使用 **VScan** 保護病毒

ONTAP 9

NetApp
August 31, 2024

目錄

使用 VScan 保護病毒

防毒組態總覽

VScan 是由 NetApp 開發的防毒掃描解決方案、可讓客戶保護資料免於受到病毒或其他惡意程式碼的侵害。

當用戶端透過 SMB 存取檔案時、 VScan 會執行病毒掃描。您可以將 VScan 設定為隨需或依排程進行掃描。您可以使用 ONTAP 命令列介面（ CLI ）或 ONTAP 應用程式設計介面（ API ）與 VScan 互動。

相關資訊

"VScan 合作夥伴解決方案"

關於NetApp防毒保護

關於NetApp掃毒

VScan 是由 NetApp 開發的防毒掃描解決方案、可讓客戶保護資料免於受到病毒或其他惡意程式碼的侵害。它結合了合作夥伴提供的防毒軟體與 ONTAP 功能、讓客戶能夠靈活地管理檔案掃描。

掃毒的運作方式

儲存系統會將掃描作業卸載至裝載協力廠商防毒軟體的外部伺服器。

根據使用中的掃描模式、當用戶端透過 SMB （存取時）存取檔案或存取特定位置、排程或立即（隨需）的檔案時、 ONTAP 會傳送掃描要求。

- 當用戶端透過SMB開啟、讀取、重新命名或關閉檔案時、您可以使用「存取時掃描」來檢查是否有病毒。檔案作業會暫停、直到外部伺服器回報檔案的掃描狀態為止。如果檔案已掃描完畢、ONTAP 則支援檔案操作。否則、它會要求伺服器進行掃描。

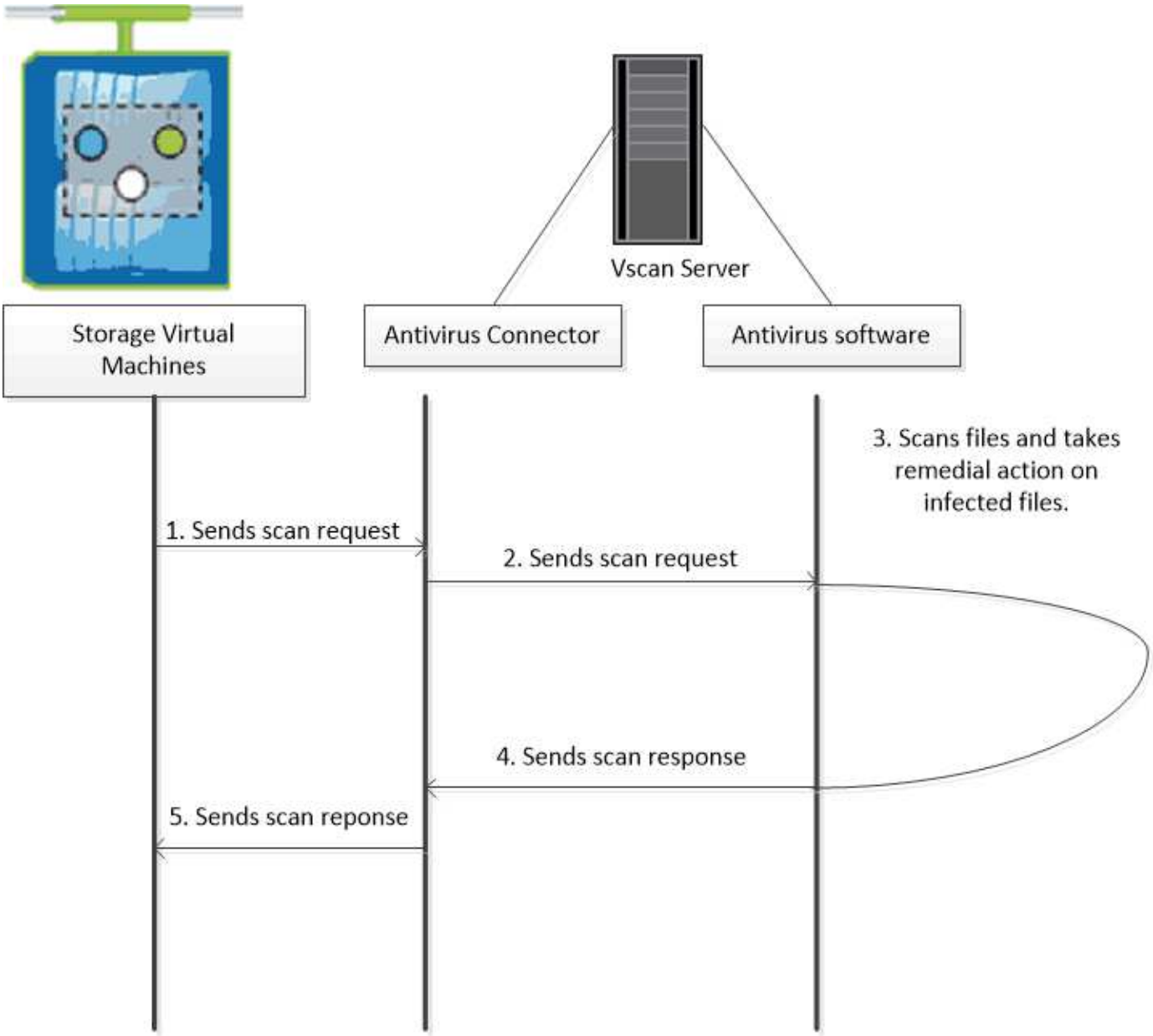
  NFS不支援存取時掃描。

- 您可以使用隨需掃描_來立即或排程檢查檔案是否有病毒。我們建議隨選掃描只在非尖峰時間執行、以避免現有的 AV 基礎架構過載、而這種基礎架構通常會設定為存取掃描的大小。外部伺服器會更新已核取檔案的掃描狀態、以便透過 SMB 降低檔案存取延遲。如果有檔案修改或軟體版本更新、它會要求從外部伺服器進行新的檔案掃描。

  您可以針對SVM命名空間中的任何路徑使用隨需掃描、即使是僅透過NFS匯出的磁碟區也一樣。

您通常可以在 SVM 上同時啟用存取和隨選掃描模式。在任一模式中、防毒軟體都會根據您的軟體設定、針對受感染的檔案採取補救行動。

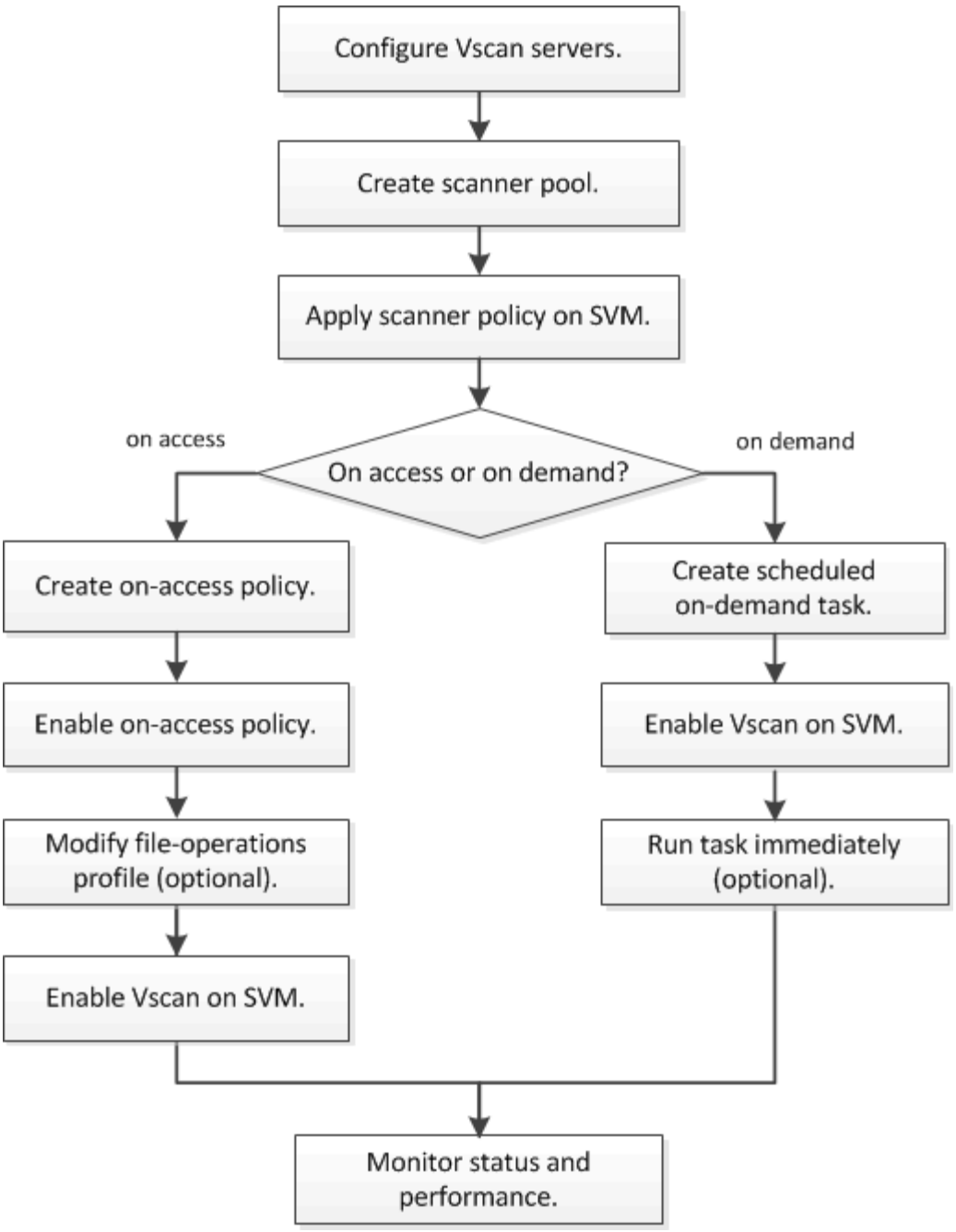
由NetApp提供並安裝在外部伺服器上的《The停止防毒連接器：處理儲存系統與防毒軟體之間的通訊。ONTAP



掃毒工作流程

您必須先建立掃描器資源池並套用掃描器原則、才能啟用掃描。您通常可以在 SVM 上同時啟用存取和隨選掃描模式。

您必須已完成CIFS組態。



後續步驟

- 在單一叢集上建立掃描器集區
- 在單一叢集上套用掃描器原則
- 建立存取時原則

防毒架構

NetApp 防毒架構包含 VScan 伺服器軟體和相關設定。

VScan 伺服器軟體

您必須在 VScan 伺服器上安裝此軟體。

- 《防毒連接器》 ONTAP

  這是 NetApp 提供的軟體、可處理 SVM 與防毒軟體之間的掃描要求與回應通訊。它可以在虛擬機器上執行、但為了達到最佳效能、請使用實體機器。您可以從 NetApp 支援網站 下載此軟體（需要登入）。

- 防毒軟體

  這是合作夥伴提供的軟體、可掃描檔案中是否有病毒或其他惡意程式碼。您可以指定在設定軟體時、對受感染檔案採取的補救行動。

VScan 軟體設定

您必須在 VScan 伺服器上設定這些軟體設定。

- 掃描器資源池

  此設定定義可連線至 SVM 的 VScan 伺服器和授權使用者。它也定義掃描要求逾時期間、之後若有可用的VScan伺服器、掃描要求會傳送至替代的VScan伺服器。

  > 您應該將 VScan 伺服器上防毒軟體的逾時時間設定為比掃描器集區掃描要求逾時時間少五秒。這可避免因為軟體的逾時時間超過掃描要求的逾時時間、導致檔案存取延遲或完全遭拒的情況。

- 貴賓使用者

  此設定是 VScan 伺服器用來連線至 SVM 的網域使用者帳戶。帳戶必須存在於掃描器集區中的授權使用者清單中。

- 掃描程式原則

  此設定決定掃描器集區是否為作用中。掃描器原則是系統定義的、因此您無法建立自訂的掃描器原則。只有這三個原則可供使用：

  - `Primary` 指定掃描儀池處於活動狀態。
  - `Secondary` 指定掃瞄器集區為作用中、只有在沒有連接主要掃瞄器集區中的 VScan 伺服器時。
  - `Idle` 指定掃描器集區為非作用中。

- 存取原則

  此設定定義存取掃描的範圍。您可以指定要掃描的檔案大小上限、掃描中要包含的檔案副檔名和路徑、以及要從掃描中排除的檔案副檔名和路徑。

  依預設、只會掃描讀寫磁碟區。您可以指定篩選條件、以允許掃描唯讀磁碟區、或限制掃描以執行存取開啟的檔案：

  - `scan-ro-volume` 可掃描唯讀磁碟區。
  - `scan-execute-access` 限制掃描至以執行存取權限開啟的檔案。

  > 「執行存取」與「執行權限」不同。 只有在以「執行目的」開啟檔案時、指定的用戶端才能在執行檔上擁有「執行存取」。

您可以設定 `scan-mandatory` 選項為「關閉」、可指定在沒有 VScan 伺服器可供病毒掃描時、允許檔案存取。在存取模式中、您可以從這兩個互斥的選項中選擇：

- 必要：使用此選項、 VScan 會嘗試將掃描要求傳送至伺服器、直到逾時期間過期為止。如果伺服器不接受掃描要求、則用戶端存取要求會遭到拒絕。
- 非必要：無論 VScan 伺服器是否可用於掃毒、 VScan 都一律允許用戶端存取。

- 隨需工作

此設定定義隨選掃描的範圍。您可以指定要掃描的檔案大小上限、掃描中要包含的檔案副檔名和路徑、以及要從掃描中排除的檔案副檔名和路徑。依預設會掃描子目錄中的檔案。

您可以使用cron排程來指定工作執行的時間。您可以使用 `vserver vscan on-demand-task run` 立即執行工作的命令。

- * VScan檔案作業設定檔（僅限存取掃描）*

。 `vscan-fileop-profile` 的參數 `vserver cifs share create` 命令定義哪些 SMB 檔案作業會觸發病毒掃描。依預設、參數會設為 `standard`，這是 NetApp 最佳實務做法。您可以在建立或修改 SMB 共用時視需要調整此參數：

- `no-scan` 指定從不觸發共享區的病毒掃描。
- `standard` 指定透過開啟、關閉及重新命名作業觸發病毒掃描。
- `strict` 指定透過開啟、讀取、關閉及重新命名作業來觸發病毒掃描。

  。 `strict` 設定檔可針對多個用戶端同時存取檔案的情況、提供增強的安全性。如果某個用戶端在寫入病毒後關閉檔案、而同一個檔案仍會在第二個用戶端上開啟、 `strict` 確保第二個用戶端上的讀取作業會在檔案關閉之前觸發掃描。

  您應該小心限制 `strict`` 包含您預期會同時存取之檔案的共用設定檔。由於此設定檔會產生更多掃描要求、因此可能會影響效能。

- `writes-only` 指定只有在關閉修改過的檔案時才觸發病毒掃描。

  自 `writes-only` 產生較少的掃描要求、通常會改善效能。

如果您使用此設定檔、掃描器必須設定為刪除或隔離無法修復的受感染檔案、因此無法存取這些檔案。例如、如果用戶端在寫入病毒後關閉檔案、而且檔案未被修復、刪除或隔離、則任何用戶端都會存取該檔案 `without` 寫信給 IT 的人會受到感染。

如果用戶端應用程式執行重新命名作業、檔案會以新名稱關閉、不會掃描。如果此類作業在您的環境中造成安全性考量、您應該使用 `standard` 或 `strict` 設定檔。

VScan 合作夥伴解決方案

NetApp 與 Trelix 、 Symantec 、 Trend Micro 和 Sentinel One 合作、提供領先業界的反惡意軟體和防毒解決方案、以 ONTAP VScan 技術為基礎。這些解決方案可協助您掃描檔案中的惡意軟體、並修正任何受影響的檔案。

如下表所示、 Trellix 、 Symantec 和 Trend Micro 的互通性詳細資料會保留在 NetApp 互通性對照表上。您也可以在合作夥伴網站上找到 Trelix 和 Symantec 的互通性詳細資料。合作夥伴將在其網站上維護 Sentinel One 和其他新合作夥伴的互通性詳細資料。

合作夥伴	解決方案文件	互通性詳細資料
Trelix （原 McAfee ）	"Trellix 產品文件"	• "NetApp 互通性對照表工具" • "端點安全儲存保護支援平台（ trellix.com ）"
Symantec	"Symantec Protection Engine 9.0.0"	• "NetApp 互通性對照表工具" • "支援對照表：通過 Symantec Protection Engine （ SPE ）認證的合作夥伴裝置、適用於網路附加儲存（ NAS ） 9.x.x" • "通過 Symantec Protection Engine （ SPE ）認證的合作夥伴裝置網路附加儲存（ NAS ） 8.x 支援對照表（ broadcom.com ）"
Trend Micro	"Trend Micro ServerProtect for Storage 6.0 入門指南"	"NetApp 互通性對照表工具"
Sentinel One	• "SentinelOne 奇異性雲端資料安全性" • "SentinelOne 支援" 此連結需要使用者登入。您可以從 Sentinel One 要求存取。	深直覺

VScan伺服器安裝與組態

VScan伺服器安裝與組態

設定一或多個 VScan 伺服器、以確保系統上的檔案已掃描到病毒。請依照廠商提供的指示、在伺服器上安裝及設定防毒軟體。

請依照 NetApp 提供的 README 檔案中的指示來安裝及設定 ONTAP 防毒連接器。或者、請遵循上的指示 "安裝 ONTAP 防毒連接器頁面"。

對於災難恢復和 MetroCluster 組態、您必須為主要 / 本機和次要 / 合作夥伴 ONTAP 叢集分別設定和設定 VScan 伺服器。

防毒軟體需求

- 如需防毒軟體需求的相關資訊、請參閱廠商文件。

- 如需 VScan 支援的廠商、軟體及版本資訊、請參閱 "VScan 合作夥伴解決方案" 頁面。

防毒連接器需求**ONTAP**

- 您可以從 NetApp 支援網站 的 * 軟體下載 * 頁面下載 ONTAP 防毒連接器。 "NetApp下載：軟體"
- 如需 ONTAP 防毒連接器支援的 Windows 版本和互通性需求的相關資訊、請參閱 "VScan 合作夥伴解決方案"。

> 您可以為叢集中的不同VScan伺服器安裝不同版本的Windows伺服器。

- Windows伺服器上必須安裝.NET 3.0或更新版本。
- 必須在Windows伺服器上啟用SMB 2.0。

安裝 **ONTAP** 防毒連接器

在 VScan 伺服器上安裝 ONTAP 防毒連接器、以啟用執行 ONTAP 的系統與 VScan 伺服器之間的通訊。安裝 ONTAP 防毒連接器後、防毒軟體就能與一或多個儲存虛擬機器（ SVM ）通訊。

關於這項工作

- 請參閱 "VScan 合作夥伴解決方案" 頁面以取得有關支援的通訊協定、防毒廠商軟體版本、 ONTAP 版本、互通性需求和 Windows 伺服器的資訊。
- 必須安裝 .NET 4.5.1 或更新版本。
- ONTAP 防毒連接器可以在虛擬機器上執行。不過、為了獲得最佳效能、 NetApp 建議使用專用虛擬機器進行防毒掃描。
- 您必須在安裝及執行 ONTAP 防毒連接器的 Windows 伺服器上啟用 SMB 2.0 。

開始之前

- 從支援網站下載 ONTAP 防毒連接器設定檔、並將其儲存至硬碟上的目錄。
- 確認您符合安裝 ONTAP 防毒連接器的要求。
- 請確認您擁有安裝防毒 Connector 的系統管理員權限。

步驟

1. 執行適當的安裝檔案來啟動防毒連接器安裝精靈。
2. 選取 *Next* 。「目的地資料夾」對話方塊隨即開啟。
3. 選取 *Next* 將防毒 Connector 安裝到列出的資料夾、或選取 *Changle* 安裝到不同的資料夾。
4. ONTAP AV Connector Windows 服務認證對話方塊隨即開啟。
5. 輸入您的 Windows 服務認證、或選取 * 新增 * 以選取使用者。對於 ONTAP 系統、此使用者必須是有效的網域使用者、而且必須存在於 SVM 的掃描器集區組態中。
6. 選擇*下一步*。「準備安裝程式」對話方塊隨即開啟。
7. 選擇 * 安裝 * 開始安裝、或選擇 * 上一步 * 來變更設定。 狀態方塊隨即開啟並記錄安裝進度、接著顯示「 Installshield Wizard Completed 」（安裝精靈已完成）對話方塊。

8. 如果您要繼續設定 ONTAP 管理或資料生命、請選取「設定 ONTAP 生命期」核取方塊。 您必須至少設定一個 ONTAP 管理或資料 LIF 、才能使用此 VScan 伺服器。
9. 如果您要檢視安裝記錄、請選取顯示 * Windows Installer 記錄 * 核取方塊。
10. 選擇 * 完成 * 結束安裝並關閉 Installshield 精靈。 桌面上會儲存 **Configure ONTAP Lifs** 圖示、以設定 ONTAP 生命。
11. 將 SVM 新增至防毒 Connector 。 您可以新增 ONTAP 管理 LIF 來將 SVM 新增至防毒連接器、此 LIF 會輪詢以擷取資料生命清單、或直接設定資料 LIF 或生命。 如果已設定 ONTAP 管理 LIF 、您也必須提供意見調查資訊和 ONTAP 管理帳戶認證。
    - 確認已啟用 SVM 的管理 LIF 或 IP 位址 `management-https`。當您只是設定資料生命時、這不是必要的。
    - 確認您已為 HTTP 應用程式建立使用者帳戶、並指派（至少為唯讀）存取的角色 `/api/network/ip/interfaces` REST API ： 如需建立使用者的詳細資訊、請參閱 "建立安全登入角色" 和 "建立安全登入" ONTAP 手冊頁。

> 您也可以新增管理 SVM 的驗證通道 SVM 、將網域使用者當成帳戶使用。如需詳細資訊、請參閱 "建立安全登入網域通道" ONTAP 手冊頁或使用 `/api/security/acccounts` 和 `/api/security/roles` REST API 可設定管理帳戶和角色。

步驟

1. 在 * 設定 ONTAP Lifs* 圖示上按一下滑鼠右鍵、此圖示會在您完成防毒連接器安裝時儲存在桌面上、然後選取 * 以系統管理員身分執行 * 。
2. 在「設定 ONTAP 生命」對話方塊中、選取偏好的組態類型、然後執行下列動作：

若要建立此類型的 LIF…	執行下列步驟…
資料LIF	a. 將「角色」設為「資料」 b. 將「資料傳輸協定」設定為「 CIFS 」 c. 將「防火牆原則」設定為「資料」 d. 將「服務原則」設定為「 default-data-files 」
管理層 LIF	a. 將「 role * 」設為「 data 」 b. 將「資料傳輸協定」設為「無」 c. 將「防火牆原則」設定為「管理」 d. 將「服務原則」設定為「預設管理」

深入瞭解 "建立 LIF"。

建立 LIF 之後、請輸入您要新增之 SVM 的資料或管理 LIF 或 IP 位址。您也可以輸入叢集管理 LIF 。如果您指定叢集管理 LIF 、則該叢集中所有服務 SMB 的 SVM 都可以使用 VScan 伺服器。

當 VScan 伺服器需要 Kerberos 驗證時、每個 SVM 資料 LIF 都必須有唯一的 DNS 名稱、而且您必須在 Windows Active Directory 中將該名稱登錄為伺服器主要名稱（ SPN ）。當每個資料 LIF 無法使用唯一的 DNS 名稱或登錄為 SPN 時、 VScan 伺服器會使用 NT LAN Manager 機制進行驗證。如果您在連線 VScan 伺服器後新增或修改 DNS 名稱和 SPN 、則必須重新啟動 VScan 伺服器上的防毒連接器服務、才能套用變更。

3. 若要設定管理 LIF 、請以秒為單位輸入輪詢持續時間。輪詢持續時間是防毒 Connector 檢查 SVM 或叢集 LIF 組態變更的頻率。預設的輪詢時間間隔為 60 秒。
4. 輸入 ONTAP 管理帳戶名稱和密碼以設定管理 LIF 。
5. 按一下 * 測試 * 以檢查連線能力並驗證驗證。驗證僅適用於管理 LIF 組態。
6. 按一下 * 更新 * 將 LIF 新增至要輪詢或連線的生命清單。
7. 按一下 * 儲存 * 以儲存登錄的連線。
8. 如果您要將連線清單匯出至登錄匯入或登錄匯出檔案、請按一下 * 匯出 * 。如果多部 VScan 伺服器使用相同的管理或資料生命負載、這項功能就很實用。

請參閱 "設定 ONTAP 防毒連接器頁面" 以取得組態選項。

設定 **ONTAP** 防毒連接器

設定 ONTAP 防毒連接器、輸入 ONTAP 管理 LIF 、輪詢資訊、 ONTAP 管理帳戶認證、或只輸入資料 LIF 、以指定您要連線的一或多個儲存虛擬機器（ SVM ）。您也可以修改 SVM 連線的詳細資料、或移除 SVM 連線。根據預設、如果已設定 ONTAP 管理 LIF 、 ONTAP 防毒連接器會使用 REST API 來擷取資料生命體清單。

修改 **SVM** 連線的詳細資料

您可以修改 ONTAP 管理 LIF 和輪詢資訊、以更新已新增至防毒 Connector 的儲存虛擬機器（ SVM ）連線的詳細資料。新增資料生命後、您無法更新這些資料生命。若要更新資料生命期、您必須先移除資料生命期、然後再以新的 LIF 或 IP 位址重新新增資料生命期。

開始之前

確認您已為 HTTP 應用程式建立使用者帳戶、並指派（至少為唯讀）存取的角色 `/api/network/ip/interfaces` REST API ： 如需建立使用者的詳細資訊、請參閱 "建立安全登入角色" 和 "建立安全登入" 命令。 您也可以新增管理 SVM 的驗證通道 SVM 、將網域使用者當成帳戶使用。 如需詳細資訊、請參閱 "建立安全登入網域通道" ONTAP 手冊頁。

步驟

1. 在 * 設定 ONTAP Lifs* 圖示上按一下滑鼠右鍵、此圖示會在您完成防毒連接器安裝時儲存在桌面上、然後選取 * 以系統管理員身分執行 * 。此時將打開 Configure Lifs （配置 ONTAP 生命）對話框。
2. 選取 SVM IP 位址、然後按一下 * 更新 * 。
3. 視需要更新資訊。
4. 按一下 * 儲存 * 以更新登錄中的連線詳細資料。
5. 如果您要將連線清單匯出至登錄匯入或登錄匯出檔案、請按一下 * 匯出 * 。 如果多部 VScan 伺服器使用相同的管理或資料生命負載、這項功能就很實用。

從防毒 **Connector** 移除 **SVM** 連線

如果不再需要 SVM 連線、您可以將其移除。

步驟

1. 在 * 設定 ONTAP Lifs* 圖示上按一下滑鼠右鍵、此圖示會在您完成防毒連接器安裝時儲存在桌面上、然後選取 * 以系統管理員身分執行 * 。此時將打開 Configure Lifs （配置 ONTAP 生命）對話框。
2. 選取一或多個 SVM IP 位址、然後按一下 * 移除 * 。
3. 按一下 * 儲存 * 以更新登錄中的連線詳細資料。
4. 如果您要將連線清單匯出至登錄匯入或登錄匯出檔案、請按一下 * 匯出 * 。 如果多部 VScan 伺服器使用相同的管理或資料生命負載、這項功能就很實用。

疑難排解

開始之前

當您在此程序中建立登錄值時、請使用右側窗格。

您可以啟用或停用防毒連接器記錄以供診斷之用。根據預設、這些記錄會停用。為了提升效能、您應該停用防毒 Connector 記錄檔、並僅在發生重大事件時啟用記錄檔。

步驟

1. 選取 * 開始 * 、在搜尋方塊中輸入「 regedit" 、然後選取 `regedit.exe` 在「程式集」清單中。
2. 在 * 登錄編輯程式 * 中、找到 ONTAP 防毒連接器的下列子機碼： `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 提供下表所示的類型、名稱和值來建立登錄值：

類型	名稱	價值
字串	追蹤路徑	C ： \avshim.log

此登錄值可以是任何其他有效路徑。

4. 提供下表所示的類型、名稱、值及記錄資訊、以建立另一個登錄值：

類型	名稱	關鍵記錄	中繼記錄	詳細記錄
雙字節	Tracelight	1.	2 或 3	4.

這會啟用儲存在步驟 3 追蹤路徑中所提供路徑值的防毒 Connector 記錄檔。

5. 刪除您在步驟 3 和 4 中建立的登錄值、以停用防毒 Connector 記錄。
6. 使用「 LogRotation 」（記錄旋轉）名稱（不含引號）、建立另一個「 multy_SZ 」類型的登錄值。在「 LogRotation 」中、 提供 "logFileSize:1 " 做為旋轉大小的項目（其中 1 代表 1MB ）、在下一行提供 "logFileCount:5" 做為 進入旋轉限制（上限為 5 ）。

這些值是選用的。如果未提供、預設值 20MB 和 10 個檔案會分別用於旋轉大小和旋轉限制。提供的整數值不提供十進位或分數值。如果您提供的值高於預設值、則會改用預設值。

7. 若要停用使用者設定的記錄輪替功能、請刪除您在步驟 6 中建立的登錄值。

可自訂橫幅

自訂橫幅可讓您在 *Configure ONTAP LIF API* 視窗中放置具法律約束力的聲明和系統存取免責聲明。

步驟

1. 透過更新中的內容來修改預設橫幅 `banner.txt` 將檔案儲存在安裝目錄中、然後儲存變更。 您必須重新開啟 Configure LIF API （設定 ONTAP LIF API ）視窗、才能查看橫幅中反映的變更。

啟用延伸條例（ **EO** ）模式

您可以啟用和停用「延伸條例」（ EOO ）模式、以確保操作安全。

步驟

1. 選取 * 開始 * 、在搜尋方塊中輸入「 regedit" 、然後選取 `regedit.exe` 在「程式集」清單中。
2. 在 * 登錄編輯程式 * 中、找到下列 ONTAP 防毒連接器子機碼：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 在右側窗格中、建立名稱為「 EO_Mode 」（不含引號）且值為「 1 」（不含引號）的新登錄值（不含引號）、以啟用「 EO Mode 」（ EO 模式）或值「 0 」（不含引號）來停用「 EO Mode 」（ EO 模式）。

依預設、如果是 `EO_Mode` 登錄項目不存在、會停用 EO 模式。啟用「 EOO 」模式時、您必須同時設定外部 Syslog 伺服器和相互憑證驗證。

設定外部 **Syslog** 伺服器

開始之前

請注意、在本程序中建立登錄值時、請使用右側窗格。

步驟

1. 選取 * 開始 * 、在搜尋方塊中輸入「 regedit" 、然後選取 `regedit.exe` 在「程式集」清單中。
2. 在 * 登錄編輯程式 * 中、針對 ONTAP 防毒連接器的系統記錄組態建立下列子機碼：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. 請提供下表所示的類型、名稱和值來建立登錄值：

類型	名稱	價值
雙字節	啟用 SysLog	1 或 0

請注意、「 1 」值會啟用 Syslog 、而「 0 」值則會停用。

4. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱
Reg_SZ	syslog_host

提供系統記錄主機 IP 位址或網域名稱作為值欄位。

5. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱
Reg_SZ	syslog_port

在值欄位中提供 Syslog 伺服器執行的連接埠編號。

6. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱
Reg_SZ	syslog_protocol

在值欄位中輸入 Syslog 伺服器上使用的傳輸協定（「 TCP 」或「 UDP 」）。

7. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱	log_crt	log_notice	log_info	log_debug
雙字節	syslog_level	2.	5.	6.	7.

8. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱	價值
雙字節	syslog_tls	1 或 0

請注意、「 1 」值會啟用含傳輸層安全性（ TLS ）的 Syslog 、而「 0 」值則會停用含 TLS 的 Syslog 。

確保已設定的外部 **Syslog** 伺服器能順暢運作

- 如果金鑰不存在或具有 null 值：
  - 傳輸協定預設為「 TCP 」。
  - 對於純「 TCP/UDP 」、連接埠預設為「 514 」、而 TLS 預設為「 6514 」。
  - 系統記錄層級預設為 5 （ log_notice ）。
- 您可以驗證是否已啟用 Syslog `syslog_enabled` 值為「 1 」。當 `syslog_enabled` 值為「 1 」、無論是否啟用「 EO 」模式、您都應該能夠登入設定的遠端伺服器。

- 如果將 EO 模式設定為「 1 」、則您可以變更 `syslog_enabled` 值從「 1 」到「 0 」、適用下列條件：
  - 如果系統記錄未在 EO 模式中啟用、則無法啟動服務。
  - 如果系統以穩定狀態執行、系統會顯示一則警告訊息、表示無法在 EO 模式中停用 Syslog 、且系統記錄會強制設定為「 1 」、您可以在登錄中看到。如果發生這種情況、您應該先停用 EO 模式、然後停用 Syslog 。
- 如果在啟用 EO 模式和 Syslog 時、系統記錄伺服器無法成功執行、則服務會停止執行。這可能是因為下列其中一項原因所致：
  - 未設定無效或不設定任何 syslog_host 。
  - 設定的傳輸協定無效、除了 UDP 或 TCP 之外。
  - 連接埠號碼無效。
- 對於 TCP 或 TLS over TCP 組態、如果伺服器未接聽 IP 連接埠、則連線會失敗、且服務會關閉。

設定 **X.509** 相互憑證驗證

管理路徑中的防毒連接器和 ONTAP 之間的安全通訊端層 (SSL) 通訊可以使用基於 X.509 憑證的相互驗證。如果啟用了 EO 模式、但找不到憑證、 AV Connector 就會終止。在防毒連接器上執行下列程序：

步驟

1. 防毒連接器會在防毒連接器執行安裝目錄的目錄路徑中搜尋防毒連接器用戶端憑證和 NetApp 伺服器的憑證授權單位（ CA ）憑證。將憑證複製到此固定目錄路徑。
2. 以 PKCS12 格式內嵌用戶端憑證及其私密金鑰、並將其命名為「 AV_CLIent.p12 」。
3. 請確定用於簽署 NetApp 伺服器憑證的 CA 憑證（以及任何至根 CA 的中繼登錄授權單位）為「隱私權增強郵件」（ PEM ）格式、且名稱為「 onta_CA.pem 」。將其放在防毒 Connector 安裝目錄中。在 NetApp ONTAP 系統上、安裝 CA 憑證（以及任何至根 CA 的中繼簽署授權單位）、以「 ONTAP 」的防毒連接器用戶端憑證簽署為「 client-ca 」類型的憑證。

設定掃描器資源池

設定掃描器集區總覽

掃描器集區會定義VScan伺服器和可連線至SVM的授權使用者。掃描器原則會決定掃描器集區是否處於作用中狀態。

如果您在 SMB 伺服器上使用匯出原則、則必須將每個 VScan 伺服器新增至匯出原則。

在單一叢集上建立掃描器集區

掃描器集區會定義VScan伺服器和可連線至SVM的授權使用者。您可以為個別 SVM 或叢集中的所有 SVM 建立掃描器集區。

您需要的產品

- SVM和VScan伺服器必須位於同一個網域或信任的網域中。
- 針對為個別 SVM 定義的掃描器集區、您必須使用 SVM 管理 LIF 或 SVM 資料 LIF 來設定 ONTAP 防毒連接器。

- 針對叢集中所有 SVM 定義的掃描器集區、您必須使用叢集管理 LIF 來設定 ONTAP 防毒連接器。
- 授權使用者清單必須包含VScan伺服器用來連線至SVM的網域使用者帳戶。
- 設定掃描器集區後、請檢查伺服器的連線狀態。

步驟

1. 建立掃描器集區：

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 為個別SVM定義的資源池指定資料SVM、並為叢集中所有SVM定義的資源池指定叢集管理SVM。
   - 為每個VScan伺服器主機名稱指定IP位址或FQDN。
   - 指定每個授權使用者的網域和使用者名稱。 如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會建立名為的掃描器集區 `SP` 在上 `vs1` SVM ：

   ```
   cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
   SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
   cifs\u1,cifs\u2
   ```

2. 確認已建立掃描器集區：

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示的詳細資料 `SP` 掃描器集區：

   ```
   cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
   SP

                                    Vserver: vs1
                                Scanner Pool: SP
                              Applied Policy: idle
                              Current Status: off
           Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: vserver
         List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
   List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
   27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
   ```

   您也可以使用 `vserver vscan scanner-pool show` 命令以檢視 SVM 上的所有掃描器集區。如需完整

的命令語法、請參閱命令的手冊頁。

以**MetroCluster** 各種不完整的組態建立掃描器資源池

您必須在MetroCluster 每個叢集上建立一個適用於整個叢集的主和次掃描儀資源池、以對應於叢集上的主要和次要SVM。

您需要的產品

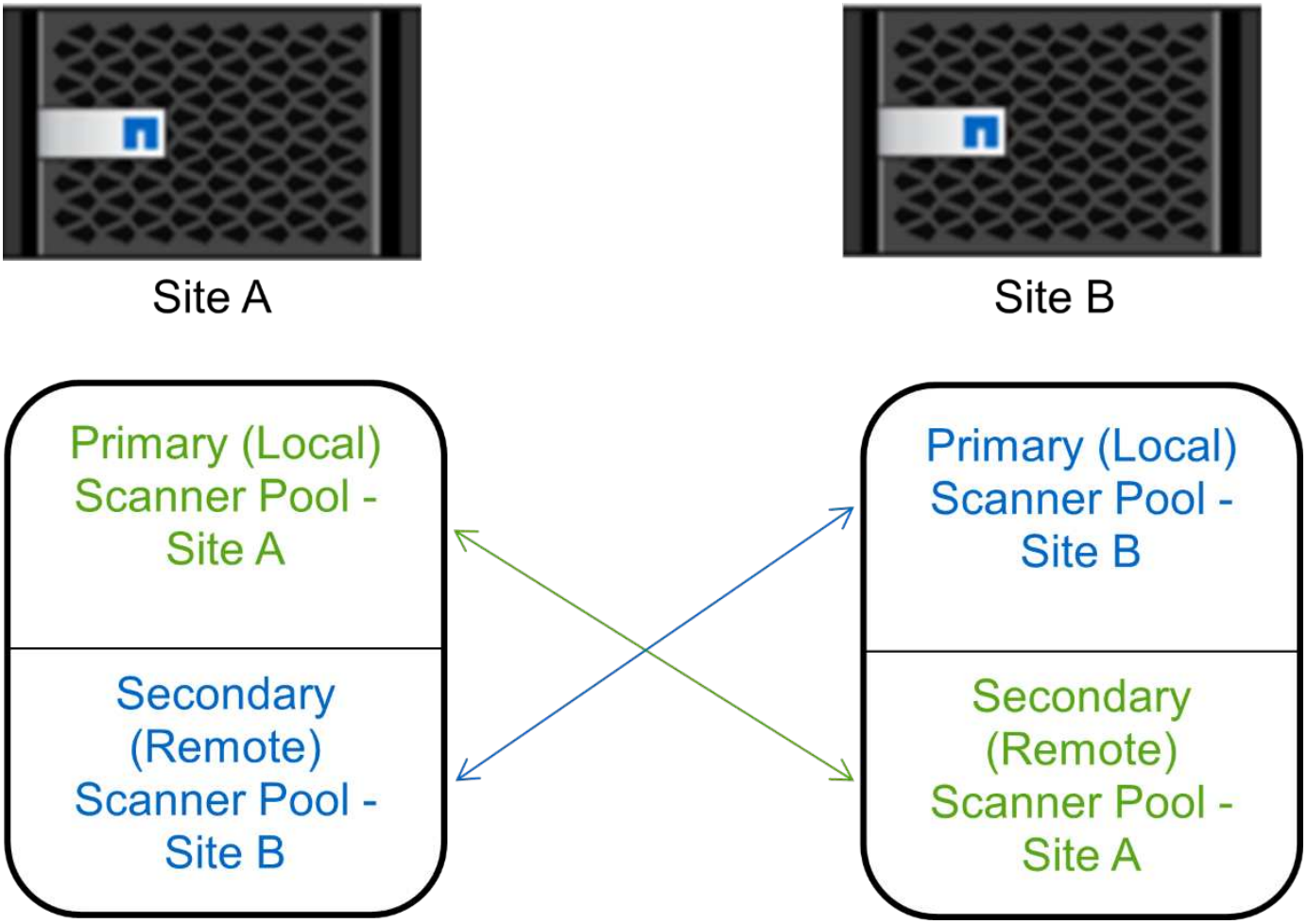
- SVM和VScan伺服器必須位於同一個網域或信任的網域中。
- 針對為個別 SVM 定義的掃描器集區、您必須使用 SVM 管理 LIF 或 SVM 資料 LIF 來設定 ONTAP 防毒連接器。
- 針對叢集中所有 SVM 定義的掃描器集區、您必須使用叢集管理 LIF 來設定 ONTAP 防毒連接器。
- 授權使用者清單必須包含VScan伺服器用來連線至SVM的網域使用者帳戶。
- 設定掃描器集區後、請檢查伺服器的連線狀態。

關於這項工作

透過實作兩個實體獨立的鏡射叢集、可利用各種組態來保護資料。MetroCluster每個叢集都會同步複寫另一個叢集的資料和SVM組態。當叢集上線時、本機叢集上的主要SVM會提供資料。當遠端叢集離線時、本機叢集上的次要SVM會提供資料。

這表示您必須在 MetroCluster 組態中的每個叢集上建立主要和次要掃描器集區、當叢集開始從次要 SVM 服務資料時、次要集區就會變成作用中。災難恢復（ DR ）的組態與 MetroCluster 類似。

此圖顯示典型的 MetroCluster / DR 組態。



步驟

1. 建立掃描器集區：

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 為個別SVM定義的資源池指定資料SVM、並為叢集中所有SVM定義的資源池指定叢集管理SVM。
   - 為每個VScan伺服器主機名稱指定IP位址或FQDN。
   - 指定每個授權使用者的網域和使用者名稱。

     您必須從包含主要SVM的叢集建立所有掃描器集區。

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會在MetroCluster 每個叢集上建立一個以功能為基礎的基本和次要掃描器集區：

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. 確認已建立掃描器集區：

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示掃描器集區的詳細資料 `pool1`：

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                               Scanner Pool: pool1_for_site1
                             Applied Policy: idle
                             Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

   您也可以使用 `vserver vscan scanner-pool show` 命令以檢視 SVM 上的所有掃描器集區。如需完整的命令語法、請參閱命令的手冊頁。

在單一叢集上套用掃描器原則

掃描器原則會決定掃描器集區是否處於作用中狀態。您必須先啟動掃瞄器集區、其定義的

VScan 伺服器才能連線至 SVM 。

關於這項工作

- 您只能將一個掃描器原則套用至掃描器集區。
- 如果您為叢集中的所有 SVM 建立了掃瞄器集區、則必須個別在每個 SVM 上套用掃瞄器原則。

步驟

1. 套用掃描器原則：

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   掃描器原則可以具有下列其中一個值：

   - `Primary` 指定掃描儀池處於活動狀態。
   - `Secondary` 指定只有在沒有連接主要掃描器集區中的 VScan 伺服器時、掃描器集區才為作用中。
   - `Idle` 指定掃描器集區為非作用中。

     以下範例顯示掃描器集區的名稱 `SP` 在上 `vs1` SVM 處於作用中狀態：

   ```
   cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
   -scanner-pool SP  -scanner-policy primary
   ```

2. 確認掃描器集區處於作用中狀態：

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示的詳細資料 `SP` 掃描器集區：

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                                Scanner Pool: SP
                              Applied Policy: primary
                              Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
```

您可以使用 `vserver vscan scanner-pool show-active` 用於查看 SVM 上活動掃描儀池的命令。如需完整的命令語法、請參閱命令的手冊頁。

將掃描器原則套用**MetroCluster** 至各種組態

掃描器原則會決定掃描器集區是否處於作用中狀態。您必須將掃描儀原則套用至MetroCluster 每個叢集上的主掃描儀資源池和次掃描儀資源池、以供選擇。

關於這項工作

- 您只能將一個掃描器原則套用至掃描器集區。
- 如果您為叢集中的所有 SVM 建立了掃瞄器集區、則必須個別在每個 SVM 上套用掃瞄器原則。
- 對於災難恢復和 MetroCluster 組態、您必須將掃描器原則套用至本機叢集和遠端叢集中的每個掃描器集區。
- 在您為本機叢集建立的原則中、您必須在中指定本機叢集 `cluster` 參數。在您為遠端叢集建立的原則中、您必須在中指定遠端叢集 `cluster` 參數。接著、遠端叢集便可在發生災難時接管病毒掃描作業。

步驟

1. 套用掃描器原則：

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   掃描器原則可以具有下列其中一個值：

   - `Primary` 指定掃描儀池處於活動狀態。
   - `Secondary` 指定只有在沒有連接主要掃描器集區中的 VScan 伺服器時、掃描器集區才為作用中。
   - `Idle` 指定掃描器集區為非作用中。

   > 您必須套用包含主要SVM之叢集的所有掃描器原則。

下列命令會將掃描儀原則套用至MetroCluster 每個叢集上的主掃描儀集區和次掃描儀集區、以供選擇：

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. 確認掃描器集區處於作用中狀態：

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示掃描器集區的詳細資料 `pool1`：

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: primary
                              Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   您可以使用 `vserver vscan scanner-pool show-active` 用於查看 SVM 上活動掃描儀池的命令。如需完整的命令語法、請參閱命令的手冊頁。

用於管理掃描器資源池的命令

您可以修改及刪除掃描器資源池、以及管理掃描器資源池的授權使用者和VScan伺服器。您也可以檢視掃描器集區的摘要資訊。

如果您想要...	輸入下列命令...
修改掃描器資源池	`vserver vscan scanner-pool modify`
刪除掃描器資源池	`vserver vscan scanner-pool delete`
新增授權使用者至掃描器集區	`vserver vscan scanner-pool privileged-users add`
從掃描器集區刪除具有權限的使用者	`vserver vscan scanner-pool privileged-users remove`
將VScan伺服器新增至掃描器集區	`vserver vscan scanner-pool servers add`
從掃描器集區刪除VScan伺服器	`vserver vscan scanner-pool servers remove`
檢視掃描器集區的摘要與詳細資料	`vserver vscan scanner-pool show`
檢視掃描器集區的授權使用者	`vserver vscan scanner-pool privileged-users show`
檢視所有掃描器集區的VScan伺服器	`vserver vscan scanner-pool servers show`

如需這些命令的詳細資訊、請參閱手冊頁。

設定存取時掃描

建立存取時原則

存取時原則定義存取時掃描的範圍。您可以為個別SVM或叢集中的所有SVM建立存取原則。如果您為叢集中的所有SVM建立了存取原則、則必須個別在每個SVM上啟用原則。

關於這項工作

- 您可以指定要掃描的檔案大小上限、掃描中要包含的檔案副檔名和路徑、以及要從掃描中排除的檔案副檔名和路徑。
- 您可以設定 `scan-mandatory` 選項為「關閉」、可指定在沒有 VScan 伺服器可供病毒掃描時、允許檔案存取。
- 根據預設、 ONTAP 會建立名為「 Default_CIFS 」的存取上原則、並為叢集中的所有 SVM 啟用該原則。
- 符合掃描排除條件的任何檔案、根據 `paths-to-exclude`、 `file-ext-to-exclude`或 `max-file-size` 即使是、也不會考慮掃描參數 `scan-mandatory` 選項設為「開啟」。（請勾選此項 "疑難排解" 有關連線問題的章節 `scan-mandatory` 選項。）
- 依預設、只會掃描讀寫磁碟區。您可以指定篩選條件、以允許掃描唯讀磁碟區、或限制掃描以執行存取開啟的檔案。

- 不會在 SMB 共用上執行病毒掃描、而持續可用的參數會設為是。
- 請參閱 "防毒架構" 節以取得關於 _VScan 檔案作業設定檔的詳細資料。
- 每個 SVM 最多可建立十（ 10 ）個存取原則。不過、您一次只能啟用一個存取原則。
  - 在存取原則中、您最多可以排除一百（ 100 ）個路徑和檔案副檔名、使其無法進行病毒掃描。
- 一些檔案排除建議：
  - 請考慮將大型檔案（可以指定檔案大小）排除在病毒掃描之外、因為這些檔案可能會導致 CIFS 使用者回應緩慢或掃描要求逾時。排除的預設檔案大小為 2GB 。
  - 請考慮排除檔案副檔名、例如 `.vhd` 和 `.tmp` 因為具有這些副檔名的檔案可能不適合掃描。
  - 請考慮排除檔案路徑、例如僅儲存虛擬硬碟或資料庫的隔離目錄或路徑。
  - 請確認所有排除項目都是在同一個原則中指定、因為一次只能啟用一個原則。NetApp 強烈建議您在防毒引擎中指定相同的排除項目集。
- 必須有存取上的原則才能使用 隨需掃描。為了避免進行存取掃描、您應該設定 `-scan-files-with-no-ext` 為假、且 `-file-ext-to-exclude` 至 * 以排除所有副檔名。

步驟

1. 建立存取時原則：

   ```
   vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
   -policy-name policy_name -protocol CIFS -max-file-size
   max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
   -file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
   extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
   -exclude paths_of_files_to_exclude -scan-mandatory on|off
   ```

   - 為個別SVM定義的原則指定資料SVM、為叢集中所有SVM定義的原則指定叢集管理SVM。
   - 。 `-file-ext-to-exclude` 設定會覆寫 `-file-ext-to-include` 設定：
   - 設定 `-scan-files-with-no-ext` 至 true 可掃描不含副檔名的檔案。 下列命令會建立名為的存取上原則 `Policy1` 在上 `vs1` SVM ：

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include “mp*”,"tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. 確認已建立存取原則： `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示的詳細資料 `Policy1` 原則：

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

啟用存取原則

存取時原則定義存取時掃描的範圍。您必須在SVM上啟用存取原則、才能掃描其檔案。

如果您為叢集中的所有SVM建立了存取原則、則必須個別在每個SVM上啟用原則。您一次只能在SVM上啟用一個存取原則。

步驟

1. 啟用存取原則：

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   下列命令會啟用名為的存取原則 `Policy1` 在上 `vs1` SVM ：

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. 確認已啟用存取原則：

   `vserver vscan on-access-policy show -instance *data_SVM* -policy-name *policy_name*`

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示的詳細資料 `Policy1` 存取原則：

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: on
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

修改SMB共用區的VScan檔案作業設定檔

SMB 共用的 _VScan 檔案作業設定檔 _ 會定義可觸發掃描的共用作業。依預設、參數會設為 `standard`。您可以在建立或修改SMB共用時、視需要調整參數。

請參閱 "防毒架構" 節以取得關於 _VScan 檔案作業設定檔的詳細資料。

> 在具有的 SMB 共用上不會執行病毒掃描 `continuously-available` 參數設為 `Yes`。

步驟

1. 修改 SMB 共用的 VScan 檔案作業設定檔值：

   ```
   vserver cifs share modify -vserver data_SVM -share-name share -path share_path
   -vscan-fileop-profile no-scan|standard|strict|writes-only
   ```

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會將 SMB 共用的 VScan 檔案作業設定檔變更為 `strict`：

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

用於管理存取原則的命令

您可以修改、停用或刪除存取時原則。您可以檢視原則的摘要和詳細資料。

如果您想要…	輸入下列命令…

建立存取時原則	`vserver vscan on-access-policy create`
修改存取時原則	`vserver vscan on-access-policy modify`
啟用存取原則	`vserver vscan on-access-policy enable`
停用存取原則	`vserver vscan on-access-policy disable`
刪除存取時原則	`vserver vscan on-access-policy delete`
檢視存取原則的摘要和詳細資料	`vserver vscan on-access-policy show`
新增至要排除的路徑清單	`vserver vscan on-access-policy paths-to-exclude add`
從要排除的路徑清單中刪除	`vserver vscan on-access-policy paths-to-exclude remove`
檢視要排除的路徑清單	`vserver vscan on-access-policy paths-to-exclude show`
新增至要排除的副檔名清單	`vserver vscan on-access-policy file-ext-to-exclude add`
從要排除的副檔名清單中刪除	`vserver vscan on-access-policy file-ext-to-exclude remove`
檢視要排除的副檔名清單	`vserver vscan on-access-policy file-ext-to-exclude show`
新增至要包含的副檔名清單	`vserver vscan on-access-policy file-ext-to-include add`
從要包含的副檔名清單中刪除	`vserver vscan on-access-policy file-ext-to-include remove`
檢視要包含的副檔名清單	`vserver vscan on-access-policy file-ext-to-include show`

如需這些命令的詳細資訊、請參閱手冊頁。

設定隨需掃描

設定隨需掃描總覽

您可以使用隨需掃描功能、立即或排程檢查檔案是否有病毒。

例如、您可能只想在非尖峰時間執行掃描、或者您可能想要掃描在存取時掃描中排除的超大型檔案。您可以使用 cron 排程來指定工作執行時間。

關於本主題

- 您可以在建立工作時指派排程。
- 在SVM上一次只能排程一項工作。
- 隨需掃描不支援掃描符號連結或串流檔案。

隨需掃描不支援掃描符號連結或串流檔案。

若要建立隨選工作、必須至少啟用一個存取原則。它可以是預設原則、也可以是使用者建立的存取原則。

建立隨需工作

隨選工作會定義隨選病毒掃描的範圍。您可以指定要掃描的檔案大小上限、要包含在掃描中的檔案副檔名和路徑、以及要從掃描中排除的檔案副檔名和路徑。依預設會掃描子目錄中的檔案。

關於這項工作

- 每個 SVM 最多可有十（ 10 ）個隨選工作、但只有一個可以使用中。
- 隨選工作會建立報告、其中包含與掃描相關的統計資料資訊。您可以使用命令或下載工作在定義位置所建立的報告檔案、來存取此報告。

開始之前

- 您必須擁有 已建立存取原則。原則可以是預設原則或使用者建立的原則。如果沒有存取原則、就無法啟用掃描。

步驟

1. 建立隨需工作：

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
-no-ext true|false -directory-recursion true|false
```

   - 。 `-file-ext-to-exclude` 設定會覆寫 `-file-ext-to-include` 設定：
   - 設定 `-scan-files-with-no-ext` 至 true 可掃描不含副檔名的檔案。

   如需完整的選項清單、請參閱 "命令參考資料"。

下列命令會建立名為的隨選工作 `Task1` 在「 VS1 ' shVM ：

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

您可以使用 `job show` 檢視工作狀態的命令。您可以使用 `job pause` 和 `job resume` 暫停及重新啟動工作的命令、或 `job stop` 命令以結束工作。

2. 確認已建立隨選工作：

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示的詳細資料 `Task1` 工作：

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

完成後

您必須先在SVM上啟用掃描、工作才會排程執行。

排程隨需工作

您可以建立工作、而無需指派排程和使用 `vserver vscan on-demand-task schedule` 命令來指派排程、或在建立工作時新增排程。

關於這項工作

指派給的排程 `vserver vscan on-demand-task schedule` 命令會覆寫已指派給的排程 `vserver vscan on-demand-task create` 命令。

步驟

1. 排程隨需工作：

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   下列命令會排程名為的存取上工作 `Task2` 在上 `vs2` SVM ：

   ```
   cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
   -name Task2 -schedule daily
   [Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
   command to view the status.
   ```

   若要檢視工作狀態、請使用 `job show` 命令。。 `job pause` 和 `job resume` 命令、分別暫停和重新啟動工作； `job stop` 命令會終止工作。

2. 確認隨選工作已排程：

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示的詳細資料 `Task 2` 工作：

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
```

完成後

您必須先在SVM上啟用掃描、工作才會排程執行。

立即執行隨需工作

無論您是否已指派排程、您都可以立即執行隨需工作。

開始之前

您必須已在SVM上啟用掃描。

步驟

1. 立即執行隨需工作：

   `vserver vscan on-demand-task run -vserver` *`data_SVM`* `-task-name` *`task_name`*

   下列命令會執行名為的存取上工作 `Task1` 在上 `vs1` SVM ：

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

> 您可以使用 `job show` 檢視工作狀態的命令。您可以使用 `job pause` 和 `job resume` 暫停及重新啟動工作的命令、或 `job stop` 命令以結束工作。

管理隨需工作的命令

您可以修改、刪除或取消排程隨需工作。您可以檢視工作的摘要和詳細資料、以及管理工作的報告。

如果您想要…	輸入下列命令…
建立隨需工作	`vserver vscan on-demand-task create`
修改隨需工作	`vserver vscan on-demand-task modify`
刪除隨需工作	`vserver vscan on-demand-task delete`
執行隨選工作	`vserver vscan on-demand-task run`
排程隨需工作	`vserver vscan on-demand-task schedule`
取消排程隨需工作	`vserver vscan on-demand-task unschedule`
檢視隨需工作的摘要和詳細資料	`vserver vscan on-demand-task show`
檢視隨需報告	`vserver vscan on-demand-task report show`
刪除隨需報告	`vserver vscan on-demand-task report delete`

如需這些命令的詳細資訊、請參閱手冊頁。

在 ONTAP 中設定隨裝即用防毒功能的最佳實務做法

請考量下列在 ONTAP 中設定隨裝即用功能的建議。

- 限制授權使用者執行掃毒作業。一般使用者不應使用授權使用者認證。若要達到此限制、請在 Active Directory 上關閉授權使用者的登入權限。
- 權限使用者不一定要是網域中擁有大量權限的任何使用者群組成員、例如系統管理員群組或備份操作員群組。授權使用者必須僅由儲存系統驗證、才能建立 VScan 伺服器連線並存取檔案進行病毒掃描。
- 請僅將執行 VScan 伺服器的電腦用於病毒掃描。若要阻止一般使用、請停用這些機器上的 Windows 終端機服務和其他遠端存取條款、並授予僅在這些機器上安裝新軟體的權限給系統管理員。
- 將 VScan 伺服器專用於病毒掃描、而不要將其用於其他作業、例如備份。您可以決定將 VScan 伺服器當作虛擬機器（ VM ）來執行。如果您將 VScan 伺服器當作 VM 執行、請確定分配給 VM 的資源並未共用、而且足以執行病毒掃描。
- 為 VScan 伺服器提供足夠的 CPU 、記憶體和磁碟容量、以避免資源過度分配。大多數 VScan 伺服器都是專為使用多個 CPU 核心伺服器而設計、並可在 CPU 之間分配負載。

- NetApp 建議使用專用網路搭配私有 VLAN 、以便從 SVM 連線至 VScan 伺服器、使掃描流量不會受到其他用戶端網路流量的影響。建立獨立的網路介面卡（ NIC ）、專用於 VScan 伺服器上的防毒 VLAN 、以及 SVM 上的資料 LIF 。如果發生網路問題、此步驟可簡化管理和疑難排解。防毒流量應使用私有網路隔離。防毒伺服器應設定為以下列其中一種方式與網域控制站（ DC ）和 ONTAP 通訊：
  - DC 應透過用於隔離流量的私有網路與防毒伺服器通訊。
  - DC 和防毒伺服器應透過不同的網路（而非先前提到的私有網路）進行通訊、這與 CIFS 用戶端網路不同。
  - 若要啟用 Kerberos 驗證以進行防毒通訊、請在 DC 上建立私人生命體的 DNS 項目、並在 DC 上建立對應於為私有 LIF 建立的 DNS 項目的服務主體名稱。將 LIF 新增至防毒連接器時、請使用此名稱。DNS 應能為每個連線至防毒 Connector 的私有 LIF 傳回唯一名稱。

如果 VScan 流量的 LIF 設定在與用戶端流量的 LIF 不同的連接埠上、則 VScan LIF 可能會在連接埠故障時容錯移轉至另一個節點。此變更會使 VScan 伺服器無法從新節點存取、且在節點上執行檔案作業的掃描通知失敗。驗證 VScan 伺服器是否可透過節點上至少一個 LIF 來存取、以便處理掃描要求、以便在該節點上執行檔案作業。

- 使用至少 1GbE 網路連接 NetApp 儲存系統和 VScan 伺服器。
- 對於具有多個 VScan 伺服器的環境、請連接所有具有類似高效能網路連線的伺服器。連接 VScan 伺服器可允許負載共用、進而改善效能。
- 對於遠端站台和分公司、 NetApp 建議使用本機 VScan 伺服器、而非遠端 VScan 伺服器、因為前者是高延遲的最佳選擇。如果成本是因素、請使用筆記型電腦或電腦來提供適度的防毒保護。您可以透過共用磁碟區或 qtree 、並從遠端站台的任何系統掃描、來排程定期完成的檔案系統掃描。
- 使用多部 VScan 伺服器來掃描 SVM 上的資料、以達到負載平衡和備援目的。CIFS 工作負載量和產生的防毒流量會因 SVM 而異。監控儲存控制器上的 CIFS 和病毒掃描延遲。持續監控結果趨勢。如果由於 VScan 伺服器上的 CPU 或應用程式佇列超過趨勢臨界值而導致 CIFS 延遲和病毒掃描延遲增加、則 CIFS 用戶端可能會經歷長時間的等待。新增其他 VScan 伺服器 以分散負載。
- 安裝最新版本的 ONTAP 防毒連接器。
- 將防毒引擎和定義保持在最新狀態。請諮詢合作夥伴、瞭解您應該多久更新一次的建議。
- 在多租戶環境中、只要 VScan 伺服器和 SVM 屬於同一個網域或信任的網域、即可與多個 SVM 共用掃描程式集區（ VScan 伺服器集區）。
- 受感染檔案的防毒軟體原則應設為「刪除」或「隔離」、這是大多數防毒廠商設定的預設值。如果「 vscan 檔案 op-profile 」設定為「 write_only 」、而且發現受感染的檔案、檔案會保留在共用區中、而且可以開啟、因為開啟檔案不會觸發掃描。防毒掃描只會在檔案關閉後觸發。
- 。 `scan-engine timeout` 值應小於 `scanner-pool request-timeout` 價值。 如果設定為較高的值、可能會延遲存取檔案、最終可能會逾時。 若要避免這種情況、請設定 `scan-engine timeout` 少於 5 秒 `scanner-pool request-timeout` 價值。請參閱掃描引擎廠商的文件、以取得如何變更的指示 `scan-engine timeout` 設定：。 `scanner-pool timeout` 您可以在進階模式中使用下列命令、並提供適當的值來變更 `request-timeout` 參數： `vserver vscan scanner-pool modify`。
- 對於規模適合存取掃描工作負載、且需要使用隨選掃描的環境、 NetApp 建議將隨選掃描工作排程在非尖峰時間、以避免現有防毒基礎架構增加負載。

如需更多關於合作夥伴的最佳實務做法、請參閱 "VScan 合作夥伴解決方案"。

在SVM上啟用掃毒

您必須在SVM上啟用掃毒、才能執行隨需存取或隨需掃描。

步驟

1. 在SVM上啟用掃毒：

   ```
   vserver vscan enable -vserver data_SVM
   ```

   您可以使用 `vserver vscan disable` 必要時停用病毒掃描的命令。

   下列命令可在上啟用病毒掃描 `vs1` SVM ：

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. 確認SVM上已啟用掃毒：

   ```
   vserver vscan show -vserver data_SVM
   ```

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示的 VScan 狀態 `vs1` SVM ：

   ```
   cluster1::> vserver vscan show -vserver vs1

                              Vserver: vs1
                        Vscan Status: on
   ```

重設掃描檔案的狀態

有時候、您可能會想要使用重設 SVM 上已成功掃描檔案的掃描狀態 `vserver vscan reset` 命令以捨棄檔案的快取資訊。例如、您可能想要使用此命令、在錯誤設定的掃描時重新啟動掃毒掃描處理。

關於這項工作

執行之後 `vserver vscan reset` 命令、所有符合資格的檔案都會在下次存取時掃描。

視要重新掃描的檔案數量和大小而定、此命令可能會對效能造成不良影響。

開始之前

此工作需要進階權限。

步驟

1. 變更為進階權限層級：

   `set -privilege advanced`

2. 重設掃描檔案的狀態：

   `vserver vscan reset -vserver data_SVM`

   下列命令會重設上掃描檔案的狀態 `vs1` SVM ：

   ```
   cluster1::> vserver vscan reset -vserver vs1
   ```

檢視VScan事件記錄資訊

您可以使用 `vserver vscan show-events` 命令可檢視受感染檔案、 VScan 伺服器更新等相關事件記錄資訊。您可以檢視叢集或特定節點、SVM或VScan伺服器的事件資訊。

開始之前

檢視 VScan 事件記錄需要進階權限。

步驟

1. 變更為進階權限層級：

   `set -privilege advanced`

2. 檢視VScan事件記錄資訊：

   `vserver vscan show-events`

   如需選項的完整清單、請參閱命令的手冊頁。

   下列命令會顯示叢集的事件記錄資訊 `cluster1`：

   ```
   cluster1::*> vserver vscan show-events

   Vserver     Node            Server          Event Type         Event Time
   ----------- --------------- --------------- -----------------
   -----------------
   vs1         Cluster-01      192.168.1.1     file-infected      9/5/2014
   11:37:38
   vs1         Cluster-01      192.168.1.1     scanner-updated    9/5/2014
   11:37:08
   vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
   11:34:55
   3 entries were displayed.
   ```

監控並疑難排解連線問題

可能涉及掃描強制選項的連線問題

您可以使用 `vserver vscan connection-status show` 檢視 VScan 伺服器連線相關資訊的命令、可能有助於疑難排解連線問題。

依預設 `scan-mandatory` 當無法掃描 VScan 伺服器連線時、存取掃描選項會拒絕檔案存取。雖然此選項提供重要的安全功能、但在少數情況下可能會導致問題。

- 在啟用用戶端存取之前、您必須確保至少有一部VScan伺服器連線至每個具有LIF的節點上的SVM。如果您需要在啟用用戶端存取後、將伺服器連線至 SVM 、則必須關閉 `scan-mandatory` SVM 上的選項、可確保檔案存取不會因無法使用 VScan 伺服器連線而遭到拒絕。您可以在伺服器連線後重新開啟選項。
- 如果目標LIF主控SVM的所有VScan伺服器連線、則移轉LIF時、伺服器與SVM之間的連線將會中斷。為了確保檔案存取不會因為無法使用 VScan 伺服器連線而遭到拒絕、您必須關閉 `scan-mandatory` 移轉 LIF 之前的選項。您可以在LIF移轉後重新開啟選項。

每個SVM應至少指派兩部VScan伺服器給它。最佳實務做法是透過不同網路、將VScan伺服器連接至儲存系統、而不使用用於用戶端存取的網路。

檢視**VScan**伺服器連線狀態的命令

您可以使用 `vserver vscan connection-status show` 用於檢視 VScan 伺服器連線狀態摘要和詳細資訊的命令。

如果您想要...	輸入下列命令...
檢視VScan伺服器連線的摘要	`vserver vscan connection-status show`
檢視VScan伺服器連線的詳細資料	`vserver vscan connection-status show-all`
檢視連線VScan伺服器的詳細資料	`vserver vscan connection-status show-connected`
檢視未連線之可用VScan伺服器的詳細資料	`vserver vscan connection-status show-not-connected`

如需這些命令的詳細資訊、請參閱 "介紹手冊頁ONTAP"。

疑難排解病毒掃描

對於常見的病毒掃描問題、有可能的原因和解決方法。病毒掃描也稱為 VScan 。

問題	如何解決此問題

VScan 伺服器無法連線至 叢集式 ONTAP 儲存系統。	檢查掃描器集區組態是否指定 VScan 伺服器 IP 位址。也請檢查掃描器集區清單中允許的權限使用者是否為作用中。若要檢查掃描器集區、請執行 `vserver vscan scanner-pool show` 儲存系統命令提示字元上的命令。如果 VScan 伺服器仍無法連線、則網路可能有問題。
用戶端觀察到高延遲。	現在可能是時候將更多 VScan 伺服器新增到掃描器集區了。
觸發的掃描過多。	修改的值 `vscan-fileop-profile` 限制監控進行病毒掃描的檔案作業數的參數。
部分檔案未被掃描。	檢查存取原則。這些檔案的路徑可能已新增至路徑排除清單、或其大小超過設定的排除值。若要檢查存取原則、請執行 `vserver vscan on-access-policy show` 儲存系統命令提示字元上的命令。
檔案存取遭拒。	檢查原則組態中是否指定了 _scan 強制設定。如果沒有連接 VScan 伺服器、此設定會拒絕資料存取。視需要修改設定。

監控狀態和效能活動

您可以監控 VScan 模組的關鍵層面、例如 VScan 伺服器連線狀態、 VScan 伺服器的健全狀況、以及已掃描的檔案數量。此資訊有助於您達成目標 您可以診斷與 VScan 伺服器相關的問題。

檢視 **VScan** 伺服器連線資訊

您可以檢視 VScan 伺服器的連線狀態、以管理已在使用中的連線 以及可供使用的連線。各種命令會顯示資訊 關於 VScan 伺服器的連線狀態。

命令 …	顯示的資訊 …
`vserver vscan connection-status show`	連線狀態摘要
`vserver vscan connection-status show-all`	連線狀態的詳細資訊
`vserver vscan connection-status show-not-connected`	可用但未連線的連線狀態
`vserver vscan connection-status show-connected`	有關連線 VScan 伺服器的資訊

如需這些命令的詳細資訊、請參閱 "指令參考資料ONTAP"。

檢視 **VScan** 伺服器統計資料

您可以檢視 VScan 伺服器專屬的統計資料、以監控效能並診斷相關問題 病毒掃描：您必須先收集資料範例、才能使用 `statistics show` 命令至 顯示 VScan 伺服器統計資料。 若要完成資料範例、請完成下列步驟：

步驟

1. 執行 `statistics start` 命令和 `optional statistics` 停止命令。

檢視 **VScan** 伺服器要求和延遲的統計資料

您可以使用 ONTAP `offbox_vscan` 以每個 SVM 為基礎的計數器來監控 VScan 的速率 每秒發送和接收的伺服器要求、以及所有 VScan 的伺服器延遲 伺服器。若要檢視這些統計資料、請完成下列步驟：

步驟

1. 執行統計資料顯示 `object offbox_vscan –instance SVM` 命令 下列計數器：

計數器 ...	顯示的資訊 ...
`scan_request_dispatched_rate`	每秒從 ONTAP 傳送至 VScan 伺服器的掃毒要求數
`scan_noti_received_rate`	ONTAP 每秒從 VScan 伺服器收到的掃毒要求數
`dispatch_latency`	ONTAP 內的延遲、可識別可用的 VScan 伺服器、並將要求傳送至該 VScan 伺服器
`scan_latency`	從 ONTAP 到 VScan 伺服器的往返延遲、包括掃描的執行時間

從 **ONTAP offbox vscan** 計數器產生的統計資料範例

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

檢視個別 **VScan** 伺服器要求和延遲的統計資料

您可以使用 ONTAP `offbox_vscan_server` 每個 SVM 上的計數器、每個隨裝即用 VScan 伺服器、 以每個節點為基礎、監控已派遣 VScan 伺服器要求的速度和上的伺服器延遲 每個 VScan 伺服器。若要收集此資訊、請完成下列步驟：

步驟

1. 執行 `statistics show -object offbox_vscan -instance SVM:servername:nodename` 具有下列計數器的命令：

計數器 ...	顯示的資訊 ...
`scan_request_dispatched_rate`	從 ONTAP 傳送的掃毒要求數
`scan_latency`	從 ONTAP 到 VScan 伺服器的往返延遲、包括掃描的執行時間 每秒至 VScan 伺服器

從 **ONTAP offbox_vscan** 伺服器計數器產生的統計資料範例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-------------------------------------------------------------------
```

檢視 **VScan** 伺服器使用率的統計資料

您也可以使用 ONTAP `offbox_vscan_server` 收集 VScan 伺服器端使用率的計數器 統計資料。這些統計資料會以每個 SVM 、每個隨裝即用 VScan 伺服器和每個節點為基礎進行追蹤。他們 包括 VScan 伺服器上的 CPU 使用率、 VScan 伺服器上掃描作業的佇列深度 （目前和最大）、已用記憶體和已用網路。 防毒連接器會將這些統計資料轉送到 ONTAP 中的統計資料計數器。他們 以每 20 秒輪詢一次的資料為基礎、必須收集多次以確保準確度； 否則、統計資料中所顯示的值只會反映上次輪詢。CPU 使用率和佇列為 監控與分析尤其重要。平均佇列的高值可能表示 VScan 伺服器有瓶頸。 收集每個 SVM 、每個隨裝即用 VScan 伺服器和每個節點上的 VScan 伺服器使用率統計資料 請完成下列步驟：

步驟

1. 收集 VScan 伺服器的使用率統計資料

   執行 `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` 命令 `offbox_vscan_server` 計數器：

計數器 ...	顯示的資訊 ...
scanner_stats_pct_cpu_used	VScan 伺服器上的 CPU 使用率
scanner_stats_pct_input_queue_avg	VScan 伺服器上掃描要求的平均佇列
scanner_stats_pct_input_queue_hiwatermark	VScan 伺服器上掃描要求的尖峰佇列
scanner_stats_pct_mem_used	VScan 伺服器上使用的記憶體
scanner_stats_pct_network_used	在 VScan 伺服器上使用的網路

VScan 伺服器的使用率統計資料範例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
-------------------------------------------------------------------
```