VScan伺服器安裝與組態

ONTAP 9

NetApp
April 24, 2024

目錄

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。