使用選項自訂SMB伺服器

ONTAP 9

NetApp
April 24, 2024

目錄

使用選項自訂SMB伺服器

可用的SMB伺服器選項

在考量如何自訂SMB伺服器時、瞭解可用的選項很有用。雖然有些選項適用於SMB伺服器的一般用途、但有幾個選項可用來啟用和設定特定的SMB功能。SMB 伺服器選項由控制 `vserver cifs options modify` 選項。

下列清單指定可在管理權限層級使用的SMB伺服器選項：

- 設定**SMB**工作階段逾時值

  設定此選項可讓您指定SMB工作階段中斷連線之前的閒置時間秒數。閒置工作階段是指使用者在用戶端上沒有開啟任何檔案或目錄的工作階段。預設值為 900 秒。

- 設定預設的**UNIX**使用者

  設定此選項可讓您指定SMB伺服器使用的預設UNIX使用者。自動建立名為「'pcuser'」的預設使用者（UID為65534）、建立名為「'pcuser'」的群組（gid為65534）、並將預設使用者新增至「'pcuser'」群組。ONTAP當您建立SMB伺服器時ONTAP 、支援將「'pcuser'」自動設定為預設UNIX使用者。

- 設定來賓**UNIX**使用者

  設定此選項可讓您指定從不受信任網域登入的使用者所對應的UNIX使用者名稱、如此可讓來自不受信任網域的使用者連線至SMB伺服器。根據預設、此選項並未設定（沒有預設值）；因此、預設值是不允許來自不受信任網域的使用者連線至SMB伺服器。

- *啟用或停用模式位元*的讀取授與執行

  啟用或停用此選項可讓您指定是否允許SMB用戶端以UNIX模式位元執行可執行檔、即使未設定UNIX執行檔位元、也能存取這些位元。此選項預設為停用。

- 啟用或停用從**NFS**用戶端刪除唯讀檔案的功能

  啟用或停用此選項可決定是否允許NFS用戶端刪除具有唯讀屬性集的檔案或資料夾。NTFS刪除語義不允許在設定唯讀屬性時刪除檔案或資料夾。UNIX刪除語義會忽略唯讀位元、改用父目錄權限來判斷是否可以刪除檔案或資料夾。預設設定為 `disabled`，從而產生 NTFS 刪除義。

- 設定**Windows**網際網路名稱服務伺服器位址

  設定此選項可讓您將Windows網際網路名稱服務（WINS）伺服器位址清單指定為以逗號分隔的清單。您必須指定IPV4位址。不支援IPv6位址。沒有預設值。

下列清單指定可在進階權限層級使用的SMB伺服器選項：

- 授予**CIFS**使用者**UNIX**群組權限

  設定此選項可決定是否可以將不是檔案擁有者的傳入CIFS使用者授予群組權限。如果 CIFS 使用者不是 UNIX 安全樣式檔案的擁有者、則此參數會設為 `true`，則會授予該檔案的群組權限。如果 CIFS 使用者不是 UNIX 安全樣式檔案的擁有者、則此參數會設為 `false`，然後，正常的 UNIX 規則適用於授予檔案權限。此

參數適用於權限設為的 UNIX 安全性樣式檔案 `mode bits` 且不適用於 NTFS 或 NFSv4 安全模式的檔案。預設設定為 `false`。

- 啟用或停用**SMB 1.0**

  SMB 1.0在SVM上預設為停用、而SVM是在ONTAP SVM上建立SMB伺服器、以供使用。

  > 從功能9.3開始ONTAP 、ONTAP 根據預設、針對以功能9.3建立的新SMB伺服器、會停用SMB 1.0。您應該盡快移轉至較新的SMB版本、以準備增強安全性和法規遵循。如需詳細資訊、請聯絡您的NetApp代表。

- *啟用或停用SMB 2.x *

  SMB 2.0是支援LIF容錯移轉的最小SMB版本。如果停用SMB 2.x、ONTAP 則無法使用支援功能的功能也會自動停用SMB 3.x

  SMB 2.0僅在SVM上受支援。此選項在SVM上預設為啟用

- * 啟用或停用 SMB 3.0*

  SMB 3.0是支援持續可用共用的最小SMB版本。Windows Server 2012和Windows 8是支援SMB 3.0的最低Windows版本。

  SMB 3.0 僅支援 SVM 。此選項在SVM上預設為啟用

- * 啟用或停用 SMB 3.1*

  Windows 10是唯一支援SMB 3.1的Windows版本。

  SMB 3.1 僅支援 SVM 。此選項在SVM上預設為啟用

- 啟用或停用**ODX**複本卸載

  支援ODX複本卸載的Windows用戶端會自動使用ODX複本卸載。此選項預設為啟用。

- 啟用或停用**ODX**複本卸載的直接複製機制

  當Windows用戶端嘗試以一種模式開啟複本的來源檔案時、直接複製機制可提高複本卸載作業的效能、避免在複本進行期間變更檔案。根據預設、直接複製機制會啟用。

- 啟用或停用自動節點參照

  使用自動節點參照時、SMB伺服器會自動將用戶端參照到本機資料LIF、並將其指向裝載透過所要求共用區存取資料的節點。

- *啟用或停用SMB*的匯出原則

  此選項預設為停用。

- 啟用或停用使用連接點做為重新分析點

  如果啟用此選項、SMB伺服器會將連接點公開給SMB用戶端做為重新分析點。此選項僅適用於SMB 2.x或SMB 3.0連線。此選項預設為啟用。

此選項僅在SVM上受支援。此選項在SVM上預設為啟用

- 設定每個**TCP**連線同時執行的最大作業數

  預設值為 255 。

- 啟用或停用本機**Windows**使用者和群組功能

  此選項預設為啟用。

- 啟用或停用本機**Windows**使用者驗證

  此選項預設為啟用。

- 啟用或停用**VSS**陰影複製功能

  利用陰影複製功能、對使用Hyper-V over SMB解決方案儲存的資料執行遠端備份。ONTAP

  此選項僅在SVM上受支援、僅在Hyper-V over SMB組態上受支援。此選項在SVM上預設為啟用

- 設定陰影複製目錄深度

  設定此選項可讓您定義在使用陰影複製功能時建立陰影複製的目錄深度上限。

  此選項僅在SVM上受支援、僅在Hyper-V over SMB組態上受支援。此選項在SVM上預設為啟用

- 啟用或停用名稱對應的多網域搜尋功能

  如果啟用、當UNIX使用者透過在Windows使用者名稱的網域部分（例如*\Joe）中使用萬用字元（*）對應至Windows網域使用者時ONTAP 、將會在所有具有雙向信任的網域中搜尋指定使用者。主網域是包含SMB伺服器電腦帳戶的網域。

  除了搜尋雙向信任的所有網域之外、您也可以設定偏好的信任網域清單。如果啟用此選項且已設定偏好的清單、則會使用偏好的清單來執行多網域名稱對應搜尋。

  預設為啟用多網域名稱對應搜尋。

- 設定檔案系統區段大小

  設定此選項可讓您設定以位元組為單位的檔案系統區段大小、ONTAP 以便向SMB用戶端回報。此選項有兩個有效值： `4096` 和 `512`。預設值為 `4096`。您可能需要將此值設為 `512` 如果 Windows 應用程式僅支援 512 位元組的扇區大小。

- 啟用或停用動態存取控制

  啟用此選項可讓您使用動態存取控制（DAC）來保護SMB伺服器上的物件、包括使用稽核來登入中央存取原則、以及使用群組原則物件來實作中央存取原則。此選項預設為停用。

  此選項僅在SVM上受支援。

- 設定未驗證工作階段的存取限制（限制匿名）

  設定此選項可決定未驗證工作階段的存取限制。這些限制適用於匿名使用者。根據預設、匿名使用者沒有存

取限制。

- 在具有**UNIX**有效安全性的磁碟區上啟用或停用**NTFS ACL**的呈現（**UNIX**安全型磁碟區或具有**UNIX**有效安全性的混合式安全型磁碟區）

  啟用或停用此選項可決定如何向SMB用戶端呈現具有UNIX安全性之檔案和資料夾的檔案安全性。如果啟用ONTAP 此功能、則使用NTFS ACL將具有UNIX安全性的磁碟區中的檔案和資料夾、顯示為具有NTFS檔案安全性。如果停用ONTAP 、則在不提供檔案安全性的情況下、將UNIX安全性的磁碟區顯示為FAT磁碟區。根據預設、磁碟區會以NTFS ACL的NTFS檔案安全性呈現。

- 啟用或停用**SMB**假開放功能

  啟用此功能可最佳化ONTAP 當查詢檔案和目錄的屬性資訊時、如何執行開放和關閉要求、進而改善SMB 2.x和SMB 3.0的效能。依預設、SMB假開放功能已啟用。此選項僅適用於使用SMB 2.x或更新版本的連線。

- 啟用或停用**UNIX**擴充功能

  啟用此選項可在SMB伺服器上啟用UNIX擴充功能。UNIX擴充功能可透過SMB傳輸協定顯示POSIX / UNIX類型的安全性。此選項預設為停用。

  如果您的環境中有UNIX型SMB用戶端（例如Mac OSX用戶端）、則應該啟用UNIX擴充功能。啟用UNIX擴充功能可讓SMB伺服器透過SMB將Posix / UNIX安全資訊傳輸到UNIX用戶端、然後將安全資訊轉譯為POSIX / UNIX安全性。

- 啟用或停用對簡短名稱搜尋的支援

  啟用此選項可讓SMB伺服器針對簡短名稱執行搜尋。啟用此選項的搜尋查詢會嘗試比對8.3檔名和長檔名。此參數的預設值為 `false`。

- *啟用或停用對自動通告DFS*功能的支援

  啟用或停用此選項可決定SMB伺服器是否自動向連線至共用的SMB 2.x和SMB 3.0用戶端通告DFS功能。在實作SMB存取的符號連結時、使用DFS轉介。ONTAP如果啟用、則無論是否啟用符號連結存取、SMB伺服器一律會通告DFS功能。如果停用、SMB伺服器只會在用戶端連線至啟用符號連結存取的共用時、才會通告「DFS功能」。

- 設定**SMB**點數上限

  從 ONTAP 9.4 開始、設定 `-max-credits` 選項可讓您在用戶端和伺服器執行 SMB 版本 2 或更新版本時、限制 SMB 連線上要授予的點數數量。預設值為 128 。

- *啟用或停用SMB多通道*支援

  啟用 `-is-multichannel-enabled` ONTAP 9.4 及更新版本中的選項可讓 SMB 伺服器在叢集及其用戶端上部署適當的 NIC 時、為單一 SMB 工作階段建立多個連線。這樣做可改善處理量和容錯能力。此參數的預設值為 `false`。

  啟用SMB多通道時、您也可以指定下列參數：

  - 每個多通道工作階段允許的最大連線數。此參數的預設值為 32 。
  - 每個多通道工作階段所通告的網路介面數量上限。此參數的預設值為 256 。

設定SMB伺服器選項

您可以在儲存虛擬機器（SVM）上建立SMB伺服器之後、隨時設定SMB伺服器選項。

步驟

1. 執行所需的動作：

如果您要設定SMB伺服器選項...	輸入命令...
管理員權限等級	`vserver cifs options modify -vserver` *`vserver_name options`*
進階權限層級	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

如需設定 SMB 伺服器選項的詳細資訊、請參閱的手冊頁 `vserver cifs options modify` 命令。

設定授予SMB使用者UNIX群組權限

即使傳入的SMB使用者不是檔案的擁有者、您也可以設定此選項、以授予群組存取檔案或目錄的權限。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 視需要設定授予UNIX群組權限：

如果您想要	輸入命令
即使使用者不是檔案的擁有者、也能存取檔案或目錄、以取得群組權限	`vserver cifs options modify -grant-unix-group-perms-to-others true`
即使使用者不是檔案的擁有者、也請停用檔案或目錄的存取權、以取得群組權限	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. 確認選項設定為所需的值： `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. 返回管理權限層級： `set -privilege admin`

設定匿名使用者的存取限制

根據預設、匿名、未驗證的使用者（也稱為_null使用者_）可以存取網路上的特定資訊。

您可以使用SMB伺服器選項來設定匿名使用者的存取限制。

關於這項工作

- `-restrict-anonymous` SMB 伺服器選項對應於 `RestrictAnonymous` Windows 中的登錄項目。

匿名使用者可以從網路上的Windows主機列出或列舉特定類型的系統資訊、包括使用者名稱和詳細資料、帳戶原則和共用名稱。您可以指定下列三種存取限制設定之一來控制匿名使用者的存取：

價值	說明
`no-restriction` （預設）	不指定匿名使用者的存取限制。
`no-enumeration`	指定僅限匿名使用者進行列舉。
`no-access`	指定匿名使用者的存取受到限制。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 設定限制匿名設定： `vserver cifs options modify -vserver vserver_name -restrict -anonymous {no-restriction|no-enumeration|no-access}`
3. 確認選項設定為所需的值： `vserver cifs options show -vserver vserver_name`
4. 返回管理權限層級： `set -privilege admin`

相關資訊

可用的SMB伺服器選項

管理如何向SMB用戶端提供UNIX安全型資料的檔案安全性

管理如何向SMB用戶端提供檔案安全性、以利UNIX安全型態的資料總覽

您可以啟用或停用將NTFS ACL呈現給SMB用戶端的功能、來選擇如何向SMB用戶端展示UNIX安全型資料的檔案安全性。每項設定都有優點、您應該瞭解如何選擇最適合您業務需求的設定。

根據預設、ONTAP 將UNIX安全型磁碟區上的UNIX權限以NTFS ACL形式呈現給SMB用戶端。有些情況需要這樣做、包括：

- 您想要使用「Windows內容」方塊中的「安全性」索引標籤來檢視及編輯UNIX權限。

  如果UNIX系統不允許此作業、您就無法從Windows用戶端修改權限。例如、您無法變更您不擁有的檔案所有權、因為UNIX系統不允許此作業。此限制可防止SMB用戶端略過在檔案和資料夾上設定的UNIX權限。

- 使用者使用某些Windows應用程式（例如Microsoft Office）來編輯及儲存UNIX安全型磁碟區上的檔案、ONTAP 而在這些應用程式中、當執行儲存作業時、必須保留UNIX權限。
- 您環境中有些Windows應用程式預期會讀取其所使用檔案的NTFS ACL。

在某些情況下、您可能會想要停用將UNIX權限呈現為NTFS ACL的功能。如果停用此功能、ONTAP 則將UNIX安全型磁碟區顯示為SMB用戶端的FAT磁碟區。您可能會想要將UNIX安全型磁碟區以FAT磁碟區的形式呈現給SMB用戶端的具體理由如下：

- 您只能在UNIX用戶端上使用掛載來變更UNIX權限。

  當SMB用戶端上對應UNIX安全型磁碟區時、「安全性」索引標籤將無法使用。對應的磁碟機似乎是以不具檔案權限的檔案系統格式化。

- 您正在使用SMB上的應用程式、在存取的檔案和資料夾上設定NTFS ACL、如果資料位於UNIX安全型磁碟區、則這些應用程式可能會失敗。

  如果ONTAP 將磁碟區報告為「FAT」、應用程式就不會嘗試變更ACL。

相關資訊

在FlexVol 功能區上設定安全樣式

在qtree上設定安全性樣式

啟用或停用**NTFS ACL**的**UNIX**安全型資料呈現

您可以針對UNIX安全型資料（UNIX安全型磁碟區和混合式安全型磁碟區、以及UNIX有效安全性）、啟用或停用將NTFS ACL呈現給SMB用戶端的功能。

關於這項工作

如果啟用此選項、ONTAP 則將具有有效UNIX安全樣式的磁碟區上的檔案和資料夾、呈現給SMB用戶端、如同使用NTFS ACL。如果停用此選項、磁碟區會以FAT磁碟區的形式呈現給SMB用戶端。預設為向SMB用戶端顯示NTFS ACL。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 設定 UNIX NTFS ACL 選項設定： `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. 確認選項設定為所需的值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回管理權限層級： `set -privilege admin`

如何保留**UNIX**權限**ONTAP**

當Windows應用程式編輯並儲存目前具有UNIX權限的FlexVol 檔案時ONTAP 、即可保留UNIX權限。

當Windows用戶端上的應用程式編輯及儲存檔案時、他們會讀取檔案的安全性內容、建立新的暫存檔、將這些內容套用至暫存檔、然後為暫存檔提供原始檔案名稱。

當Windows用戶端執行安全性內容查詢時、會收到完全代表UNIX權限的建構ACL。此建構ACL的唯一目的是在Windows應用程式更新檔案時、保留檔案的UNIX權限、以確保產生的檔案具有相同的UNIX權限。不使用建構的ACL來設定任何NTFS ACL。ONTAP

使用**Windows**安全性索引標籤管理**UNIX**權限

如果您想要在混合式安全型磁碟區或SVM上的qtree中、處理檔案或資料夾的UNIX權限、可以使用Windows用戶端上的「安全性」索引標籤。或者、您也可以使用可查詢及設定Windows ACL的應用程式。

- 修改UNIX權限

  您可以使用「Windows安全性」索引標籤來檢視及變更混合式安全性型磁碟區或qtree的UNIX權限。如果您使用Windows安全性主索引標籤來變更UNIX權限、則必須先移除您要編輯的現有ACE（這會將模式位元設為0）、才能進行變更。或者、您也可以使用進階編輯器來變更權限。

  如果使用模式權限、您可以直接變更所列的UID、GID和其他（電腦上有帳戶的其他人）的模式權限。例如、如果顯示的UID具有r-x權限、您可以將UID權限變更為rwx。

- 將UNIX權限變更為NTFS權限

  您可以使用「Windows安全性」索引標籤、將UNIX安全性物件取代為混合式安全性型磁碟區或qtree上的Windows安全性物件、其中檔案和資料夾具有UNIX有效的安全性樣式。

  您必須先移除所有列出的UNIX權限項目、才能將其取代為所需的Windows使用者和群組物件。然後您可以在Windows使用者和群組物件上設定NTFS型ACL。只要移除所有UNIX安全性物件、並將Windows使用者和群組新增至混合式安全性型磁碟區或qtree中的檔案或資料夾、即可將檔案或資料夾上的有效安全性樣式從UNIX變更為NTFS。

  變更資料夾的權限時、預設的Windows行為是將這些變更傳播到所有子資料夾和檔案。因此、如果您不想將安全性樣式的變更傳播到所有子資料夾、子資料夾和檔案、則必須將傳播選項變更為所需的設定。