



Microsoft Hyper-V和SQL Server的SMB組態 ONTAP 9

NetApp
April 24, 2024

目錄

Microsoft Hyper-V和SQL Server的SMB組態	1
Microsoft Hyper-V與SQL Server的SMB組態總覽	1
設定ONTAP 適用於Microsoft Hyper-V和SQL Server over SMB解決方案的支援功能	1
不中斷營運：透過SMB執行Hyper-V和SQL Server	2
使用遠端VSS進行共用型備份	6
ODX複製卸載如何透過SMB共用搭配Hyper-V和SQL Server使用	9
組態需求與考量	10
SQL Server與Hyper-V over SMB組態的建議	17
透過SMB組態規劃Hyper-V或SQL Server	17
利用ONTAP Hyper-V和SQL Server、透過SMB建立不中斷營運的支援組態	21
透過SMB組態管理Hyper-V和SQL Server	34
使用統計資料、透過SMB監控Hyper-V和SQL Server活動	37
驗證組態是否能夠不中斷營運	41

Microsoft Hyper-V和SQL Server的SMB組態

Microsoft Hyper-V與SQL Server的SMB組態總覽

利用支援支援的功能、您可以透過SMB傳輸協定、為兩個Microsoft應用程式啟用不中斷營運：Microsoft Hyper-V和Microsoft SQL Server。ONTAP

如果您想在下列情況下實作SMB不中斷營運、請使用這些程序：

- 已設定基本SMB傳輸協定檔案存取。
- 您想要啟用位於SVM中的SMB 3.0或更新版本檔案共用、以儲存下列物件：
 - Hyper-V虛擬機器檔案
 - SQL Server系統資料庫

相關資訊

如需 ONTAP 技術和與外部服務互動的其他資訊、請參閱下列技術報告（TR）：

- ["NetApp技術報告4172：Microsoft Hyper-V over SMB 3.0 with ONTAP NetApp最佳實務做法"](#)
- ["NetApp技術報告4369..適用於Microsoft SQL Server的最佳實務做法、SnapManager 以及適用於SQL Server with叢集Data ONTAP 式的版本"](#)

設定ONTAP 適用於Microsoft Hyper-V和SQL Server over SMB 解決方案的支援功能

您可以使用持續可用的SMB 3.0及更新版本檔案共用、將Hyper-V虛擬機器檔案或SQL Server系統資料庫及使用者資料庫儲存在位於SVM的磁碟區上、同時為計畫性和非計畫性事件提供不中斷營運（NDOS）。

Microsoft Hyper-V over SMB

若要建立Hyper-V over SMB解決方案、您必須先設定ONTAP 支援功能以提供Microsoft Hyper-V伺服器的儲存服務。此外、您也必須設定Microsoft叢集（如果使用叢集式組態）、Hyper-V伺服器、持續可用的SMB 3.0連線至CIFS伺服器所託管的共用、以及選擇性的備份服務、以保護儲存在SVM磁碟區上的虛擬機器檔案。



Hyper-V伺服器必須在Windows 2012 Server或更新版本上設定。支援獨立式和叢集式Hyper-V伺服器組態。

- 如需建立Microsoft叢集和Hyper-V伺服器的相關資訊、請參閱Microsoft網站。
- 適用於Hyper-V的解決方案是以主機為基礎的應用程式、可提供快速的Snapshot複製型備份服務、專為透過SMB組態與Hyper-V整合而設計。SnapManager

如需SnapManager 在SMB組態上搭配Hyper-V使用的相關資訊、請參閱《SnapManager 適用於Hyper-V的_E__安裝與管理指南》。

Microsoft SQL Server over SMB

若要透過SMB建立SQL Server解決方案、您必須先設定ONTAP 支援功能、為Microsoft SQL Server應用程式提供儲存服務。此外、您也必須設定Microsoft叢集（如果使用叢集式組態）。接著您可以在Windows伺服器上安裝及設定SQL Server、並建立持續可用的SMB 3.0連線、以連線至CIFS伺服器所託管的共用區。您可以選擇性地設定備份服務、以保護儲存在SVM磁碟區上的資料庫檔案。



SQL Server必須安裝並設定於Windows 2012 Server或更新版本。支援獨立式和叢集式組態。

- 如需建立Microsoft叢集及安裝及設定SQL Server的相關資訊、請參閱Microsoft網站。
- 適用於Microsoft SQL Server的解決方案外掛程式是以主機為基礎的應用程式、可協助快速、以Snapshot複製為基礎的備份服務、其設計可透過SMB組態與SQL Server整合。SnapCenter

如需使用SnapCenter 適用於Microsoft SQL Server的解決方案的資訊、請參閱 "[適用於Microsoft SQL Server的支援外掛程式SnapCenter](#)" 文件。

不中斷營運：透過SMB執行Hyper-V和SQL Server

Hyper-V和SQL Server在SMB上的不中斷營運意味著什麼

Hyper-V與SQL Server在SMB上的不中斷營運、是指結合各種功能、讓應用程式伺服器與所包含的虛擬機器或資料庫維持線上狀態、並在許多管理工作期間提供持續可用度。這包括儲存基礎架構的計畫性和非計畫性停機。

透過SMB支援的應用程式伺服器不中斷營運包括：

- 計畫性接管與恢復
- 非計畫性接管
- 升級
- 計畫性集合體重新配置（ARL）
- LIF移轉與容錯移轉
- 計畫性Volume搬移

可在SMB上執行不中斷營運的傳輸協定

隨著SMB 3.0的推出、Microsoft已發行新的傳輸協定、提供必要的功能、以支援Hyper-V和SQL Server在SMB上的不中斷營運。

透過SMB為應用程式伺服器提供不中斷營運時、可使用下列通訊協定：ONTAP

- SMB 3.0
- 見證人

關於Hyper-V和SQL Server在SMB上不中斷營運的重要概念

在設定Hyper-V或SQL Server over SMB解決方案之前、您應該先瞭解一些關於不中斷營運（NDOS）的概念。

- 持續可用的共享區

擁有持續可用共用內容集的SMB 3.0共用區。透過持續可用的共用區連線的用戶端、可在接管、恢復及集合重新配置等中斷事件中繼續運作。

- 節點

屬於叢集成員的單一控制器。為了區分SFO配對中的兩個節點、一個節點有時稱為「*local node*」、另一個節點有時稱為「*Partner node*」或「*remRemote node*」。儲存設備的主要擁有者是本機節點。當主要擁有者故障時、可控制儲存設備的次要擁有者是合作夥伴節點。每個節點都是其儲存設備的主要擁有者、也是其合作夥伴儲存設備的次要擁有者。

- 不中斷的集合體重新配置

能夠在叢集的SFO配對內的合作夥伴節點之間移動集合體、而不會中斷用戶端應用程式。

- 不中斷的容錯移轉

請參閱_Takeove_。

- 不中斷的LIF移轉

能夠執行LIF移轉、而不會中斷透過該LIF連線至叢集的用戶端應用程式。對於SMB連線、這僅適用於使用SMB 2.0或更新版本連線的用戶端。

- 不中斷營運

能夠執行ONTAP 重大的非資料管理與升級作業、並在不中斷用戶端應用程式的情況下、承受節點故障。此術語指的是不中斷接管、不中斷升級和不中斷營運的整體移轉功能集合。

- 不中斷升級

能夠在不中斷應用程式的情況下升級節點硬體或軟體。

- 不中斷磁碟區移動

能夠在整個叢集內自由移動磁碟區、而不會中斷使用該磁碟區的任何應用程式。對於SMB連線、所有SMB版本都支援不中斷營運的Volume移動。

- 持續處理

SMB 3.0的屬性、可在中斷連線時、讓持續可用的連線以透明方式重新連線至CIFS伺服器。與耐久的處理程序類似、CIFS伺服器會在與連線用戶端的通訊中斷後、持續維護處理程序一段時間。然而、持續性的處理能力比持久性的處理能力更強。除了讓用戶端有機會在重新連線後60秒內回收處理、CIFS伺服器也會在60秒內拒絕任何其他用戶端存取要求存取檔案的權限。

關於持續處理的資訊會鏡射到SFO合作夥伴的持續儲存設備上、這可讓持續處理中斷連線的用戶端在發生SFO合作夥伴取得節點儲存設備所有權的事件後、回收持久處理。除了在LIF移動時提供不中斷營運（可

持久處理支援) 之外、持續控點還可提供不中斷營運的接管、恢復及集合重新定位功能。

- * SFO贈品*

從接管事件中恢復時、將集合體傳回其主位置。

- * SFO配對*

一對節點、其控制器設定為在兩個節點之一停止運作時、為彼此提供資料。視系統機型而定、兩個控制器都可以放在單一機箱中、或是控制器可以放在不同的機箱中。在雙節點叢集中稱為HA配對。

- 接管

當儲存設備的主要擁有者故障時、合作夥伴控制儲存設備的程序。在SFO環境中、容錯移轉和接管是同義詞。

SMB 3.0功能如何支援透過SMB共用進行不中斷營運

SMB 3.0提供關鍵功能、可支援透過SMB共用區執行Hyper-V和SQL Server不中斷營運。其中包括 *continuously-available* 共用屬性和一種稱為 *Persistent Handle* 的檔案處理方式、可讓 SMB 用戶端回收檔案開啟狀態、並以透明方式重新建立 SMB 連線。

可將持續處理權授予具有SMB 3.0功能的用戶端、這些用戶端會使用持續可用的共用內容集連線至共用區。如果SMB工作階段中斷連線、CIFS伺服器會保留持續處理狀態的相關資訊。CIFS伺服器會在允許用戶端重新連線的60秒期間、封鎖其他用戶端要求、讓具有持續控制代碼的用戶端在網路中斷連線後、得以回收處理代碼。具有持續控點的用戶端可以使用儲存虛擬機器 (SVM) 上的其中一個資料LIF來重新連線、方法是透過相同的LIF或不同的LIF來重新連線。

集合重新定位、接管和恢復都會發生在SFO配對之間。為了無縫管理中斷連線和重新連線工作階段與具有持續處理程序的檔案、合作夥伴節點會保留一份所有持續處理鎖定資訊的複本。無論活動是計畫性或非計畫性的、SFO合作夥伴都能不中斷地管理持續處理重新連線。有了這項新功能、連接到CIFS伺服器的SMB 3.0連線、就能以透明且不中斷營運的方式、容錯移轉到另一個指派給SVM的資料LIF、而這是過去發生的破壞性事件。

雖然使用持續性控點可讓CIFS伺服器以透明方式容錯移轉SMB 3.0連線、但如果故障導致Hyper-V應用程式容錯移轉至Windows Server叢集中的另一個節點、用戶端就無法回收這些中斷連線控點的檔案控點。在此案例中、如果在不同節點上重新啟動Hyper-V應用程式、處於中斷連線狀態的檔案處理程序可能會封鎖其存取。「容錯移轉叢集」是SMB 3.0的一部分、可提供機制來使過時且相互衝突的處理程序失效。使用此機制、Hyper-V叢集可在Hyper-V叢集節點故障時快速恢復。

見證傳輸協定如何加強透明的容錯移轉

見證傳輸協定為SMB 3.0持續可用的共用 (CA共用) 提供增強的用戶端容錯移轉功能。見證可縮短容錯移轉的速度、因為它會跳過LIF容錯移轉恢復期間。當節點無法使用時、它會通知應用程式伺服器、而不需要等待SMB 3.0連線逾時。

容錯移轉是無縫的、因為用戶端上執行的應用程式並未察覺發生容錯移轉。如果見證無法使用、容錯移轉作業仍會成功執行、但沒有見證的容錯移轉效率較低。

滿足下列需求時、可進行見證增強容錯移轉：

- 它只能與啟用SMB 3.0的SMB 3.0型CIFS伺服器搭配使用。

- 共用區必須使用SMB 3.0、並設定持續可用度共用內容。
- 應用程式伺服器所連接之節點的SFO合作夥伴、必須至少有一個作業資料LIF指派給應用程式伺服器的儲存虛擬機器（SVM）。



見證協議在SFO配對之間運作。由於LIF可以移轉至叢集內的任何節點、因此任何節點都可能需要成為其SFO合作夥伴的見證人。如果應用程式伺服器的SVM託管資料在合作夥伴節點上沒有作用中的資料LIF、見證傳輸協定就無法在指定節點上提供SMB連線的快速容錯移轉。因此、叢集中的每個節點必須至少有一個資料LIF、才能讓裝載其中一個組態的每個SVM使用。

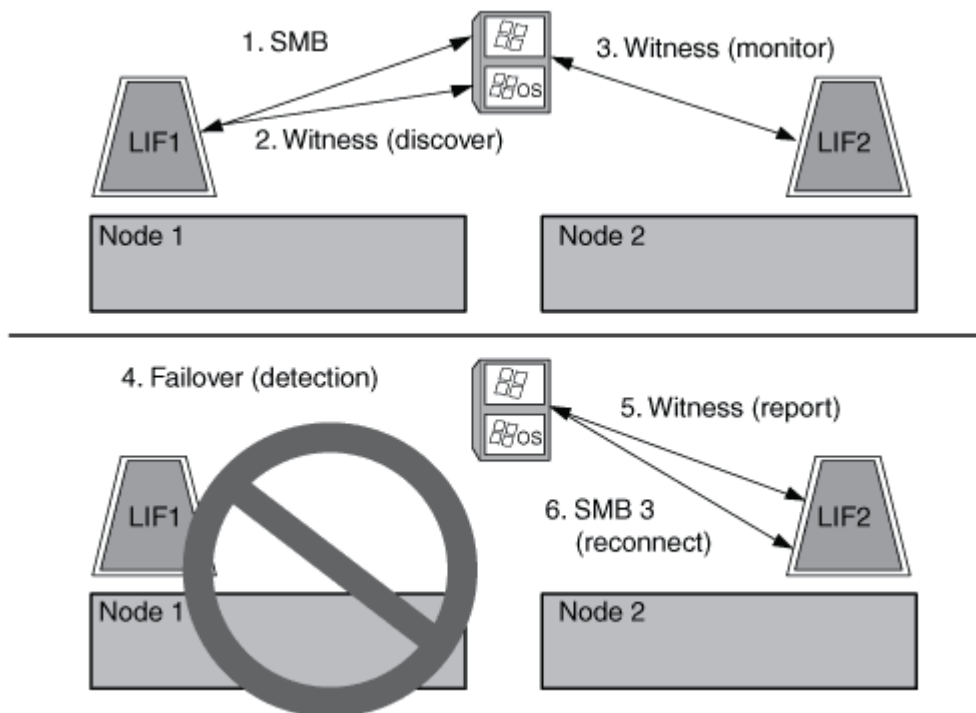
- 應用程式伺服器必須使用儲存在DNS中的CIFS伺服器名稱來連線至CIFS伺服器、而非使用個別的LIF IP位址。

見證協定的運作方式

利用節點的SFO合作夥伴作為見證人、實作見證協議。ONTAP如果發生故障、合作夥伴會快速偵測故障、並通知SMB用戶端。

見證傳輸協定使用下列程序提供增強的容錯移轉：

1. 當應用程式伺服器建立與Node1的持續可用SMB連線時、CIFS伺服器會通知應用程式伺服器有覆核人可用。
2. 應用程式伺服器從Node1要求見證伺服器的IP位址、並接收指派給儲存虛擬機器（SVM）的Node2（SFO合作夥伴）資料LIF IP位址清單。
3. 應用程式伺服器會選擇其中一個IP位址、建立節點2的見證連線、並在節點1上持續可用的連線必須移動時登錄以通知。
4. 如果節點1上發生容錯移轉事件、見證可簡化容錯移轉事件、但不涉及還原。
5. 見證會偵測容錯移轉事件、並透過見證連線通知應用程式伺服器SMB連線必須移至節點2。
6. 應用程式伺服器會將SMB工作階段移至節點2、並在不中斷用戶端存取的情況下恢復連線。



使用遠端VSS進行共用型備份

利用遠端VSS總覽進行共享型備份

您可以使用遠端VSS、對儲存在CIFS伺服器上的Hyper-V虛擬機器檔案執行共用型備份。

Microsoft遠端VSS（Volume陰影複製服務）是現有Microsoft VSS基礎架構的延伸。有了遠端VSS、Microsoft已擴充VSS基礎架構、以支援SMB共用的陰影複製。此外、Hyper-V 等伺服器應用程式也能將 VHD 檔案儲存在 SMB 檔案共用上。有了這些副檔名、就能為儲存資料和組態檔案在共享區上的虛擬機器取得應用程式一致的陰影複本。

遠端VSS概念

您應該瞭解一些必要概念、瞭解如何透過SMB組態搭配Hyper-V來使用遠端VSS（Volume陰影複製服務）。

- * VSS（Volume陰影複製服務） *

一種Microsoft技術、用於在特定時間點、在特定磁碟區上製作資料的備份複本或快照。VSS可協調資料伺服器、備份應用程式和儲存管理軟體、以支援建立及管理一致的備份。

- 遠端VSS（遠端Volume陰影複製服務）

一種Microsoft技術、用於在透過SMB 3.0共用存取資料的特定時間點、取得資料一致狀態的共用型資料備份複本。也稱為_Volume陰影複製服務_。

- 陰影複製

共享區中包含的一組重複資料、可在明確定義的即時時間內完成。陰影複製可用來建立一致的資料時間點備份、讓系統或應用程式能夠繼續更新原始磁碟區上的資料。

- 陰影複製集

一或多個陰影複本的集合、每個陰影複本對應一個共用。陰影複製集中的陰影複製代表必須在相同作業中備份的所有共用。啟用VSS的應用程式上的VSS用戶端會識別要包含在集合中的陰影複本。

- 陰影複製集自動恢復

備份程序的一部分、用於啟用VSS的遠端備份應用程式、其中包含陰影複製的複本目錄會使時間點保持一致。在備份開始時、應用程式上的VSS用戶端會觸發應用程式對排定要備份的資料（Hyper-V的虛擬機器檔案）執行軟體檢查點。然後VSS用戶端可讓應用程式繼續執行。建立陰影複製集之後、遠端VSS會將陰影複製集設為可寫入、並將可寫入的複本公開給應用程式。應用程式會使用先前取得的軟體檢查點執行自動還原、以準備陰影複製集以供備份。自動還原功能可復原自建立檢查點以來對檔案和目錄所做的變更、使陰影複製達到一致的狀態。自動還原是啟用VSS備份的選用步驟。

- 陰影複製ID

唯一識別陰影複製的GUID。

- 陰影複製集ID

唯一識別陰影複製識別碼集合到同一部伺服器的GUID。

- *適用於Hyper-V * SnapManager

此軟體可自動化及簡化Microsoft Windows Server 2012 Hyper-V的備份與還原作業適用於Hyper-V的支援使用遠端VSS搭配自動還原功能、可透過SMB共用區來備份Hyper-V檔案。SnapManager

相關資訊

[關於Hyper-V和SQL Server在SMB上不中斷營運的重要概念](#)

[使用遠端VSS進行共用型備份](#)

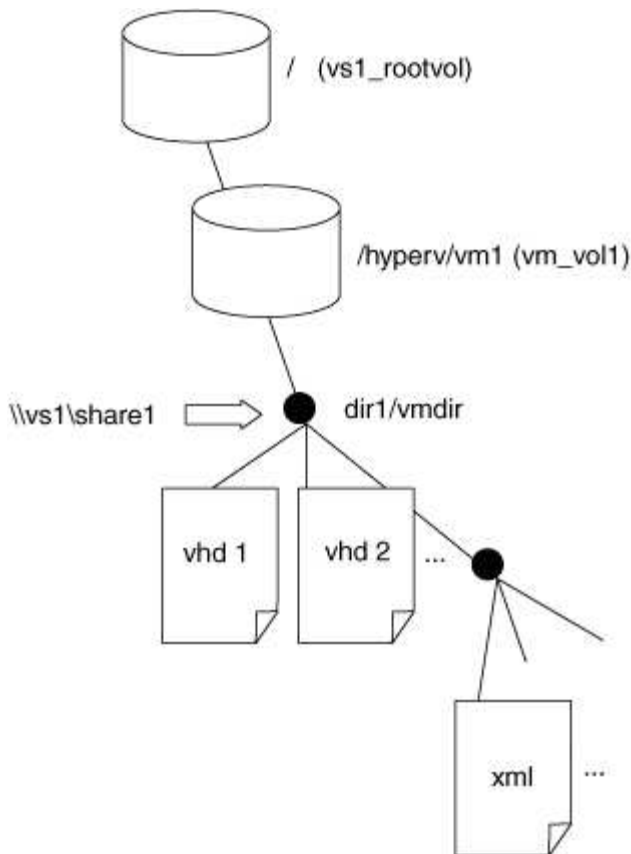
遠端VSS使用的目錄結構範例

遠端VSS會在建立陰影複製時、遍歷儲存Hyper-V虛擬機器檔案的目錄結構。請務必瞭解適當的目錄結構、以便成功建立虛擬機器檔案的備份。

成功建立陰影複製所支援的目錄結構符合下列需求：

- 只有目錄和一般檔案存在於用來儲存虛擬機器檔案的目錄結構中。
目錄結構不包含交會、連結或非一般檔案。
- 虛擬機器的所有檔案都位於單一共用區內。
- 用於儲存虛擬機器檔案的目錄結構不會超過陰影複製目錄的設定深度。
- 共用區的根目錄僅包含虛擬機器檔案或目錄。

在下圖中、建立名為 VM_vol1 的磁碟區時、會在其上建立連接點 /hyperv/vml 儲存虛擬機器（SVM）VS1 上。包含虛擬機器檔案的子目錄會建立在交會點之下。Hyper-V 伺服器的虛擬機器檔案是透過具有路徑的共享 1 來存取 /hyperv/vml/dirl/vmdir。陰影複製服務會建立所有虛擬機器檔案的陰影複製、這些檔案都包含在共享區1（直到陰影複製目錄設定的深度）下的目錄結構中。



適用於Hyper-V的解決方案SnapManager 如何透過SMB管理Hyper-V的遠端VSS型備份

您可以使用SnapManager 支援Hyper-V的支援功能來管理遠端VSS型備份服務。使用支援Hyper-V的託管備份服務來建立空間效率極高的備份集、有許多好處SnapManager 。

針對Hyper-V託管備份進行的最佳化包括：SnapManager

- 支援VMware的整合功能可在探索SMB共用位置時提供效能最佳化。SnapDrive ONTAP
提供含有共享區所在Volume名稱的功能。ONTAP SnapDrive
- 針對Hyper-V、指定陰影複製服務需要複製的SMB共用中虛擬機器檔案清單。SnapManager
藉由提供目標式虛擬機器檔案清單、陰影複製服務不需要建立共用中所有檔案的陰影複製。
- 儲存虛擬機器（SVM）會保留Snapshot複本以SnapManager 供Hyper-V使用、以供還原。
沒有備份階段。備份是節省空間的Snapshot複本。

適用於Hyper-V的支援透過SMB為HyperV提供備份與還原功能、程序如下：SnapManager

1. 準備陰影複製作業

適用於Hyper-V應用程式的VSS用戶端會設定陰影複製集。SnapManagerVSS用戶端會收集陰影複製集中要包含哪些共享的資訊、並將此資訊提供ONTAP 給效益管理系統。一組可能包含一或多個陰影複製、而一個陰影複製對應一個共用區。

2. 建立陰影複製集（如果使用自動還原）

針對陰影複製集中的每個共用區ONTAP、它會建立陰影複製、並使陰影複製可寫入。

3. 揭露陰影複製集

在建立陰影複製之後ONTAP、它們會暴露SnapManager 於適用於Hyper-V的功能、讓應用程式的VSS寫入器能夠執行自動還原。

4. 自動恢復陰影複製集

在建立陰影複製集期間、備份集內的檔案會有一段時間發生作用中變更。應用程式的VSS寫入器必須更新陰影複本、以確保在備份前處於完全一致的狀態。



自動還原的執行方式取決於應用程式。遠端VSS不涉及此階段。

5. 完成並清除陰影複製集

VSS用戶端會在ONTAP 完成自動還原之後通知功能不全。陰影複製集會設為唯讀、然後準備好備份。使用SnapManager 支援Hyper-V的功能進行備份時、Snapshot複本中的檔案會成為備份、因此在備份階段、會針對備份集中包含共用的每個磁碟區建立Snapshot複本。備份完成後、陰影複製集會從CIFS伺服器移除。

ODX複製卸載如何透過SMB共用搭配Hyper-V和SQL Server使用

卸載資料傳輸（ODX）也稱為_copy offload_、可在相容儲存裝置內或之間直接傳輸資料、而無需透過主機電腦傳輸資料。透過SMB安裝、在應用程式伺服器上執行複製作業時、利用VMware版複製卸載功能可為您帶來效能優勢。ONTAP

在非ODX檔案傳輸中、資料會從來源CIFS伺服器讀取、並透過網路傳輸至用戶端電腦。用戶端電腦會透過網路將資料傳輸回目的地CIFS伺服器。總而言之、用戶端電腦會從來源讀取資料、然後寫入目的地。使用ODX檔案傳輸時、資料會直接從來源複製到目的地。

由於ODX卸載複本是直接在來源與目的地儲存設備之間執行、因此效能優勢顯著。實現的效能效益包括加快來源與目的地之間的複製時間、降低用戶端上的資源使用率（CPU、記憶體）、以及降低網路I/O頻寬使用率。

ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

下列使用案例支援使用ODX複本和移動：

- Volume內

來源與目的地檔案或LUN位於同一個磁碟區內。

- 磁碟區間、相同節點、相同儲存虛擬機器（SVM）

來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料歸同一個SVM所有。

- 磁碟區間、不同節點、相同SVM

來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料歸同一個SVM所有。

- SVM之間、相同節點

來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料由不同的SVM擁有。

- SVM之間、不同節點

來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料由不同的SVM擁有。

Hyper-V解決方案的ODX複製卸載特定使用案例包括：

- 您可以使用ODX複本卸載傳遞搭配Hyper-V、在虛擬硬碟（VHD）檔案內或之間複製資料、或在同一個叢集內的對應SMB共用區和連接的iSCSI LUN之間複製資料。

如此一來、從客體作業系統的複本就能傳遞到基礎儲存設備。

- 建立固定大小的VHD時、ODX會使用已知的零權杖、以零初始化磁碟。
- 如果來源與目的地儲存設備位於同一個叢集、則ODX複本卸載可用於虛擬機器儲存移轉。



若要利用ODX複本卸載傳遞與Hyper-V的使用案例、來賓作業系統必須支援ODX、而來賓作業系統的磁碟必須是支援ODX的儲存設備（SMB或SAN）所支援的SCSI磁碟。客體作業系統上的IDE磁碟不支援ODX傳遞。

SQL Server解決方案的ODX複製卸載特定使用案例包括：

- 您可以使用ODX複製卸載、在對應的SMB共用區之間、或是在同一個叢集內的SMB共用區與連線的iSCSI LUN之間匯出及匯入SQL Server資料庫。
- 如果來源與目的地儲存設備位於同一個叢集、則ODX複製卸載可用於資料庫匯出與匯入。

組態需求與考量

不需提供授權與授權ONTAP

在建立SQL Server或Hyper-V over SMB解決方案以在SVM上執行不中斷營運時、您必須瞭解ONTAP 特定的功能與授權需求。

版本需求ONTAP

- Hyper-V over SMB

支援在SMB共用區上執行不中斷營運、以在Windows 2012或更新版本上執行Hyper-V。ONTAP

- SQL Server over SMB

支援在SMB共用區上執行不中斷營運、適用於在Windows 2012或更新版本上執行的SQL Server 2012或更新版本。ONTAP

如需ONTAP 有關支援版本的支援、如需在SMB共用區上執行不中斷營運的更新資訊、請參閱互通性對照表 (Interoperability Matrix) 。

"NetApp 互通性對照表工具"

授權要求

需要下列授權：

- CIFS
- FlexClone (僅適用於SMB上的Hyper-V)

如果使用遠端VSS進行備份、則需要此授權。陰影複製服務使用FlexClone來建立檔案的時間點複本、以便在建立備份時使用。

如果您使用不使用遠端VSS的備份方法、則FlexClone授權為選用項目。

FlexClone 授權包含在中 "ONTAP One"。如果您沒有 ONTAP One、您應該 "確認已安裝必要的授權"，必要時 "安裝它們"。

網路與資料LIF需求

在建立SQL Server或Hyper-V over SMB組態以進行不中斷營運時、您必須瞭解特定的網路和資料LIF需求) 。

網路傳輸協定需求

- 支援IPV4和IPV6網路。
- 需要SMB 3.0或更新版本。

SMB 3.0提供所需的功能、可建立持續可用的SMB連線、以提供不中斷營運的必要功能。

- DNS伺服器必須包含將CIFS伺服器名稱對應至指派給儲存虛擬機器 (SVM) 上資料LIF的IP位址的項目。

在存取虛擬機器或資料庫檔案時、Hyper-V或SQL Server應用程式伺服器通常會透過多個資料生命體建立多個連線。為了正常運作、應用程式伺服器必須使用CIFS伺服器名稱來建立這類多個SMB連線、而非建立多個唯一IP位址的連線。

見證也需要使用CIFS伺服器的DNS名稱、而非個別的LIF IP位址。

從支援中小企業多通道技術的中小企業組態開始ONTAP、您就能改善Hyper-V和SQL伺服器的處理量和容錯能力。若要這麼做、您必須在叢集和用戶端上部署多個1G、10G或更大的NIC。

資料LIF需求

- 透過SMB解決方案託管應用程式伺服器的SVM、必須在叢集中的每個節點上至少有一個作業資料LIF。

SVM資料LIF可容錯移轉至叢集內的其他資料連接埠、包括目前未裝載應用程式伺服器所存取資料的節點。此外、由於見證節點永遠是應用程式伺服器所連接節點的SFO合作夥伴、因此叢集中的每個節點都是潛在的見證節點。

- 資料生命期不得設定為自動還原。

在接管或恢復事件之後、您應該手動將資料生命期還原至其主連接埠。

- 所有資料LIF IP位址都必須在DNS中有一個項目、而且所有項目都必須解析為CIFS伺服器名稱。

應用程式伺服器必須使用CIFS伺服器名稱連線至SMB共用區。您不得設定應用程式伺服器使用LIF IP位址進行連線。

- 如果CIFS伺服器名稱與SVM名稱不同、則DNS項目必須解析為CIFS伺服器名稱。

SMB伺服器與磁碟區需求、適用於SMB上的Hyper-V

在建立Hyper-V over SMB組態以實現不中斷營運時、您必須注意特定的SMB伺服器和磁碟區需求。

SMB 伺服器需求

- 必須啟用SMB 3.0。

此功能預設為啟用。

- 預設UNIX使用者CIFS伺服器選項必須設定有效的UNIX使用者帳戶。

應用程式伺服器會在建立SMB連線時使用機器帳戶。由於所有SMB存取都需要Windows使用者成功對應至UNIX使用者帳戶或預設UNIX使用者帳戶、ONTAP 所以無法將應用程式伺服器的機器帳戶對應至預設的UNIX使用者帳戶。

- 必須停用自動節點參照（此功能預設為停用）。

如果您想要使用自動節點參照來存取Hyper-V機器檔案以外的資料、則必須為該資料建立個別的SVM。

- 必須在SMB伺服器所屬的網域中同時允許Kerberos和NTLM驗證。

不針對遠端VSS通告Kerberos服務、因此應將網域設定為允許使用NTLM。ONTAP

- 必須啟用陰影複製功能。

此功能預設為啟用。

- 陰影複製服務在建立陰影複製時所使用的Windows網域帳戶、必須是SMB伺服器本機BUILTIN\Administrator或BUILTIN\Backup Operators群組的成員。

Volume需求

- 用於儲存虛擬機器檔案的磁碟區必須建立為NTFS安全型磁碟區。

若要使用持續可用的SMB連線、為應用程式伺服器提供NDOS、包含共用區的磁碟區必須是NTFS磁碟區。此外、它必須永遠是NTFS磁碟區。您無法將混合式安全型磁碟區或UNIX安全型磁碟區變更為NTFS安全型磁碟區、並透過SMB共用區直接用於NDOS。如果您將混合式安全型磁碟區變更為NTFS安全型磁碟區、並打算在SMB共用區的NDOS中使用、則必須手動將ACL放在磁碟區頂端、並將該ACL傳播至所有內含的檔案和資料夾。否則、如果來源或目的地磁碟區最初建立為混合或UNIX安全型磁碟區、之後改為NTFS安全型

態、則將檔案移至另一個磁碟區的虛擬機器移轉或資料庫檔案匯出及匯入可能會失敗。

- 若要成功執行陰影複製作業、您必須在磁碟區上有足夠的可用空間。

可用空間必須至少與陰影複製備份集中所含共用區內的所有檔案、目錄及子目錄所使用的總空間相同。此需求僅適用於具有自動還原功能的陰影複製。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

SMB伺服器需求和適用於SMB以上的SQL Server

在透過SMB組態建立SQL Server以進行不中斷營運時、您必須瞭解特定的SMB伺服器和磁碟區需求。

SMB 伺服器需求

- 必須啟用SMB 3.0。

此功能預設為啟用。

- 預設UNIX使用者CIFS伺服器選項必須設定有效的UNIX使用者帳戶。

應用程式伺服器會在建立SMB連線時使用機器帳戶。由於所有SMB存取都需要Windows使用者成功對應至UNIX使用者帳戶或預設UNIX使用者帳戶、ONTAP 所以無法將應用程式伺服器的機器帳戶對應至預設的UNIX使用者帳戶。

此外、SQL Server使用網域使用者做為SQL Server服務帳戶。服務帳戶也必須對應至預設的UNIX使用者。

- 必須停用自動節點參照（此功能預設為停用）。

如果您想要使用自動節點參照來存取SQL Server資料庫檔案以外的資料、則必須為該資料建立個別的SVM。

- 用於將SQL Server安裝在ONTAP 更新上的Windows使用者帳戶必須指派SeSecurityPrivilege權限。

此權限指派給SMB伺服器本機BUILTIN\Administrators群組。

Volume需求

- 用於儲存虛擬機器檔案的磁碟區必須建立為NTFS安全型磁碟區。

若要使用持續可用的SMB連線、為應用程式伺服器提供NDOS、包含共用區的磁碟區必須是NTFS磁碟區。此外、它必須永遠是NTFS磁碟區。您無法將混合式安全型磁碟區或UNIX安全型磁碟區變更為NTFS安全型磁碟區、並透過SMB共用區直接用於NDOS。如果您將混合式安全型磁碟區變更為NTFS安全型磁碟區、並打算在SMB共用區的NDOS中使用、則必須手動將ACL放在磁碟區頂端、並將該ACL傳播至所有內含的檔案和資料夾。否則、如果來源或目的地磁碟區最初建立為混合或UNIX安全型磁碟區、之後改為NTFS安全型態、則將檔案移至另一個磁碟區的虛擬機器移轉或資料庫檔案匯出及匯入可能會失敗。

- 雖然包含資料庫檔案的磁碟區可以包含連接點、但在建立資料庫目錄結構時、SQL Server不會交叉連接點。

- 為了讓Microsoft SQL Server備份作業順利完成、您必須在磁碟區上有足夠的可用空間。SnapCenter

SQL Server資料庫檔案所在的磁碟區必須夠大、足以容納資料庫目錄結構、以及位於共用區內的所有內含檔案。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

持續可用的SMB Hyper-V共用需求與考量

在設定支援不中斷營運的Hyper-V over SMB組態的持續可用共用時、您必須瞭解特定的需求與考量。

共用需求

- 應用程式伺服器使用的共用必須設定為持續可用的內容集。

連線至持續可用共用區的應用程式伺服器會接收持續的處理常式、以便在發生中斷事件（例如接管、恢復和集合重新配置）之後、不中斷地重新連線至SMB共用區、並回收檔案鎖定。

- 如果您想要使用啟用遠端VSS的備份服務、就無法將Hyper-V檔案放入包含連接的共用中。

在自動還原案例中、如果在瀏覽共用區時遇到交會、陰影複製建立就會失敗。在非自動還原案例中、陰影複製建立並不會失敗、但交會不會指向任何內容。

- 如果您想要使用啟用遠端VSS的備份服務進行自動還原、就無法將Hyper-V檔案放入包含下列項目的共用區：

- symlinks、hardlink或widelinks
- 非一般檔案

如果要陰影複製的共用區中有任何連結或非一般檔案、陰影複製建立就會失敗。此需求僅適用於具有自動還原功能的陰影複製。

- 若要成功執行陰影複製作業、您必須在磁碟區上有足夠的可用空間（僅適用於SMB上的Hyper-V）。

可用空間必須至少與陰影複製備份集中所含共用區內的所有檔案、目錄及子目錄所使用的總空間相同。此需求僅適用於具有自動還原功能的陰影複製。

- 應用程式伺服器所使用的持續可用共用區不得設定下列共用內容：
 - 主目錄
 - 屬性快取
 - BranchCache

考量

- 持續可用的共用支援配額。
- Hyper-V over SMB組態不支援下列功能：

- 稽核
- FPolicy
- 不會在與的 SMB 共用上執行病毒掃描 continuously-availability 參數設為 Yes。

持續可用的SQL Server與SMB之間的共用需求和考量

在設定支援不中斷營運的SMB組態上的SQL Server持續可用共用時、您必須瞭解特定的需求和考量。

共用需求

- 用於儲存虛擬機器檔案的磁碟區必須建立為NTFS安全型磁碟區。

若要使用持續可用的SMB連線、為應用程式伺服器提供不中斷營運的作業、包含共用區的磁碟區必須是NTFS磁碟區。此外、它必須永遠是NTFS磁碟區。您無法將混合式安全型磁碟區或UNIX安全型磁碟區變更為NTFS安全型磁碟區、並將其直接用於透過SMB共用進行不中斷營運的作業。如果您將混合式安全型磁碟區變更為NTFS安全型磁碟區、並打算在SMB共用區上執行不中斷營運作業、則必須手動將ACL放在磁碟區頂端、並將該ACL傳播至所有內含的檔案和資料夾。否則、如果來源或目的地磁碟區最初建立為混合或UNIX安全型磁碟區、之後改為NTFS安全型態、則將檔案移至另一個磁碟區的虛擬機器移轉或資料庫檔案匯出及匯入可能會失敗。

- 應用程式伺服器使用的共用必須設定為持續可用的內容集。

連線至持續可用共用區的應用程式伺服器會接收持續的處理常式、以便在發生中斷事件（例如接管、恢復和集合重新配置）之後、不中斷地重新連線至SMB共用區、並回收檔案鎖定。

- 雖然包含資料庫檔案的磁碟區可以包含連接點、但在建立資料庫目錄結構時、SQL Server不會交叉連接點。
- 為了讓Microsoft SQL Server作業順利完成、您必須在磁碟區上有足夠的可用空間。SnapCenter

SQL Server資料庫檔案所在的磁碟區必須夠大、足以容納資料庫目錄結構、以及位於共用區內的所有內含檔案。

- 應用程式伺服器所使用的持續可用共用區不得設定下列共用內容：
 - 主目錄
 - 屬性快取
 - BranchCache

分享考量

- 持續可用的共用支援配額。
- 下列功能不支援SQL Server over SMB組態：
 - 稽核
 - FPolicy
- 不會在與的 SMB 共用上執行病毒掃描 continuously-availability 共用屬性集。

基於SMB組態的Hyper-V遠端VSS考量

在使用支援遠端VSS的備份解決方案進行Hyper-V over SMB組態時、您必須注意某些考量事項。

一般遠端VSS考量

- 每個Microsoft應用程式伺服器最多可設定64個共用區。

如果陰影複製集中有超過64個共用區、陰影複製作業就會失敗。這是Microsoft的要求。

- 每部CIFS伺服器只允許一個作用中的陰影複製集。

如果在同一部CIFS伺服器上持續執行陰影複製作業、陰影複製作業將會失敗。這是Microsoft的要求。

- 在遠端VSS建立陰影複製的目錄結構中、不允許任何交會。
 - 在自動還原案例中、如果在瀏覽共用區時遇到交會、陰影複製建立將會失敗。
 - 在非自動還原案例中、陰影複製建立並不會失敗、但交會不會指向任何內容。

遠端VSS考量、僅適用於具有自動還原功能的陰影複製

某些限制僅適用於具有自動還原功能的陰影複製。

- 建立陰影複製時、最多可允許五個子目錄的目錄深度。

這是陰影複製服務建立陰影複製備份集的目錄深度。如果包含虛擬機器檔案的目錄巢狀深於五個層級、陰影複製建立就會失敗。這是為了限制複製共用時的目錄周遊。您可以使用CIFS伺服器選項來變更最大目錄深度。

- 磁碟區上的可用空間量必須足夠。

可用空間必須至少與陰影複製備份集中所含共用區內的所有檔案、目錄及子目錄所使用的總空間相同。

- 在遠端VSS建立陰影複製的目錄結構中、不允許任何連結或非一般檔案。

如果共用區中有任何連結或非一般檔案到陰影複製、陰影複製建立就會失敗。複製程序不支援。

- 目錄不允許使用NFSv4 ACL。

雖然建立陰影複製會保留檔案上的NFSv4 ACL、但目錄上的NFSv4 ACL會遺失。

- 建立陰影複製集的時間上限為60秒。

Microsoft規格允許建立陰影複製集的時間上限為60秒。如果VSS用戶端在此時間內無法建立陰影複製集、陰影複製作業將會失敗、因此會限制陰影複製集中的檔案數量。備份集中可包含的檔案或虛擬機器實際數量各不相同、這個數目取決於許多因素、而且必須針對每個客戶環境來決定。

SQL Server和Hyper-V在SMB上的ODX複製卸載需求

如果您想要移轉虛擬機器檔案、或直接從來源匯出及匯入資料庫檔案至目的地儲存位置、

而不想透過應用程式伺服器傳送資料、則必須啟用ODX複本卸載。您必須瞭解使用ODX複製卸載搭配SQL Server和Hyper-V over SMB解決方案的特定需求。

使用ODX複本卸載可提供顯著的效能效益。此CIFS伺服器選項預設為啟用。

- 必須啟用SMB 3.0才能使用ODX複本卸載。
- 來源磁碟區至少必須為1.25 GB。
- 必須在使用複本卸載的磁碟區上啟用重複資料刪除功能。
- 如果您使用壓縮磁碟區、壓縮類型必須是可調適的、而且只支援8K大小的壓縮群組。

不支援次要壓縮類型

- 若要使用ODX複本卸載來移轉磁碟內和磁碟之間的Hyper-V來賓、必須將Hyper-V伺服器設定為使用SCSI磁碟。

預設是設定IDE磁碟、但如果使用IDE磁碟建立磁碟、則移轉來賓時ODX複製卸載無法運作。

SQL Server與Hyper-V over SMB組態的建議

為了確保SQL Server和Hyper-V over SMB組態健全且可運作、您必須熟悉建議的最佳實務做法、才能設定解決方案。

一般建議

- 將應用程式伺服器檔案與一般使用者資料分開。

如果可能、請將整個儲存虛擬機器（SVM）及其儲存設備用於應用程式伺服器的資料。

- 為獲得最佳效能、請勿在用於儲存應用程式伺服器資料的SVM上啟用SMB簽署。
- 為獲得最佳效能及改善容錯能力、SMB多通道可在ONTAP 單一SMB工作階段中、在VMware與用戶端之間提供多重連線。
- 請勿在Hyper-V或SQL Server中使用的任何共享區上、透過SMB組態建立持續可用的共享區。
- 停用用於持續可用性之共用的變更通知。
- 請勿在執行Volume搬移的同時執行Aggregate重新配置（ARL）、因為ARL有會暫停某些作業的階段。
- 對於Hyper-V over SMB解決方案、請在建立叢集式虛擬機器時、使用來賓iSCSI磁碟機。共享 .VHDX ONTAP SMB 共用中的 Hyper-V over SMB 不支援檔案。

透過SMB組態規劃Hyper-V或SQL Server

完成Volume組態工作表

這份工作表提供一種簡單的方法、可記錄在建立SQL Server磁碟區和SMB上Hyper-V組態時所需的值。

對於每個Volume、您必須指定下列資訊：

- 儲存虛擬機器 (SVM) 名稱

所有磁碟區的SVM名稱都相同。

- Volume名稱
- Aggregate名稱

您可以在叢集中任何節點上的集合體上建立磁碟區。

- 尺寸
- 交會路徑

建立用於儲存應用程式伺服器資料的磁碟區時、請謹記下列事項：

- 如果根磁碟區沒有NTFS安全樣式、則在建立磁碟區時、必須將安全樣式指定為NTFS。

根據預設、磁碟區會繼承SVM根磁碟區的安全樣式。

- 磁碟區應設定預設磁碟區空間保證。
- 您可以選擇性地設定自動調整空間大小的管理設定。
- 您應該設定決定 Snapshot 複本空間保留的選項 0。
- 必須停用套用至磁碟區的Snapshot原則。

如果停用SVM Snapshot原則、則不需要為磁碟區指定Snapshot原則。這些磁碟區會繼承SVM的Snapshot原則。如果SVM的Snapshot原則未停用、且設定為建立Snapshot複本、則您必須在磁碟區層級指定Snapshot原則、而且必須停用該原則。啟用陰影複製服務的備份與SQL Server備份、可管理Snapshot複本的建立與刪除作業。

- 您無法為磁碟區設定負載共用鏡像。

您應選擇要在其中建立應用程式伺服器所使用之共用區的交會路徑、以便共用入口點下方不會有結定的磁碟區。

例如、如果您想要將虛擬機器檔案儲存在四個名為「vol1」、「vol2」、「vol3」和「vol4」的磁碟區、您可以建立範例中所示的命名空間。接著您可以在下列路徑為應用程式伺服器建立共用： /data1/vol1、 /data1/vol2、 /data2/vol3`和 ` /data2/vol4。

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Active			
vs1	data1	true		/data1	RW_volume
vs1	vol1	true		/data1/vol1	RW_volume
vs1	vol2	true		/data1/vol2	RW_volume
vs1	data2	true		/data2	RW_volume
vs1	vol3	true		/data2/vol3	RW_volume
vs1	vol4	true		/data2/vol4	RW_volume

資訊類型	價值
Volume 1：Volume名稱、Aggregate、大小、交會路徑	
Volume 2：Volume 名稱、Aggregate、大小、交會路徑 _	
Volume 3：Volume 名稱、Aggregate、大小、交會路徑 _	
Volume 4：Volume 名稱、Aggregate、大小、交會路徑 _	
Volume 5：Volume 名稱、Aggregate、大小、交會路徑 _	
Volume 6：Volume 名稱、Aggregate、大小、交會路徑 _	
其他磁碟區：磁碟區名稱、Aggregate、大小、交會路徑	

完成SMB共用組態工作表

使用這份工作表單來記錄在建立SQL Server和Hyper-V over SMB組態的持續可用SMB共用時所需的值。

SMB的相關資訊會共用內容和組態設定

對於每個共用區、您必須指定下列資訊：

- 儲存虛擬機器（SVM）名稱

SVM名稱與所有共用相同

- 共用名稱
- 路徑
- 共用內容

您必須設定下列兩個共用內容：

- oplocks
- continuously-available

不得設定下列共用內容：

- homedirectory attributecache
- branchcache
- access-based-enumeration
 - 必須停用 symlinks (的值) -symlink-properties 參數必須為 null (「」)。

共享路徑的相關資訊

如果您使用遠端VSS來備份Hyper-V檔案、則在從Hyper-V伺服器建立SMB連線至儲存虛擬機器檔案的儲存位置時、選擇要使用的共用路徑非常重要。雖然可以在命名空間的任何點建立共用、但Hyper-V伺服器使用的共用路徑不應包含輔助磁碟區。陰影複製作業無法在包含交會點的共用路徑上執行。

建立資料庫目錄結構時、SQL Server無法跨交會。您不應該為包含交會點的SQL Server建立共用路徑。

例如、如果您想要將虛擬機器檔案或資料庫檔案儲存在磁碟區“vol1”、“vol2”、“vol3”及“vol4”上、請在下列路徑為應用程式伺服器建立共用：/data1/vol1、/data1/vol2、/data2/vol3`和`/data2/vol4。

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	data1	true	/data1	RW_volume
vs1	vol1	true	/data1/vol1	RW_volume
vs1	vol2	true	/data1/vol2	RW_volume
vs1	data2	true	/data2	RW_volume
vs1	vol3	true	/data2/vol3	RW_volume
vs1	vol4	true	/data2/vol4	RW_volume



雖然您可以在上建立共用 /data1 和 /data2 管理管理路徑、您不得將應用程式伺服器設定為使用這些共用來儲存資料。

規劃工作表

資訊類型	價值
Volume 1：SMB共用名稱和路徑	
Volume 2：SMB 共享名稱和路徑 _	
_Volume 3：SMB共用名稱和路徑	
Volume 4：SMB共用名稱與路徑	
Volume 5：SMB 共享名稱和路徑 _	
Volume 6：SMB 共享名稱和路徑 _	

資訊類型	價值
Volume 7：SMB 共享名稱和路徑 _	
其他磁碟區：SMB共用名稱和路徑	

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NTLMv2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::*> vsriver cifs options show -vsriver vs1 -fields vsriver,is-
exportpolicy-enabled

vsriver  is-exportpolicy-enabled
-----
vs1      false

cluster1::*> set -privilege admin

```

確認網域帳戶對應至預設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。

當您建立儲存虛擬機器（SVM）時、ONTAP 會自動建立名為「pcuser」的預設使用者（其 UID 為 65534）和名為「pcuser」的群組（具有的 GID 65534）、並將預設使用者新增至「pcuser」群組。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：

```
vsriver cifs options show -vsriver vsriver_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：

```
vsriver services unix-user show -vsriver vsriver_name
```

3. 如果未設定預設使用者選項、而且沒有UNIX使用者可指定為預設UNIX使用者、請建立預設UNIX使用者和預設群組、然後將預設使用者新增至群組。

一般而言、預設使用者的使用者名稱為「pcuser」、必須指派的 UID 65534。預設群組通常會指定群組名稱「pcuser」。指派給群組的 GID 必須是 65534。

- a. 建立預設群組：

```
vsriver services unix-group create -vsriver vsriver_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。

如需使用此命令的詳細資訊、請參閱手冊頁。

範例

下列命令會判斷CIFS伺服器的預設使用者尚未設定、但會判斷「pcuser」使用者和「pcuser」群組是否存在。在SVM VS1上、「pcuser」使用者會被指派為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::> vsserver 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::> vsserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vsserver 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 vsserver_name -fields vsserver,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 vs1 -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 vs1 -fields vs1,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 vs1,volume,security-style
vs1      volume      security-style
-----
vs1      vs1_root      unix

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

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

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。

您需要的產品

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 options 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\
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 [xref:./smb-hyper-v-sql/"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	<code>volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</code>
非NTFS	<code>volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -security-style ntfs -junction-path path</code>

2. 驗證Volume組態是否正確：

```
volume show -vserver vservice_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 vservers_name -junction
```

2. 建立持續可用的SMB共用區：

```
vserver cifs share create -vserver vservers_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

```

Vserver	Volume	Active	Junction Path	Junction 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。

您需要的產品

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。

您需要的產品

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
```

透過SMB組態管理Hyper-V和SQL Server

設定現有共用以確保持續可用度

您可以修改現有的共用區、使其成為持續可用的共用區、讓Hyper-V和SQL Server應用程式伺服器在不中斷營運的情況下存取Hyper-V虛擬機器和組態檔、以及SQL Server資料庫檔案。

關於這項工作

如果共用具有下列特性、您就無法將現有共用區用作持續可用的共用區、以便透過SMB與應用程式伺服器進行不中斷營運：

- 如果是 `homedirectory` 共用屬性是在該共用上設定
- 如果共用包含已啟用的 `symlink` 或 `wdelinks`
- 如果共用區包含位於共用根目錄下方的輔助磁碟區

您必須確認下列兩個共用參數設定正確：

- `-offline-files` 參數設為任一 `manual`（預設）或 `none`。
- 必須停用 `symlink`。

必須設定下列共用內容：

- `continuously-available`
- `oplocks`

不得設定下列共用內容。如果目前共用內容清單中有這些內容、則必須從持續可用的共用區中移除：

- `attributecache`
- `branchcache`

步驟

1. 顯示目前的共用參數設定和目前設定的共用內容清單：

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

2. 如有必要、請修改共用參數以停用 `symlink`、並使用將離線檔案設為手動 `vserver cifs share properties modify` 命令。

您可以設定的值來停用符號連結 `-symlink` 參數至 `""`。

- 您可以設定的值來停用符號連結 `-symlink` 參數至 ""。
- 您可以設定 `-offline-files` 指定參數至正確的設定 `manual`。

3. 新增 `continuously-available` 共用屬性、如有需要、也可共用 `oplocks` 共享內容：

```
vserver cifs share properties add -vserver vserver_name -share-name share_name  
-share-properties continuously-available[,oplock]
```

如果是 `oplocks` 尚未設定共用屬性、您必須將其與一起新增 `continuously-available` 共用屬性。

4. 移除持續可用共用區上不支援的任何共用內容：

```
vserver cifs share properties remove -vserver vserver_name -share-name  
share_name -share-properties properties[,...]
```

您可以使用以逗號分隔的清單來指定共用屬性、以移除一或多個共用屬性。

5. 確認 `-symlink` 和 `-offline-files` 參數設定正確：

```
vserver cifs share show -vserver vserver_name -share-name share_name -fields  
symlink-properties,offline-files
```

6. 確認已設定的共用內容清單正確無誤：

```
vserver cifs shares properties show -vserver vserver_name -share-name  
share_name
```

範例

以下範例說明如何在儲存虛擬機器 (SVM) VS1上、針對NDOS設定名為「shafre1」的現有共用區、並搭配SMB上的應用程式伺服器：

- 透過設定、共用區上的 `symlinks` 會停用 `-symlink` 參數至 ""。
- ◦ `-offline-file` 參數已修改並設為 `manual`。
- ◦ `continuously-available` 共用屬性即會新增至共用。
- ◦ `oplocks` 共用屬性已在共用屬性清單中、因此不需要新增。
- ◦ `attributecache` 共用內容即會從共用中移除。
- ◦ `browsable` 對於透過 SMB 與應用程式伺服器使用的 NDOS 持續可用共用區、則可選用 `Share` 屬性、並保留為其中一個共用屬性。

```
cluster1::> vsserver cifs share show -vsriver vs1 -share-name share1
```

```

        Vserver: vs1
        Share: share1
CIFS Server NetBIOS Name: vs1
        Path: /data
        Share Properties: oplocks
                        browsable
                        attributecache
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: data
        Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1::> vsserver cifs share modify -vsriver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1::> vsserver cifs share properties add -vsriver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vsserver cifs share properties remove -vsriver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1::> vsserver cifs share show -vsriver vs1 -share-name share1
-fields symlink-properties,offline-files
vsriver  share-name symlink-properties offline-files
```

```
-----
vs1      share1      -              manual
```

```
cluster1::> vsserver cifs share properties show -vsriver vs1 -share-name
share1
```

```

        Vserver: vs1
        Share: share1
Share Properties: oplocks
                browsable
                continuously-available
```

啟用或停用適用於SMB備份上Hyper-V的VSS陰影複製

如果您使用支援VSS的備份應用程式來備份儲存在SMB共用區上的Hyper-V虛擬機器檔案、則必須啟用VSS陰影複製。如果您不使用支援VSS的備份應用程式、可以停用VSS陰影複製。預設為啟用VSS陰影複製。

關於這項工作

您可以隨時啟用或停用VSS陰影複製。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行下列其中一項動作：

如果您想要VSS陰影複製...	輸入命令...
已啟用	<pre>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</pre>
已停用	<pre>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</pre>

3. 返回管理權限層級：

```
set -privilege admin
```

範例

下列命令可在SVM VS1上啟用VSS陰影複製：

```
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 modify -vserver vs1 -shadowcopy-enabled
true

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

使用統計資料、透過SMB監控Hyper-V和SQL Server活動

判斷可用的統計資料物件和計數器

在取得CIFS、SMB、稽核和BranchCache雜湊統計資料的相關資訊及監控效能之前、您必須先知道哪些物件和計數器可供您取得資料。

步驟

- 1. 將權限層級設為進階：

```
set -privilege advanced
```

- 2. 執行下列其中一項動作：

如果您想要判斷...	輸入...
可用的物件	<code>statistics catalog object show</code>
可用的特定物件	<code>statistics catalog object show object <i>object_name</i></code>
可用的計數器	<code>statistics catalog counter show object <i>object_name</i></code>

請參閱手冊頁、以取得可用物件和計數器的詳細資訊。

- 3. 返回管理權限層級：

```
set -privilege admin
```

範例

下列命令會顯示與叢集中CIFS和SMB存取相關之所選統計物件的說明、如進階權限層級所示：


```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
      audit_ng          CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
      cifs              The CIFS object reports activity of the
                        Common Internet File System protocol
                        ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
      nblade_cifs       The Common Internet File System (CIFS)
                        protocol is an implementation of the
Server
                        ...
```

```
cluster1::*> statistics catalog object show -object smb1
      smb1              These counters report activity from the
SMB
                        revision of the protocol. For information
                        ...
```

```
cluster1::*> statistics catalog object show -object smb2
      smb2              These counters report activity from the
                        SMB2/SMB3 revision of the protocol. For
                        ...
```

```
cluster1::*> statistics catalog object show -object hashd
      hashd             The hashd object provides counters to
measure
                        the performance of the BranchCache hash
daemon.
```

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

下列命令會顯示的一些計數器相關資訊 `cifs` 進階權限層級的物件：



此範例不會顯示的所有可用計數器 `cifs` 物件；輸出被截斷。

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

顯示SMB統計資料

您可以顯示各種SMB統計資料、以監控效能及診斷問題。

步驟

1. 使用 `statistics start` 和選用 `statistics stop` 用於收集資料範例的命令。
2. 執行下列其中一項動作：

如果您要顯示下列項目的統計資料...	輸入下列命令...
SMB的所有版本	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x和SMB 3.0	<code>statistics show -object smb2</code>
節點的 SMB 子系統	<code>statistics show -object nblade_cifs</code>

深入瞭解 `statistics` 命令：

- ["統計資料會顯示"](#)
- ["統計資料開始"](#)
- ["統計資料停止"](#)

驗證組態是否能夠不中斷營運

使用健全狀況監控來判斷不中斷營運狀態是否健全

健全狀況監控提供有關整個叢集系統健全狀況狀態的資訊。健全狀況監視器會透過SMB組態監控Hyper-V和SQL Server、以確保應用程式伺服器的營運不中斷（NDOS）。如果狀態為降級、您可以檢視問題的詳細資料、包括可能原因和建議的還原動作。

有多個健全狀況監視器。此功能可監控個別健全狀況監視器的整體系統健全狀況和健全狀況。ONTAP節點連線能力健全狀況監視器包含CIFS/NDO子系統。監視器有一組健全狀況原則、可在特定實體狀況可能導致中斷時觸發警示、如果發生中斷情況、則會產生警示並提供修正行動的相關資訊。對於SMB組態而言、會針對下列兩種情況產生警示：

警示ID	嚴重性	條件
HaNotReadyCifsNdo_Alert	主要	節點上某個集合體中某個磁碟區所裝載的一或多個檔案、已透過持續可用的SMB共用區開啟、並承諾在發生故障時持續存在；不過、HA與該合作夥伴的關係可能未設定或不健全。

警示ID	嚴重性	條件
NoStandbyLifCifsNdo_Alert	次要	儲存虛擬機器（SVM）正透過節點主動透過SMB提供資料、且持續在持續可用的共用區上開啟SMB檔案；然而、其合作夥伴節點並未揭露SVM的任何作用中資料生命期。

使用系統健全狀況監控來顯示不中斷營運狀態

您可以使用 `system health` 顯示叢集整體系統健全狀況和 CIFS-n 子系統健全狀況的相關資訊、回應警示、設定未來警示、以及顯示如何設定健全狀況監控的資訊。

步驟

1. 執行適當的動作來監控健全狀況：

如果您要顯示...	輸入命令...
系統的健全狀況、反映個別健全狀況監視器的整體狀態	<code>system health status show</code>
CIFS/NDO子系統健全狀況的相關資訊	<code>system health subsystem show -subsystem CIFS-NDO -instance</code>

2. 顯示有關CIFS/n警示監控如何設定的資訊、方法是執行適當的動作：

如果您想要顯示有關...的資訊	輸入命令...
CIFS/NDO子系統的健全狀況監視器組態與狀態、例如受監控的節點、初始化狀態和狀態	<code>system health config show -subsystem CIFS-NDO</code>
CIF-NDO會發出健全狀況監視器可能產生的警示	<code>system health alert definition show -subsystem CIFS-NDO</code>
CIF-NDO健全狀況監視原則、可決定何時發出警示	<code>system health policy definition show -monitor node-connect</code>



使用 `-instance` 顯示詳細資訊的參數。

範例

下列輸出顯示有關叢集和CIFS/n子系統整體健全狀況狀態的資訊：

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                Subsystem: CIFS-NDO
                Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
  Number of Suppressed Alerts: 0
                Node: node2
  Subsystem Refresh Interval: 5m
```

下列輸出顯示CIFS/n子系統健全狀況監視器的組態與狀態詳細資訊：

```

cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

驗證持續可用的**SMB**共用組態

為了支援不中斷營運、Hyper-V和SQL Server SMB共用必須設定為持續可用的共用。此外、您還必須檢查其他某些共用設定。您應該確認共用已正確設定、以便在發生計畫性或非計畫性的中斷事件時、為應用程式伺服器提供無縫且不中斷營運的作業。

關於這項工作

您必須確認下列兩個共用參數設定正確：

- -offline-files 參數設為任一 manual（預設）或 none。

- 必須停用symlink。

若要正常執行不中斷營運、必須設定下列共用內容：

- continuously-available
- oplocks

不得設定下列共用內容：

- homedirectory
- attributecache
- branchcache
- access-based-enumeration

步驟

1. 確認離線檔案已設定為 manual 或 disabled 而且會停用符號連結：

```
vserver cifs shares show -vserver vs1
```

2. 確認SMB共用區已設定為持續可用度：

```
vserver cifs shares properties show -vserver vs1
```

範例

下列範例顯示儲存虛擬機器（SVM、先前稱為Vserver）VS1上名為「shafre1」的共用區設定。離線檔案設為 manual 且會停用符號連結（在中以連字號指定） Symlink Properties 欄位輸出）：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
          Vserver: vs1
          Share: share1
CIFS Server NetBIOS Name: VS1
          Path: /data/share1
      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
```

下列範例顯示SVM VS1上名為「shafre1」之共用區的共用內容：

```
cluster1::> vsriver cifs share properties show -vsriver vs1 -share-name
share1
Vserver      Share      Properties
-----
vs1          share1    oplocks
              continuously-available
```

驗證LIF狀態

即使您將採用Hyper-V的儲存虛擬機器（SVM）和SQL Server設定為採用SMB組態、以在叢集中的每個節點上擁有生命、在日常作業期間、某些生命體可能會移至另一個節點上的連接埠。您必須驗證LIF狀態、並採取任何必要的修正行動。

關於這項工作

若要提供無縫且不中斷營運的作業支援、叢集中的每個節點必須至少有一個LIF用於SVM、而且所有LIF都必須與主連接埠相關聯。如果部分已設定的生命期目前未與其主連接埠建立關聯、您必須修正任何連接埠問題、然後將生命期還原至其主連接埠。

步驟

1. 顯示SVM的已設定LIF相關資訊：

```
network interface show -vsriver vsriver_name
```

在此範例中、「lif1」不在主連接埠上。

```
network interface show -vsriver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
vs1						
	lif1	up/up	10.0.0.128/24	node2	e0d	
false						
	lif2	up/up	10.0.0.129/24	node2	e0d	
true						

2. 如果部分生命區不在其主連接埠上、請執行下列步驟：

- a. 針對每個LIF、判斷LIF的主連接埠：

```
network interface show -vsriver vsriver_name -lif lif_name -fields home-  
node,home-port
```

```
network interface show -vsriver vs1 -lif lif1 -fields home-node,home-port
```



```

vserver lif  home-node  home-port
-----
vs1      lif1 node1      e0d

```

- b. 針對每個LIF、判斷LIF的主連接埠是否正常運作：

```
network port show -node node_name -port port -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

```

node      port link
-----
node1     e0d  up

```

+ 在此範例中、「lif1」應移轉回其主連接埠、node1:e0d。

3. 如果有任何應與生命相關聯的主連接埠網路介面不在中 up 請解決問題、讓這些介面正常運作。
4. 如有需要、請將生命 回復至主連接埠：

```
network interface revert -vserver vserver_name -lif lif_name
```

```
network interface revert -vserver vs1 -lif lif1
```

5. 確認叢集中的每個節點都有SVM的作用中LIF：

```
network interface show -vserver vserver_name
```

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	
true	lif2	up/up	10.0.0.129/24	node2	e0d	
true						

判斷SMB工作階段是否持續可用

顯示SMB工作階段資訊

您可以顯示已建立SMB工作階段的相關資訊、包括SMB連線和工作階段ID、以及使用工作階段之工作站的IP位址。您可以顯示工作階段SMB傳輸協定版本的相關資訊、以及持續可用的保護層級、協助您識別工作階段是否支援不中斷營運。

關於這項工作

您可以在SVM上以摘要形式顯示所有工作階段的資訊。不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊：


- 您可以使用選用的 `-fields` 參數顯示有關所選欄位的輸出。
您可以輸入 `-fields ?` 決定您可以使用哪些欄位。
- 您可以使用 `-instance` 顯示已建立 SMB 工作階段的詳細資訊的參數。
- 您可以使用 `-fields` 參數或 `-instance` 參數可以單獨使用、也可以搭配其他選用參數使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示 SMB 工作階段資訊...	輸入下列命令...
以摘要形式顯示SVM上的所有工作階段	<code>vserver cifs session show -vserver <i>vserver_name</i></code>
在指定的連線ID上	<code>vserver cifs session show -vserver <i>vserver_name</i> -connection-id integer</code>
從指定的工作站IP位址	<code>vserver cifs session show -vserver <i>vserver_name</i> -address <i>workstation_IP_address</i></code>
在指定的LIF IP位址上	<code>vserver cifs session show -vserver <i>vserver_name</i> -lif -address <i>LIF_IP_address</i></code>
在指定的節點上	<code>`*vserver cifs session show -vserver <i>vserver_name</i> -node {node_name</code>
<code>local}*`</code>	從指定的Windows使用者

如果您要顯示 SMB 工作階段資訊...	輸入下列命令...
<pre> vserver cifs session show -vserver vserver_name -windows-user user_name </pre> <p>的格式 <code>user_name</code> 是 <code>[domain]\user</code>。</p>	使用指定的驗證機制
<pre> vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mechanism </pre> <p>的價值 <code>-auth</code> <code>-mechanism</code> 可以是下列其中一項：</p> <ul style="list-style-type: none"> • NTLMv1 • NTLMv2 • Kerberos • Anonymous 	使用指定的傳輸協定版本

<p>如果您要顯示SMB工作階段資訊...</p>	<p>輸入下列命令...</p>
<div data-bbox="175 195 493 407"> <pre> vserver cifs session show -vserver vserver_name -protocol-version protocol_version </pre> </div> <div data-bbox="175 443 493 546"> <p>的價值 -protocol -version 可以是下列其中一項：</p> </div> <div data-bbox="203 583 331 840"> <ul style="list-style-type: none"> • SMB1 • SMB2 • SMB2_1 • SMB3 • SMB3_1 </div> <div data-bbox="258 1318 316 1375">  </div> <div data-bbox="370 884 466 1810"> <p>持續可用的保護功能和SMB多通道功能僅適用於SMB 3.0及更新版本的工作階段。若要在所有合格的工作階段中檢視其狀態、您應該指定此參數、並將值設為SMB3或更新版本。</p> </div>	<div data-bbox="505 195 876 226"> <p>提供特定等級的持續可用保護</p> </div>

<p>如果您要顯示SMB工作階段資訊...</p>	<p>輸入下列命令...</p>
<div data-bbox="181 197 495 510"> <pre> vserver cifs session show -vserver vserver_name -continuously -available continuously_avail able_protection_le vel </pre> </div> <div data-bbox="181 550 495 651"> <p>的價值 -continuously -available 可以是下列其中一項：</p> </div> <div data-bbox="207 690 347 833"> <ul style="list-style-type: none"> • No • Yes • Partial </div> <div data-bbox="214 1354 269 1411">  </div> <div data-bbox="331 882 462 1883"> <p>如果持續可用的狀態為 Partial、這表示工作階段至少包含一個開啟的持續可用檔案、但工作階段有一些檔案無法以持續可用的保護開啟。您可以使用 <code>\vserver cifs sessions file show</code> 命令來判斷已建立工作階段上的哪些檔案未以持續可用的保護開啟。</p> </div>	<p>具有指定的SMB簽署工作階段狀態</p>

範例

下列命令會顯示SVM VS1上從IP位址為10.1.1.1的工作站所建立之工作階段的工作階段資訊：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1        DOMAIN\joe        2         23s
```

下列命令會顯示SVM VS1具有持續可用保護之工作階段的詳細工作階段資訊。連線是使用網域帳戶建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

下列命令會顯示SVM VS1上使用SMB 3.0和SMB多通道之工作階段的工作階段資訊。在此範例中、使用者使用LIF IP位址從具有SMB 3.0功能的用戶端連線到此共用區、因此驗證機制預設為NTLMv2。連線必須使用Kerberos驗證、才能以持續可用的保護進行連線。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

顯示開啟SMB檔案的相關資訊

您可以顯示開啟SMB檔案的相關資訊、包括SMB連線和工作階段ID、託管磁碟區、共用名稱和共用路徑。您也可以顯示檔案持續可用保護層級的相關資訊、這有助於判斷開啟的檔案是否處於支援不中斷營運的狀態。

關於這項工作

您可以在已建立的SMB工作階段中顯示開啟檔案的相關資訊。當您需要判斷SMB工作階段中特定檔案的SMB工作階段資訊時、所顯示的資訊非常有用。

例如、如果您有 SMB 工作階段、其中某些開啟的檔案會以持續可用的保護開啟、有些則無法以持續可用的保護開啟（的值）`-continuously-available` 欄位輸入 `vserver cifs session show` 命令輸出為 `Partial`）、您可以使用此命令來判斷哪些檔案無法持續使用。

您可以使用、以摘要形式顯示已建立的儲存虛擬機器（SVM）SMB 工作階段上所有開啟檔案的資訊 `vserver cifs session file show` 不含任何選用參數的命令。

不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊。如果您只想檢視開啟檔案的一小部分資訊、這項功能就很有幫助。

- 您可以使用選用的 `-fields` 參數、可在您選擇的欄位上顯示輸出。

您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

- 您可以使用 `-instance` 顯示開啟 SMB 檔案的詳細資訊的參數。

您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示開啟的SMB檔案...	輸入下列命令...
在SVM上以摘要形式顯示	<code>vserver cifs session file show -vserver vserver_name</code>
在指定的節點上	<code>`*vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}*`</code>	在指定的檔案ID上
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	在指定的SMB連線ID上
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	在指定的SMB工作階段ID上
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	在指定的託管Aggregate上
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	在指定的磁碟區上
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	在指定的SMB共用區上
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	在指定的SMB路徑上
<code>vserver cifs session file show -vserver vserver_name -path path</code>	提供指定等級的持續可用保護

<p>如果您要顯示開啟的SMB檔案...</p> <pre>vserver cifs session file show -vserver vserver_name -continuously -available continuously_available_status</pre> <p>的價值 <code>-continuously-available</code> 可以是下列其中一項：</p> <ul style="list-style-type: none"> • No • Yes <div>  <p>如果持續可用的狀態為 `No` 這表示這些開啟的檔案無法不中斷地從接管和恢復恢復。在高可用度關係中、他們也無法從合作夥伴之間的一般Aggregate重新配置中恢復。</p> </div>	<p>輸入下列命令...</p> <p>指定的重新連線狀態</p>
--	-----------------------------------

您可以使用其他選用參數來精簡輸出結果。如需詳細資訊、請參閱手冊頁。

範例

下列範例顯示SVM VS1上開啟檔案的相關資訊：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:   1
File       File       Open Hosting      Continuously
ID         Type        Mode Volume      Share      Available
-----
41         Regular    r      data          data      Yes
Path: \mytest.rtf
```

下列範例顯示SVM VS1上開啟檔案ID為82的SMB檔案的詳細資訊：

```
cluster1::> vsriver cifs session file show -vsriver vs1 -file-id 82
-instance
```

```
      Node: node1
      Vserver: vs1
      File ID: 82
      Connection ID: 104617
      Session ID: 1
      File Type: Regular
      Open Mode: rw
Aggregate Hosting File: aggr1
  Volume Hosting File: data1
      CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
      Share Mode: rw
      Range Locks: 1
Continuously Available: Yes
      Reconnected: No
```

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。