關於NetApp防毒保護

ONTAP 9

NetApp
February 12, 2026

目錄

關於NetApp防毒保護

了解 NetApp 使用 ONTAP Vscan 進行病毒掃描

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。

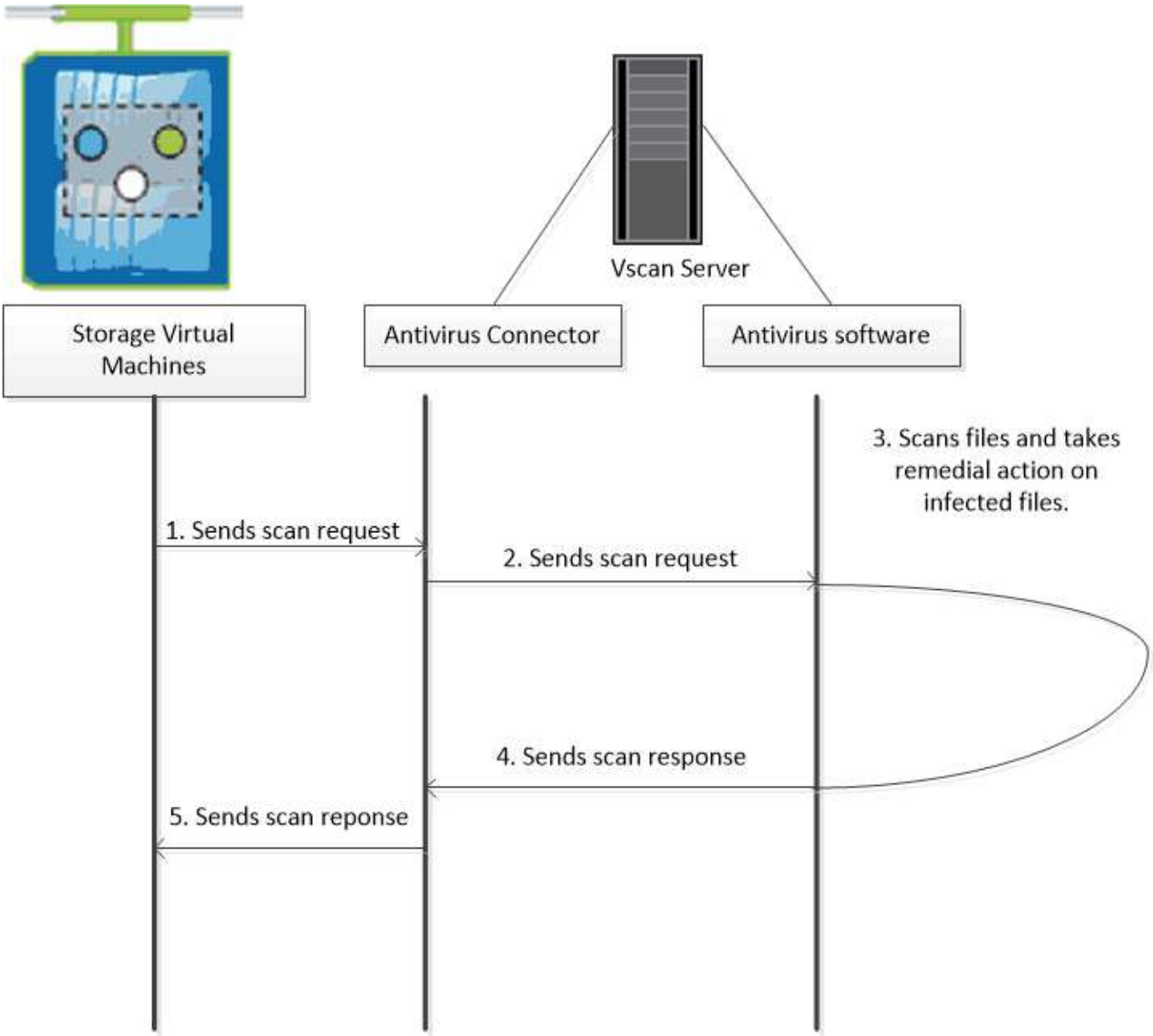
  NFS不支援存取時掃描。

- 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。

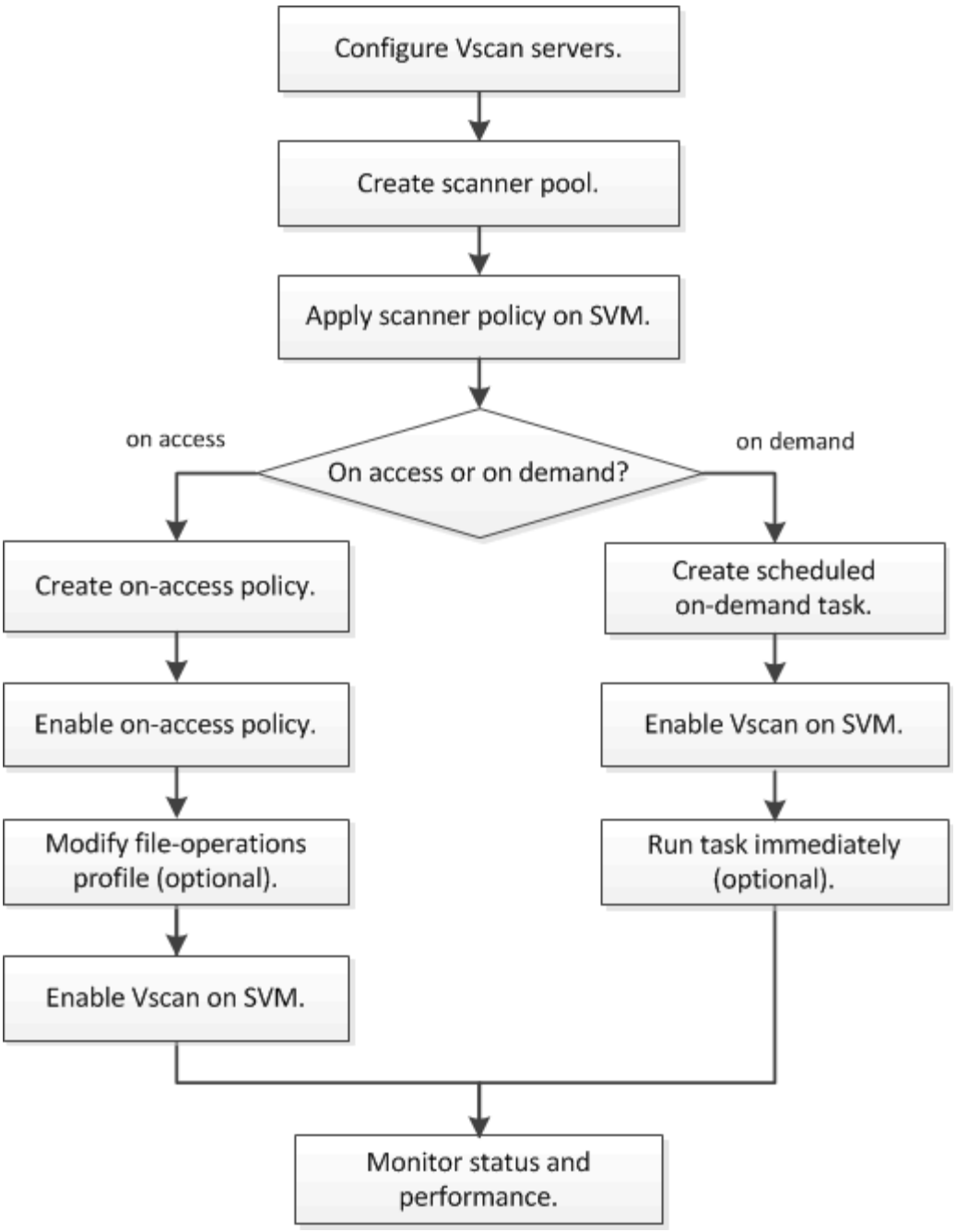
由NetApp提供並安裝在外部伺服器上的《The停止防毒連接器：處理儲存系統與防毒軟體之間的通訊。ONTAP



使用 ONTAP Vscan 進行病毒掃描工作流程

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。



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。

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

採用 ONTAP Vscan 的防毒架構

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`命令立即執行工作。如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task run`資訊，請參閱。

- * 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。

    您應該小心將 `strict`設定檔限制為包含預期將同時存取的檔案的共用。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。

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

了解 ONTAP Vscan 合作夥伴解決方案

NetApp 與 Trelix ， Symantec ， Trend Micro ， Sentinel One ， Deep Instinct 及 OPSWAT 合作，提供以 ONTAP VScan 技術為基礎的領先業界的惡意軟體防護與防毒解決方案。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 ， Symantec ， Deep Instinct 和 OPSWAT 的互通性詳細資料。合作夥伴將在其網站上維護 Sentinel One ， Deep Instinct ， OPSWAT 及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"
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。	不適用
深直覺	適用於 NAS 的深度直覺 DSX • "文件與互通性" 此連結需要使用者登入。您可以從深切本能要求存取。 • "資料表"	不適用

合作夥伴	解決方案文件	互通性詳細資料
OPSWAT	OPSWAT MetaDefender 儲存安全性 • "MetaDefender 儲存安全性與 NetApp 整合" • "OPSWAT 合作夥伴頁面" • "整合解決方案簡介"	不適用