中指定的路徑 `-path` 共享區建立期間的選項。如果指定的路徑不存在、則命令會失敗。

2. 建立與指定SVM相關的SMB共用區： `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. 確認共用區已建立：`vserver cifs share show -share-name share_name`

範例

下列命令會在 SVM 上建立名為「 HARE1 」的 SMB 共用區 `vs1.example.com`。其目錄路徑為 `/users`，然後使用預設內容建立。

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

驗證SMB用戶端存取

您應該存取並寫入資料至共用區、以確認SMB設定正確。您應該使用SMB伺服器名稱和任何NetBios別名來測試存取。

步驟

1. 登入Windows用戶端。
2. 使用SMB伺服器名稱進行測試存取：

   a. 在 Windows 檔案總管中、以下列格式將磁碟機對應至共用區： `\\\SMB_Server_Name\Share_Name`

      如果對應不成功、則DNS對應可能尚未傳播到整個網路。您必須在稍後使用SMB伺服器名稱來測試存取。

      如果 SMB 伺服器名稱為 vs1.example.com 、且共用名稱為 share1 、則應輸入下列內容： `\\vs0.example.com\SHARE1`

   b. 在新建立的磁碟機上、建立測試檔案、然後刪除該檔案。

   您已使用SMB伺服器名稱驗證共用的寫入存取權。

3. 對任何NetBios別名重複步驟2。

建立SMB共用存取控制清單

建立SMB共用區的存取控制清單（ACL）來設定共用權限、可讓您控制使用者和群組對共用區的存取層級。

開始之前

您必須決定要授予哪些使用者或群組存取該共用區的權限。

關於這項工作

您可以使用本機或網域Windows使用者或群組名稱來設定共用層級ACL。

建立新 ACL 之前、您應該先刪除預設的共用 ACL `Everyone / Full Control`，這會帶來安全風險。

在工作群組模式中、本機網域名稱是SMB伺服器名稱。

步驟

1. 刪除預設的共用 ACL ：`vserver cifs share access-control delete -vserver *vserver_name* -share *share_name* -user-or-group everyone`
2. 設定新ACL：

如果您想要使用...來設定**ACL**	輸入命令...
Windows使用者	`vserver cifs share access-control create -vserver *vserver_name* -share *share_name* -user-group-type windows -user-or-group *Windows_domain_name*\\*user_name* -permission access_right`
Windows群組	`vserver cifs share access-control create -vserver *vserver_name* -share *share_name* -user-group-type windows -user-or-group *Windows_group_name* -permission access_right`

3. 使用驗證套用至共用的 ACL 是否正確 `vserver cifs share access-control show` 命令。

範例

下列命令提供 `Change` 「銷售團隊」 Windows 群組在「 vs1.example.com`"SVM: 」上的「銷售」共用區的權限

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

下列命令會提供 `Change` 允許本機Windows群組名為「老虎團隊」和 `Full_Control` 本機 Windows 使用者在「 'VS1' SVM 」上的「 datavol5 」共用區的「 Shue Chang 」權限：

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

設定共用區中的NTFS檔案權限

若要讓具有共用存取權的使用者或群組能夠存取檔案、您必須從Windows用戶端設定該共用區中檔案和目錄的NTFS檔案權限。

開始之前

執行此工作的系統管理員必須擁有足夠的NTFS權限、才能變更所選物件的權限。

關於這項工作

"中小企業管理" 而您的Windows文件則包含如何設定標準和進階NTFS權限的相關資訊。

步驟

1. 以系統管理員身分登入Windows用戶端。
2. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
3. 填寫*對應網路磁碟機*方塊：
   a. 選取*磁碟機*字母。
   b. 在 * 資料夾 * 方塊中、輸入 SMB 伺服器名稱、其中包含您要套用權限的資料、以及共用名稱。

      如果您的 SMB 伺服器名稱為 smb_server01 、而您的共用名稱為「 'SPARE1' 」、則您必須輸入 `\\SMB_SERVER01\SHARE1`。

> 您可以指定 SMB 伺服器的資料介面 IP 位址、而非 SMB 伺服器名稱。

c. 單擊*完成*。

您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

4. 選取您要設定NTFS檔案權限的檔案或目錄。
5. 以滑鼠右鍵按一下檔案或目錄、然後選取*內容*。
6. 選取*安全性*索引標籤。

   「安全性」索引標籤會顯示已設定NTFS權限的使用者和群組清單。「物件的權限」方塊會顯示所選使用者或群組有效的「允許」和「拒絕」權限清單。

7. 按一下 * 編輯 * 。

   「物件的權限」方塊隨即開啟。

8. 執行所需的動作：

如果你想...	請執行下列動作...
設定新使用者或群組的標準NTFS權限	a. 按一下「 * 新增 * 」。 「選取使用者、電腦、服務帳戶或群組」視窗即會開啟。 b. 在「輸入要選取的物件名稱」方塊中、輸入您要新增NTFS權限的使用者或群組名稱。 c. 按一下「確定」。
變更或移除使用者或群組的標準NTFS權限	在*群組或使用者名稱*方塊中、選取您要變更或移除的使用者或群組。

9. 執行所需的動作：

如果您想要...	請執行下列動作
為新的或現有的使用者或群組設定標準NTFS權限	在「物件權限>」方塊中、針對您要允許或不允許選取的使用者或群組存取的類型、選取*允許*或*拒絕*方塊。
移除使用者或群組	按一下「移除」。

> 如果部分或全部的標準權限方塊無法選取、這是因為權限是從父物件繼承而來。*特殊權限*方塊無法選取。如果選取此選項、表示已為選取的使用者或群組設定一或多個精細的進階權限。

10. 在您完成新增、移除或編輯該物件的NTFS權限之後、請按一下「確定」。

驗證使用者存取權

您應該測試您設定的使用者是否可以存取SMB共用區及其所包含的檔案。

步驟

1. 在Windows用戶端上、以目前擁有共用存取權的其中一位使用者身分登入。
2. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
3. 填寫*對應網路磁碟機*方塊：

   a. 選取*磁碟機*字母。

   b. 在*資料夾*方塊中、輸入您要提供給使用者的共用名稱。

      如果您的 SMB 伺服器名稱為 smb_server01 、而您的共用名稱為「 'SPARE1' 」、則您必須輸入 `\\SMB_SERVER01\share1`。

   c. 單擊*完成*。

   您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

4. 建立測試檔案、確認其存在、將文字寫入其中、然後移除測試檔案。