安全性
ONTAP 9

NetApp
January 08, 2026

目錄

安全性

用戶端驗證與授權

使用標準方法來保護用戶端和系統管理員存取儲存設備的安全、並防止病毒入侵。ONTAP先進的技術可用於加密閒置資料和WORM儲存設備。

利用信任的來源驗證用戶端機器和使用者的身分、藉此驗證其身分。ONTAP利用比較使用者的認證資料與檔案或目錄上設定的權限、即可授權使用者存取檔案或目錄。ONTAP

驗證

您可以建立本機或遠端使用者帳戶：

- 本機帳戶是指帳戶資訊位於儲存系統上的帳戶。
- 遠端帳戶是指帳戶資訊儲存在Active Directory網域控制器、LDAP伺服器或NIS伺服器上的帳戶。

使用本機或外部名稱服務來查詢主機名稱、使用者、群組、netgroup和名稱對應資訊。ONTAP支援下列名稱服務：ONTAP

- 本機使用者
- DNS
- 外部NIS網域
- 外部 LDAP 網域

名稱服務交換器表_指定搜尋網路資訊的來源、以及搜尋這些資訊的順序（提供UNIX系統上/etc/nsswitch.conf檔案的等效功能）。當NAS用戶端連線至SVM時ONTAP 、此功能會檢查指定的名稱服務、以取得所需的資訊。

- Kerberos support_* Kerberos是一種網路驗證傳輸協定、可在用戶端伺服器實作中加密使用者密碼、以提供「長驗證」。支援Kerberos 5驗證、具備完整性檢查（krb5i）和Kerberos 5驗證功能、可進行隱私權檢查（krb5p）ONTAP 。

授權

此功能可評估三種安全層級、以判斷實體是否有權針對位於SVM上的檔案和目錄執行要求的動作。ONTAP存取權取決於評估安全性層級後的有效權限：

- 匯出（NFS）和共用（SMB）安全性

  匯出及共用安全性適用於用戶端存取特定NFS匯出或SMB共用區。具有管理權限的使用者可以從SMB和NFS用戶端管理匯出和共用層級的安全性。

- 儲存層級的存取保護檔案和目錄安全性

  儲存層級的存取保護安全性適用於存取SVM磁碟區的SMB和NFS用戶端。僅支援NTFS存取權限。為了對UNIX使用者執行安全性檢查、以存取已套用Storage Level Access Guard的磁碟區上的資料、UNIX使用者必須對應至擁有該磁碟區的SVM上的Windows使用者。ONTAP

- NTFS、UNIX及NFSv4原生檔案層級安全性

  代表儲存物件的檔案或目錄中存在原生檔案層級安全性。您可以從用戶端設定檔案層級的安全性。無論使用SMB或NFS存取資料、檔案權限都有效。

使用 **SAML** 驗證

ONTAP 支援安全性聲明標記語言（ SAML ）、以驗證遠端使用者。支援數個常見的身分識別供應商（ IDP ）。如需支援的 IDP 及啟用 SAML 驗證指示的詳細資訊、請參閱 "設定SAML驗證"。

OAuth 2.0 搭配 **ONTAP REST API** 用戶端

開放授權（ OAuth 2.0 ）架構的支援從 ONTAP 9.14 開始提供。當用戶端使用 REST API 存取 ONTAP 時、您只能使用 OAuth 2.0 來進行授權和控制存取決策。不過、您可以使用任何 ONTAP 管理介面（包括 CLI 、系統管理員和 REST API ）來設定和啟用此功能。

標準 OAuth 2.0 功能可與數個常用的授權伺服器一起支援。您可以使用以相互 TLS 為基礎的寄件者限制存取權杖、進一步增強 ONTAP 安全性。此外還有多種授權選項可供選擇、包括獨立的範圍、以及與 ONTAP REST 角色和本機使用者定義的整合。請參閱 "ONTAP OAuth 2.0 實作總覽" 以取得更多資訊。

系統管理員驗證與**RBAC**

系統管理員使用本機或遠端登入帳戶、在叢集和SVM上自我驗證。角色型存取控制（RBAC）決定系統管理員可以存取的命令。

驗證

您可以建立本機或遠端叢集和SVM系統管理員帳戶：

- 本機帳戶是指帳戶資訊、公開金鑰或安全性憑證位於儲存系統上的帳戶。
- 遠端帳戶是指帳戶資訊儲存在Active Directory網域控制器、LDAP伺服器或NIS伺服器上的帳戶。

除了DNS、ONTAP 在驗證用戶端時、除了使用相同的名稱服務來驗證系統管理員帳戶。

RBAC

指派給系統管理員的_role_決定系統管理員可以存取的命令。當您為系統管理員建立帳戶時、可以指派角色。您可以指派不同的角色、或視需要定義自訂角色。

掃毒

您可以在儲存系統上使用整合式防毒功能、保護資料免受病毒或其他惡意程式碼的侵害。名為 *VScann* 的還原病毒掃描、結合同級最佳的協力廠商防毒軟體與各種功能、讓您靈活控制掃描檔案的時間與時間。 ONTAP ONTAP

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。由NetApp提供且ONTAP 安裝在外部伺服器上的_《The 停止 防毒連接器（停止 防毒連接器）」、負責處理儲存系統與防毒軟體之間的通訊。

- 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、直到外部伺服器報告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。

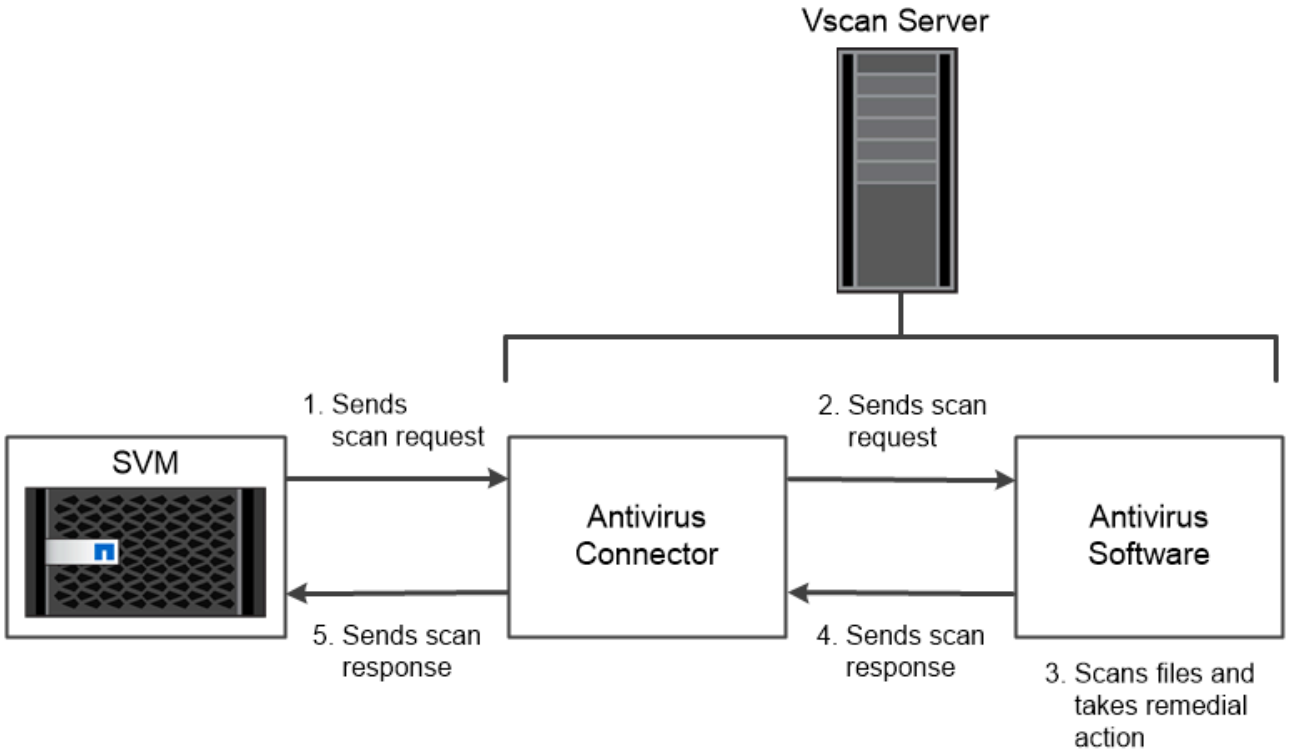
  NFS 不支援存取掃描。

- 您可以使用隨需掃描_來立即或排程檢查檔案是否有病毒。例如、您可能只想在非尖峰時間執行掃描。外部伺服器會更新已檢查檔案的掃描狀態、以便在下次透過SMB存取檔案時、這些檔案的檔案存取延遲（假設尚未修改）通常會縮短。

  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。

您通常會在SVM上啟用這兩種掃描模式。在這兩種模式中、防毒軟體都會根據您在軟體中的設定、對受感染的檔案採取補救行動。

在災難恢復和MetroCluster 不穩定的組態中執行*病毒掃描 若要進行災難恢復和MetroCluster 還原組態、您必須為本機和合作夥伴叢集分別設定VScan伺服器。



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

加密

支援以軟體和硬體為基礎的加密技術、可確保儲存媒體在重新調整用途、退回、放錯地方或遭竊時、無法讀取閒置的資料。ONTAP

所有SSL連線均符合聯邦資訊處理標準（FIPS）140-2。ONTAP您可以使用下列加密解決方案：

- 硬體解決方案：
  - NetApp儲存加密（NSE）

    NSE是使用自我加密磁碟機（SED）的硬體解決方案。

  - NVMe SED

    針對未獲得FIPS 140-2認證的NVMe SED、提供完整磁碟加密。ONTAP
- 軟體解決方案：
  - NetApp Aggregate Encryption（NAE）

    Nae是一種軟體解決方案、可加密任何磁碟機類型上的任何資料磁碟區、並為每個Aggregate啟用唯一金鑰。

  - NetApp Volume Encryption（NVE）

    NVE是一種軟體解決方案、可加密任何磁碟機類型的任何資料磁碟區、每個磁碟區都有一個唯一的金鑰。

同時使用軟體（NAE或NVE）和硬體（NSE或NVMe SED）加密解決方案、在閒置時實現雙重加密。儲存效率不受 NAE 或 NVE 加密影響。

NetApp儲存加密

NetApp儲存加密（NSE）支援在寫入資料時加密資料的SED。如果沒有儲存在磁碟上的加密金鑰、就無法讀取資料。而加密金鑰則只能由驗證的節點存取。

在I/O要求上、節點會使用從外部金鑰管理伺服器或Onboard Key Manager擷取的驗證金鑰、驗證自己是否為SED：

- 外部金鑰管理伺服器是儲存環境中的第三方系統、使用金鑰管理互通性傳輸協定（KMIP）為節點提供驗證金鑰。
- 內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供驗證金鑰。

NSE支援自我加密HDD和SSD。您可以將NetApp Volume Encryption與NSE搭配使用、將NSE磁碟機上的資料加倍加密。

如果您在具有 Flash Cache 模組的系統上使用 NSE 、您也應該啟用 NVE 或 NAE 。NSE 不會加密位於 Flash Cache 模組上的資料。

NVMe自我加密磁碟機

NVMe SED 不具備 FIPS 140-2 認證，但這些磁碟使用 AES 256 位元透明磁碟加密來保護靜止資料。

資料加密作業（例如產生驗證金鑰）會在內部執行。驗證金鑰是在儲存系統第一次存取磁碟時產生。之後、磁碟會在每次要求資料作業時要求儲存系統驗證、以保護閒置的資料。

NetApp Aggregate加密

NetApp Aggregate Encryption（NAE）是一項軟體技術、用於加密Aggregate上的所有資料。NAE的優點是、磁碟區包含在集合層級的重複資料刪除中、而NVE磁碟區則排除在外。

啟用NAE之後、即可使用Aggregate金鑰加密Aggregate內的磁碟區。

從 ONTAP 9 7 開始"NVE 授權"、新建立的集合體和磁碟區會在您擁有和內建或外部金鑰管理時、依預設進行加密。

NetApp Volume Encryption

NetApp Volume Encryption（NVE）是一項軟體技術、可一次加密閒置一個磁碟區的資料。只有儲存系統才能存取的加密金鑰可確保在基礎裝置與系統分離時、無法讀取磁碟區資料。

包括快照和中繼資料在內的資料都會加密。資料的存取權是由唯一的XTS-AES-256金鑰提供、每個磁碟區一個金鑰。內建的Onboard Key Manager可保護同一系統上的金鑰與您的資料。

您可以在任何類型的Aggregate（HDD、SSD、混合式、陣列LUN）上使用NVE、搭配任何RAID類型、也可以在ONTAP 任何支援的支援功能中使用、包括ONTAP Select 用作支援的功能、包括用作支援的功能。您也可以使用NVE搭配NetApp儲存加密（NSE）、對NSE磁碟機上的資料進行雙重加密。

*使用KMIP伺服器的時機*雖然成本較低、而且使用內建金鑰管理程式通常較為方便、但如果符合下列任一項條件、您應該設定KMIP伺服器：

- 您的加密金鑰管理解決方案必須符合聯邦資訊處理標準（FIPS）140-2或OASIS KMIP標準。
- 您需要多叢集解決方案。KMIP伺服器透過集中管理加密金鑰來支援多個叢集。

  KMIP伺服器透過集中管理加密金鑰來支援多個叢集。

- 您的企業需要更高的安全性、將驗證金鑰儲存在系統或與資料不同的位置。

  KMIP伺服器會將驗證金鑰與資料分開儲存。

相關資訊

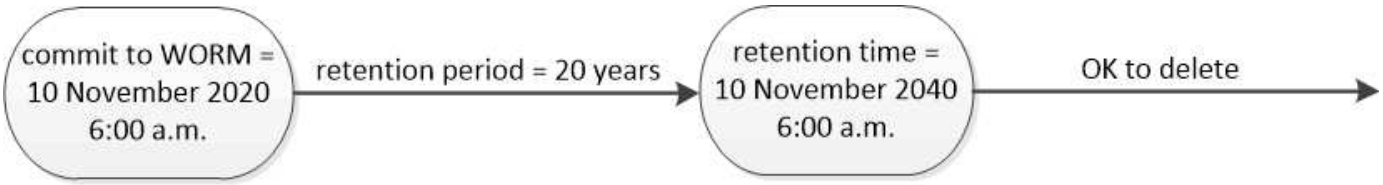
"常見問題集- NetApp Volume Encryption與NetApp Aggregate Encryption"

WORM 儲存設備

_ SnapLock 此為高效能法規遵循解決方案、適用於使用_一次寫入、多次讀取（WORM）_儲存設備、以未經修改的形式保留重要檔案、以利法規遵循與治理。

單一授權可讓您以嚴格的 _ 法規遵循模式使用 SnapLock 、 _ 以滿足如 SEC 法規 17a-4(f) 及較寬鬆 _ 企業模式等外部要求、以符合內部規定的數位資產保護法規。使用防竄改的_ComplianceClock_來判斷WORM檔案的保留期間何時結束。SnapLock

您可以在次要儲存設備上使用 SnapLock for SnapVault ，以 WORM 保護快照。您可以使用SnapMirror將WORM檔案複寫到其他地理位置、以進行災難恢復及其他用途。



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.