利用ONTAP Hyper-V和SQL Server、透過SMB建立不中斷營運的支援組態

ONTAP 9

NetApp
February 12, 2026

目錄

利用ONTAP Hyper-V和SQL Server、透過SMB建立不中斷營運的支援組態

利用ONTAP Hyper-V和SQL Server over SMB總覽建立不中斷營運的支援組態

您必須執行幾ONTAP 個支援功能的組態步驟、才能準備好在SMB上執行不中斷營運的Hyper-V和SQL Server安裝。

在您透過ONTAP SMB建立不中斷營運的Hyper-V和SQL Server的支援功能之前、必須先完成下列工作：

- 必須在叢集上設定時間服務。
- 必須為SVM設定網路。
- 必須建立SVM。
- 必須在SVM上設定資料LIF介面。
- 必須在SVM上設定DNS。
- 必須為SVM設定所需的名稱服務。
- 必須建立 SMB 伺服器。

相關資訊

透過SMB組態規劃Hyper-V或SQL Server

組態需求與考量

驗證是否同時允許Kerberos和NTLMv2驗證（Hyper-V over SMB共享）

Hyper-V over SMB的不中斷營運需要資料SVM和Hyper-V伺服器上的CIFS伺服器同時允許Kerberos和NTLMv2驗證。您必須驗證CIFS伺服器和Hyper-V伺服器上的設定、以控制允許的驗證方法。

關於這項工作

建立持續可用的共用連線時、必須進行Kerberos驗證。遠端VSS程序的一部分使用了NTLMv2驗證。因此、Hyper-V over SMB組態必須支援使用這兩種驗證方法的連線。

下列設定必須設定為允許Kerberos和NTLMv2驗證：

- 必須在儲存虛擬機器（SVM）上停用SMB的匯出原則。

在SVM上一律會啟用Kerberos和NTLMv2驗證、但匯出原則可用來根據驗證方法來限制存取。

SMB的匯出原則是選用的、預設為停用。如果停用匯出原則、則CIFS伺服器預設會允許Kerberos和NTLMv2驗證。

- CIFS伺服器和Hyper-V伺服器所屬的網域必須同時允許Kerberos和NTLMv2驗證。

Active Directory網域預設會啟用Kerberos驗證。不過、可以使用「安全性原則」設定或「群組原則」來禁止NTLMv2驗證。

步驟

1. 請執行下列步驟、確認SVM上的匯出原則已停用：
   a. 將權限層級設為進階：

      set -privilege advanced

   b. 確認 `-is-exportpolicy-enabled` CIFS 伺服器選項設為 `false`：

      vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

   c. 返回管理權限層級：

      set -privilege admin

2. 如果未停用SMB的匯出原則、請停用這些原則：

   vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. 確認網域中同時允許使用NTLMv2和Kerberos驗證。

   如需判斷網域中允許使用哪些驗證方法的相關資訊，請參閱Microsoft TechNet程式庫。

4. 如果網域不允許NTMLv2驗證、請使用Microsoft文件中所述的其中一種方法來啟用NTLMv2驗證。

範例

下列命令可驗證SVM VS1上的SMB匯出原則是否已停用：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

確認網域帳戶對應至 ONTAP 中的預設 UNIX 使用者

Hyper-V和SQL Server使用網域帳戶建立SMB連線、以連線至持續可用的共用區。若要成功建立連線、電腦帳戶必須成功對應至UNIX使用者。完成此作業最方便的方法是將電腦帳戶對應至預設UNIX使用者。

關於這項工作

Hyper-V和SQL Server使用網域電腦帳戶建立SMB連線。此外、SQL Server也會使用網域使用者帳戶做為進行SMB連線的服務帳戶。

建立儲存虛擬機器 (SVM) 時，ONTAP 會自動建立名為 `pcuser` （UID 為 `65534`) 和名為 `pcuser` （GID 為 `65534` ），並將預設使用者新增至 `pcuser`團體。如果您要在將叢集升級Data ONTAP 至S8.2之前、在現有的AnSVM上設定Hyper-V over SMB解決方案、則預設使用者和群組可能不存在。如果沒有、您必須先建立這些項目、才能設定CIFS伺服器的預設UNIX使用者。

步驟

1. 判斷是否有預設的UNIX使用者：

```
vserver cifs options show -vserver <vserver_name>
```

2. 如果未設定預設使用者選項、請判斷是否有UNIX使用者可以指定為預設UNIX使用者：

```
vserver services unix-user show -vserver <vserver_name>
```

3. 如果未設定預設用戶選項，且沒有可指定為預設 UNIX 用戶的 UNIX 用戶，則建立預設群組和預設 UNIX 用戶，並將預設用戶新增至該群組。

   通常，預設使用者的使用者名稱是“pcuser”，並且必須分配 UID `65534` .預設群組一般被賦予群組名稱“pcuser”。指派給群組的 GID 必須是 `65534`。

   a. 建立預設群組：

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

   b. 建立預設使用者、並將預設使用者新增至預設群組：

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

   c. 確認已正確設定預設使用者和預設群組：

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

4. 如果未設定CIFS伺服器的預設使用者、請執行下列步驟：
   a. 設定預設使用者：

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

   b. 確認預設UNIX使用者已正確設定：

```
vserver cifs options show -vserver <vserver_name>
```

5. 若要驗證應用程式伺服器的電腦帳戶是否正確對應至預設使用者、請將磁碟機對應至 SVM 上的共用、然後使用確認 Windows 使用者與 UNIX 使用者的對應 `vserver cifs session show` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver cifs options`資訊，請參閱。

範例

。 `pcuser`使用者被指定為 SVM vs1 上的 CIFS 伺服器的預設使用者。

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
```

```
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

確認**SVM**根磁碟區的安全樣式已設定為**NTFS**

為了確保Hyper-V和SQL Server在SMB上的不中斷營運成功、磁碟區必須以NTFS安全型態建立。由於根磁碟區的安全性樣式預設會套用至儲存虛擬機器（SVM）上建立的磁碟區、因此根磁碟區的安全性樣式應設定為NTFS。

關於這項工作

- 您可以在建立SVM時指定根磁碟區的安全樣式。
- 如果建立 SVM 時根磁碟區未設定為 NTFS 安全樣式、您可以稍後使用變更安全樣式 `volume modify` 命令。

步驟

1. 判斷SVM根磁碟區目前的安全樣式：

   `volume show -vserver *vserver_name* -fields vserver,volume,security-style`

2. 如果根磁碟區不是NTFS安全型磁碟區、請將安全樣式變更為NTFS：

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. 確認SVM根磁碟區已設定為NTFS安全樣式：

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

範例

下列命令可驗證SVM VS1上的根磁碟區安全樣式是否為NTFS：

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

確認已設定必要的CIFS伺服器選項

您必須確認已根據Hyper-V和SQL Server在SMB上的不中斷營運需求、啟用並設定所需的CIFS伺服器選項。

關於這項工作

- 必須啟用SMB 2.x和SMB 3.0。
- 必須啟用ODX複本卸載、才能使用效能提升的複本卸載功能。
- 如果Hyper-V over SMB解決方案使用支援遠端VSS的備份服務（僅限Hyper-V）、則必須啟用VSS陰影複製服務。

步驟

1. 確認儲存虛擬機器（SVM）上已啟用所需的CIFS伺服器選項：
   a. 將權限層級設為進階：

      set -privilege advanced

   b. 輸入下列命令：

      vserver cifs options show -vserver *vserver_name*

下列選項應設定為 `true`：

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` （僅適用於 Hyper-V ）

2. 如果任何選項未設定為 `true`，請執行下列步驟：
   a. 將它們設為 `true` 使用 `vserver cifs options modify` 命令。
   b. 確認選項已設定為 `true` 使用 `vserver cifs options show` 命令。
3. 返回管理權限層級：

```
set -privilege admin
```

範例

下列命令可驗證SVM VS1上是否已啟用Hyper-V over SMB組態所需的選項。在此範例中、ODX複本卸載必須啟用、才能符合選項需求。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

設定SMB多通道以獲得效能與備援

從支援支援支援的9.4開始ONTAP 、您可以設定SMB多通道、ONTAP 在單一SMB工作階

段中、在支援的情況下提供多個連接功能。這樣做可改善Hyper-V和SQL Server在SMB組態上的處理量和容錯能力。

開始之前

只有當用戶端在SMB 3.0或更新版本上進行交涉時、才能使用SMB多通道功能。根據預設、SMB 3.0及更新版本會在ONTAP 支援SMB的伺服器上啟用。

關於這項工作

如果ONTAP 在故障叢集上識別出適當的組態、SMB用戶端會自動偵測並使用多個網路連線。

SMB工作階段中的同時連線數目取決於您已部署的NIC：

- *用戶端和ONTAP 叢集上的1G NIC *

  用戶端每個NIC建立一個連線、並將工作階段連結至所有連線。

- *用戶端與ONTAP 支援叢集*上的10G與更大容量NIC

  用戶端每個NIC最多可建立四個連線、並將工作階段連結至所有連線。用戶端可在多個10G和更大容量的NIC上建立連線。

您也可以修改下列參數（進階權限）：

- `-max-connections-per-session`

  每個多通道工作階段允許的最大連線數。預設為32個連線。

  如果您想要啟用比預設值更多的連線、則必須對用戶端組態進行類似的調整、也就是預設的32個連線。

- `-max-lifs-per-session`

  每個多通道工作階段所通告的網路介面數量上限。預設為256個網路介面。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 在SMB伺服器上啟用SMB多通道：

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. 驗證ONTAP 此功能是否回報SMB多通道工作階段：

```
vserver cifs session show
```

4. 返回管理權限層級：

```
set -privilege admin
```

範例

下列範例顯示所有SMB工作階段的相關資訊、顯示單一工作階段的多個連線：

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                  0
4s
                                    Administrator
```

下列範例顯示使用工作階段ID 1之SMB工作階段的詳細資訊：

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
                Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
                Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

建立NTFS資料磁碟區

您必須先在儲存虛擬機器（SVM）上建立NTFS資料磁碟區、然後才能透過SMB應用程式伺服器設定持續可用的共用區、以便搭配Hyper-V或SQL Server使用。使用Volume組態工作表建立資料磁碟區。

關於這項工作

您可以使用選用參數來自訂資料Volume。如需自訂磁碟區的詳細資訊、請參閱 "邏輯儲存管理"。

建立資料磁碟區時、不應在包含下列項目的磁碟區內建立交會點：

- Hyper-V檔案ONTAP 、用於製作陰影複製
- 使用SQL Server備份的SQL Server資料庫檔案

> 如果您不慎建立使用混合式或UNIX安全性樣式的磁碟區、則無法將磁碟區變更為NTFS安全性樣式磁碟區、然後直接使用它來建立持續可用的共用區、以利不中斷營運。除非將組態中使用的磁碟區建立為NTFS安全型磁碟區、否則Hyper-V和SQL Server在SMB上的不中斷營運將無法正常運作。您必須刪除磁碟區並以NTFS安全型態重新建立磁碟區、 或者、您也可以在Windows主機上對應磁碟區、並在磁碟區頂端套用ACL、然後將ACL傳播到磁碟區中的所有檔案和資料夾。

步驟

1. 輸入適當的命令來建立資料Volume：

如果您想要在**SVM**中建立磁碟區、而根磁碟區的安全樣式是...	輸入命令...
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
非NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path**

2. 驗證Volume組態是否正確：

   volume show -vserver *vserver_name* -volume *volume_name*

建立持續可用的**SMB**共用區

建立資料磁碟區之後、您可以建立持續可用的共用區、讓應用程式伺服器用來存取Hyper-V虛擬機器、組態檔和SQL Server資料庫檔案。您應該在建立SMB共用時使用共用組態工作表。

步驟

1. 顯示現有資料磁碟區及其交會路徑的相關資訊：

   volume show -vserver *vserver_name* -junction

2. 建立持續可用的SMB共用區：

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - 您可以選擇性地將註解新增至共用組態。
   - 根據預設、離線檔案共用屬性是在共用上設定、並設為 `manual`。
   - ONTAP 會建立具有 Windows 預設共用權限的共用 `Everyone / Full Control`。

3. 針對共用組態工作表中的所有共用重複上一個步驟。
4. 使用確認您的組態正確無誤 `vserver cifs share show` 命令。
5. 將磁碟機對應至每個共用區、並使用* Windows內容*視窗設定檔案權限、即可在持續可用的共用區上設定NTFS檔案權限。

範例

下列命令可在儲存虛擬機器（SVM、先前稱為Vserver）VS1上建立名為「data2」的持續可用共用區。透過設定、符號連結會停用 `-symlink` 參數至 `""`：

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

將SeSecurityPrivilege權限新增至使用者帳戶（適用於SMB共用的SQL Server）

用於安裝SQL伺服器的網域使用者帳戶必須指派「eSecurity權限」權限、才能在CIFS伺服器上執行某些動作、而這些動作需要預設未指派給網域使用者的權限。

開始之前

用於安裝SQL Server的網域帳戶必須已經存在。

關於這項工作

將權限新增至SQL Server安裝程式的帳戶時ONTAP 、可能會聯絡網域控制器來驗證帳戶。如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 新增「eSecurity權限」權限：

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   的值 `-user-or-group-name` 參數是用於安裝 SQL Server 的網域使用者帳戶名稱。

2. 確認已將權限套用至帳戶：

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

範例

下列命令會在儲存虛擬機器（SVM）VS1的範例網域中、將「『安全性權限』」權限新增至SQL Server安裝程式的帳戶：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

設定VSS陰影複製目錄深度（適用於SMB共用上的Hyper-V）

您也可以在SMB共用區內設定最大目錄深度、以便建立陰影複製。如果您想要手動控制ONTAP 子目錄的最大層級、以便在其中建立陰影複製、則此參數非常實用。

開始之前

必須啟用VSS陰影複製功能。

關於這項工作

預設為建立最多五個子目錄的陰影複本。如果值設為 `0`， ONTAP 會為所有子目錄建立陰影複本。

> 雖然您可以指定陰影複製集目錄深度包含五個子目錄或所有子目錄、但Microsoft要求陰影複製集建立必須在60秒內完成。如果目前無法完成陰影複製集建立、則陰影複製集會失敗。您選擇的陰影複製目錄深度不得導致建立時間超過時間限制。

步驟

1. 將權限層級設為進階：

   set -privilege advanced

2. 將VSS陰影複製目錄深度設定為所需的層級：

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
integer

vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. 返回管理權限層級：

```
set -privilege admin
```

版權資訊

商標資訊