安全性與資料加密
ONTAP 9

NetApp
March 11, 2026

目錄

安全性與資料加密

自主勒索軟體保護

瞭解 **ONTAP** 自主勒索軟體保護

從 ONTAP 9.10.1 開始，ONTAP 管理員可以啟用自主勒索軟體防護（ARP）功能，在 NAS（NFS 和 SMB）環境中執行工作負載分析，從而主動偵測並警告可能表明勒索軟體攻擊的異常活動。從 ONTAP 9.17.1 開始，ARP 也支援區塊設備卷，包括包含 LUN 或 NVMe 命名空間的 SAN 卷，以及包含來自 VMware 等虛擬機器管理程式的虛擬磁碟的 NAS 卷。從 ONTAP 9.17.1P5 開始，也支援 Hyper-V、KVM 和 OpenStack 虛擬機器管理程式。

ARP 直接內建於 ONTAP 中，確保與 ONTAP 的其他功能實現整合控制和協調。 ARP即時運行，在檔案系統中寫入或讀取資料時進行處理，並快速偵測和回應潛在的勒索軟體攻擊。

ARP 除了按計畫建立快照外，還會定期建立鎖定快照，以增加保護。它可以智慧地管理快照的保存時長。如果沒有偵測到異常活動，快照將迅速回收。但是，如果偵測到攻擊，則會將攻擊開始前建立的快照保留較長時間。有關更多信息，包括ONTAP版本添加的更改，請參閱 ARP快照。

授權與能力

您需要取得授權才能使用 ARP。請決定是預設在新磁碟區上啟用 ARP，還是手動為每個磁碟區啟用 ARP。

ARP 的授權選項

ARP 支援包含在內"ONTAP One 許可證"。如果您沒有ONTAP One 許可證，則可以使用其他許可證來用於 ARP，具體取決於您的ONTAP版本。

發行版**ONTAP**	授權
更新版本ONTAP	`Anti_ransomware`
零點9.10.1 ONTAP	`MT_EK_MGMT` （多租戶密鑰管理）

- 如果您要從ONTAP 9.10.1 升級到ONTAP 9.11.1 或更高版本，且系統上已設定 ARP，則無需安裝新的 `Anti-ransomware`許可證。對於新的 ARP 配置，需要新的許可證。
- 如果您從ONTAP 9.11.1 或更高版本還原到ONTAP 9.10.1，並且已使用 Anti_ransomware 授權啟用 ARP，您將看到警告訊息，可能需要重新設定 ARP。"瞭解如何還原Arp" 。

ARP 啟用選項

ARP 在叢集、SVM 和磁碟區層級提供靈活的啟用選項，可讓您為新磁碟區設定自動預設啟用，或根據需要在現有磁碟區上手動啟用 ARP。

新磁碟區上的自動預設啟用

從 ONTAP 9.18.1 開始，對於 AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系統，所有新建磁碟區預設會自動啟

用 ARP。此預設會自動啟用 ARP 的功能不適用於 "不支援的磁碟區或組態"。

升級後，新磁碟區上的 ARP 預設啟用將在 12 小時寬限期後生效；對於新 ONTAP 9.18.1 安裝，則 ARP 預設啟用將立即生效，前提是已安裝 ARP 授權。您必須手動啟用 ARP在現有磁碟區上。

在寬限期內，您可以"使用 System Manager 或 ONTAP CLI 在叢集層級選擇退出新磁碟區的預設啟用"。如果您未選擇退出，則寬限期結束後建立的所有新磁碟區都會自動啟用 ARP。如果寬限期結束後需求發生變化，您也可以隨時靈活地啟用或停用預設啟用功能。

在新磁碟區上手動啟用預設功能

如果您在叢集層級停用了 ARP 的自動預設啟用，也可以選擇"手動在所有新磁碟區上預設啟用 ARP"在 SVM 層級進行設定。對於 ONTAP 9.17.1 及更早版本，這是將 ARP 設定為在新磁碟區上預設啟用的唯一方法。

在所有或特定現有磁碟區上啟用 **ARP**

從 9.18.1 版本開始，您可以從叢集層級手動在所有現有磁碟區上啟用 ARP（選擇 叢集 **>** 安全性，然後在 **Anti-ransomware** 區段中按一下 ⋮，接著選擇 在所有現有磁碟區上啟用）。

如果您希望將 ARP 啟用限制在特定磁碟區上，您可以"以每個磁碟區為基礎啟用 ARP"。

勒索軟體保護策略**ONTAP**

有效的勒索軟體防護需要多層防護協同運作。

雖然 ONTAP 包含 FPolicy、快照、SnapLock 和 Active IQ Digital Advisor（也稱為 Digital Advisor）等功能來幫助抵禦勒索軟體，但 ARP 提供了一層額外的防禦。

若要深入瞭解 NetApp 產品組合中可防範勒索軟體的其他功能，請參閱：

- "勒索軟體和 NetApp 的保護產品組合"
- "使用 PowerShell 進行 ONTAP 網路保險庫加固"

ARP 偵測到什麼

ONTAP ARP 旨在防禦拒絕服務攻擊，即攻擊者扣留資料直至支付贖金。 ARP基於以下方式提供即時勒索軟體偵測：

- 將傳入資料識別為加密或純文字。
- 可偵測下列項目的分析：
  - 熵：（用於 NAS 和 SAN）對文件中資料隨機性的評估
  - 檔案副檔名類型：（僅在 NAS 中使用）不符合預期副檔名類型的檔案副檔名
  - 檔案 **IOPS**：（僅在ONTAP 9.11.1 開始的 NAS 中使用）資料加密時異常卷活動激增

ARP 只需少量檔案被加密即可偵測到大多數勒索軟體攻擊的傳播，自動回應以保護數據，並提醒您疑似攻擊正在發生。

ⓘ 沒有任何勒索軟體偵測系統可以保證完全的安全。如果防毒軟體無法偵測到入侵，ARP 可提供額外的防禦層。

了解 **ARP** 模式

在為磁碟區啟用 ARP 後，它將進入學習期以建立基線。 ARP 在轉換到主動偵測模式之前會分析系統指標以建立警報設定檔。在主動模式下，ARP 監控異常活動，如果偵測到異常行為，則採取保護措施並產生警報。

對於 ARP，學習模式和主動模式行為因ONTAP版本、磁碟區類型和協定（NAS 或 SAN）而異。

NAS 環境和模式類型

下表總結了ONTAP 9.10.1 與 NAS 環境的更高版本之間的差異。

對於採用早期 ARP 模型的版本，建議在開始主動監控之前先進行一段時間的學習。對於支援 NAS 的環境ARP/AI沒有學習期，立即開始主動監控。

模式	說明	卷類型和版本
學習	對於某些版本的ONTAP和某些磁碟區類型，啟用 ARP 時，ARP 會自動設定為學習模式。在學習模式下， ONTAP系統會根據以下分析領域（熵、檔案副檔名類型和檔案 IOPS）制定警報設定檔。 建議您將 ARP 保持在學習模式 30 天。從ONTAP 9.13.1 開始，ARP 會自動確定最佳學習間隔並自動切換，切換可能在 30 天之前完成。對於ONTAP 9.13.1 之前的版本，您可以手動進行切換。 從ONTAP 9.16.1 開始， FlexVol磁碟區僅存在活動模式，任何升級到此版本或更高版本的FlexVol磁碟區都會自動從學習模式過渡到活動模式。 對於ONTAP 9.16.1 到 9.17.1，ARP/AI 尚不支援FlexGroup卷，並繼續運行較舊的 ARP 模型。因此，對於這些帶有FlexGroup卷的版本，仍然建議留出一段學習期。 從ONTAP 9.18.1 開始， FlexVol和FlexGroup磁碟區都只有活動模式。任何升級後的捲都會自動切換到活動模式。 "了解有關從學習模式切換到主動模式的更多信息" 。 命令 `security anti-ransomware volume workload-behavior show`會顯示已在磁碟區中偵測到的副檔名。如果您在學習模式早期執行此命令，並顯示正確的檔案類型呈現，則不應將該資料當作移至作用中模式的基礎，因為 ONTAP 仍在收集其他計量。如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume workload-behavior show`資訊，請參閱。	• FlexVol卷（採用ONTAP 9.10.1 至 9.15.1） • FlexGroup卷，版本從ONTAP 9.13.1 到ONTAP 9.17.1
積極的	在主動模式下，如果檔案副檔名被標記為異常，您應該評估該警報。您可以根據警報採取行動來保護數據，也可以將警報標記為誤報。將警報標記為誤報會更新警報設定檔。例如，如果警報是由新的檔案副檔名觸發的，並且您將警報標記為誤報，則下次觀察到該檔案副檔名時，您將不會收到警報。	所有支援的ONTAP版本以及FlexVol和FlexGroup卷

SAN 環境和模式類型

SAN 環境會使用評估期（類似 NAS 環境中的學習模式），然後自動過渡到主動偵測。下表總結了評估模式和主動模式。

模式	說明	卷類型和版本
評估	進行為期兩到四週的評估期，以確定基線加密行為，同時 ARP/AI 在評估期內為 SAN 磁碟區提供即時主動保護。在建立基線閾值期間，可以進行偵測並發出警報。您可以透過執行以下命令來確定評估期間是否結束： `security anti-ransomware volume show`**命令和檢查** `Block device detection status`。 "了解有關 SAN 捲和熵評估期的更多信息" 。	• 帶有ONTAP 9.17.1 及更高版本的FlexVol 卷
積極的	評估期結束後，您可以透過運行 `security anti-ransomware volume show`**指揮和檢查** `Block device detection status`.的狀態 `Active_suitable_workload`表示可以成功監測到評估的熵值。 ARP會根據評估過程中審查的數據自動調整自適應閾值。	• 帶有ONTAP 9.17.1 及更高版本的FlexVol 卷

威脅評估和 **ARP** 快照

ARP 根據接收到的數據，並結合現有的分析數據來評估威脅機率。當 ARP 偵測到異常情況時，會指派一個度量值。ARP 可能會在偵測到異常時分配一個快照，也可能定期分配一個快照。

ARP 閾值

- * 低 * ：磁碟區最早偵測到異常（例如，在磁碟區中觀察到新的副檔名）。此偵測層級僅適用於 ONTAP 9 。16.1 之前的版本，但沒有 ARP/AI 。
  - 從ONTAP 9.11.1 開始，您可以"自訂ARP檢測參數" 。
  - 在 ONTAP 9.10.1 中、向上提報至中度的臨界值為 100 個以上的檔案。
- 中：偵測到高熵，或觀察到多個具有相同前所未見檔案副檔名的檔案。這是ONTAP 9.16.1 及更高版本中帶有 ARP/AI 的基準檢測等級。

當ONTAP運行分析報告確定異常是否與勒索軟體設定檔匹配時，威脅會升級為中等。當攻擊機率為中等時，ONTAP會產生 EMS 通知，提示您評估威脅。 ONTAPONTAP 不會傳送關於低威脅的警示；但是，從 ONTAP 9.14.1 開始，您可以 "修改預設警報設定"。"回應異常活動" 。

您可以在 System Manager 的 * 事件 * 區段或命令中檢視中度威脅的相關資訊 `security anti-ransomware volume show`。在 ONTAP 9.16.1 之前的版本中，如果沒有 ARP/AI ，也可以使用命令來檢視低威脅事件 `security anti-ransomware volume show`。如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume show`資訊，請參閱。

ARP快照

當偵測到攻擊的早期跡象時，ARP 會建立快照。然後進行詳細分析，以確認或排除潛在攻擊。由於 ARP 快照是在攻擊得到完全確認之前主動創建的，因此它們也可能會定期為某些合法應用程式產生。這些快照的存在不應被視為異常。如果確認發生攻擊，則攻擊機率將升級為 `Moderate`並產生攻擊通知。

從ONTAP 9.17.1 開始，會定期為 NAS 和 SAN 磁碟區產生 ARP 快照，並回應偵測到的異常。ONTAP在 ARP 快照前新增一個名稱，以便於識別。

從ONTAP 9.11.1 開始，您可以修改保留設定。有關更多信息，請參閱"修改快照選項" 。

下表總結了不同版本的 ARP 快照差異。

功能	**ONTAP 9.17.1** 及更高版本	**ONTAP 9.16.1** 及更早版本
建立觸發器	• 快照以固定的 4 小時間隔創建，無論任何特定觸發器如何 • 確認攻擊 根據觸發類型建立“定期”或“攻擊”快照。	• 偵測到高熵 • 偵測到新的檔案副檔名（9.15.1 及更早版本） • 偵測到文件操作激增（9.15.1 及更早版本） 快照建立間隔基於觸發器類型。
前綴名稱約定	“反勒索軟體定期備份” “反勒索軟體攻擊備份”	“反勒索軟體備份”
刪除行為	ARP快照被鎖定，管理員無法刪除	ARP快照被鎖定，管理員無法刪除
最大快照數	"六個快照可配置限制"	"六個快照可配置限制"
保留期	快照通常保留 12 小時。 • NAS 卷：如果透過檔案分析確認了攻擊，則攻擊前建立的快照將保留，直到管理員將攻擊標記為真或誤報（明確懷疑）。 • SAN 磁碟區或 VM 資料儲存：如果透過區塊熵分析確認了攻擊，則攻擊前建立的快照將保留 10 天（可設定）。	• 根據觸發條件確定（不固定） • 攻擊先前建立的快照將保留，直到管理員將攻擊標記為真或誤報（明確嫌疑）。
明確嫌疑行動	管理員可以執行清除嫌疑的操作，該操作根據確認設定保留： • 誤報保留時間為 24 小時 • 真實陽性保留時間為 7 天	管理員可以執行清除嫌疑的操作，該操作根據確認設定保留： • 誤報保留時間為 24 小時 • 真實陽性保留時間為 7 天 此預防性保留行為在ONTAP 9.16.1 之前不存在
到期時間	所有快照均設定了到期時間	無

如何在**ONTAP** 勒索軟體攻擊後恢復資料

ARP 基於成熟的ONTAP資料保護和災難復原技術，可有效應對勒索軟體攻擊。當偵測到攻擊的早期跡象時，ARP 會建立鎖定快照。您需要先確認攻擊是真實攻擊還是誤報。如果您確認有攻擊，則可以使用 ARP 快照復原磁碟區。

鎖定的快照無法透過正常方式刪除。但是，如果您稍後決定將攻擊標記為誤報， ONTAP會刪除鎖定的副本。

您可以從選定的快照中恢復受影響的文件，而不必恢復整個磁碟區。

有關應對攻擊和恢復資料的更多信息，請參閱以下主題：

- "回應異常活動"
- "從 ARP 快照恢復數據"
- "從ONTAP快照恢復"
- "智慧型勒索軟體還原"

ARP 的多管理驗證保護

從 ONTAP 9.13.1 開始，我們建議您啟用多重管理驗證（ MAV ），以便在進行自主勒索軟體保護（ ARP ）組態時，需要兩個或更多已驗證的使用者管理員。如需更多資訊、請參閱 "啟用多重管理驗證"。

人工智慧的自主勒索軟體保護（ **ARP/AI** ）

從ONTAP 9.16.1 開始，ARP 採用機器學習模型進行反勒索軟體分析，從而提升了網路彈性。該模型能夠在 NAS 環境中以 99% 的準確率檢測不斷演變的勒索軟體形式。的機器學習模型在模擬勒索軟體攻擊前後都基於大量文件資料集進行了預訓練。這種資源密集的訓練是在ONTAP之外進行的，使用開源取證研究資料集來訓練模型。整個建模流程不會使用客戶數據，因此不存在隱私問題。此訓練產生的預訓練模型隨ONTAP一起提供。但無法透過ONTAP CLI 或ONTAP API 存取或修改此模型。

立即過渡到主動防禦**ARP/AI**

使用ARP/AI，就沒有學習週期。對於以下受支援的磁碟區類型，ARP/AI 在安裝或升級後立即啟動：

- NAS FlexVol卷，支援ONTAP 9.16.1 及更高版本
- NAS FlexGroup卷， ONTAP9.18.1 及更高版本
- 使用ONTAP 9.17.1 及更高版本的 SAN 磁碟區（立即激活，即使在期間）"評估期" ）

對於已啟用 ARP 功能的現有捲和新磁碟區，將叢集升級至支援 ARP/AI 的ONTAP版本後，ARP/AI 保護將自動啟動。

ARP/AI 自動更新

為了持續提供對最新勒索軟體威脅的最新保護，ARP/AI 提供頻繁的自動更新，這些更新在ONTAP常規升級和發布週期之外進行。如果您"已啟用自動更新"在您選擇安全檔案自動更新後，您也將能夠開始接收 ARP/AI 的自動安全性更新。您也可以選擇"手動進行這些更新"並控制更新發生的時間。

從 ONTAP 9 。 16.1 開始，除了系統和韌體更新之外，還可使用系統管理員來提供 ARP/AI 的安全性更新。

"深入瞭解 ARP/AI 更新"

ARP/AI 與 **ARP** 模型之間的差異概覽

功能	**ARP**	**ARP/AI**
ONTAP 版本	ONTAP 9.10.1-9.15.1	ONTAP 9.16.1 及更新版本；9.15.1（技術預覽）
偵測方法	分析檔案活動、資料熵和檔案副檔名類型	基於大型取證資料集訓練的 AI / 機器學習模型；分析熵和檔案行為

功能	ARP	ARP/AI
學習期	NAS FlexVol Volume 需要 30 天學習模式（9.13.1 及更高版本支援自動切換）	無需學習期；啟用後立即生效
磁碟區類型支援	• FlexVol：9.10.1 及更高版本 • FlexGroup：9.13.1 及更高版本 • SAN:不支援	• FlexVol：9.16.1 及更高版本 • FlexGroup：9.18.1 及更高版本 • SAN：9.17.1 及更新版本（含評估期間）
Snapshot 建立	由高熵、新的檔案副檔名或檔案操作激增所觸發	以固定 4 小時間隔建立，並在確認攻擊時建立
Snapshot 保留	保留直到管理員清除可疑活動	預設時間為 12 小時；依攻擊確認情況延長（誤報為 24 小時，確認為正確為 7 天）
更新	靜態偵測邏輯（僅在 ONTAP 升級時更新）	自動安全性更新，與 ONTAP 版本無關
部署	手動啟用（按磁碟區）或 SVM 層級預設設定	可手動按磁碟區啟用或設定 SVM 等級的預設設定；對於 9.18.1 及更高版本中支援的系統，所有新磁碟區均預設在叢集層級啟用
評估期	不適用	SAN 磁碟區需要（2-4 週）來建立基線加密閾值

相關資訊

- "指令參考資料ONTAP"

ONTAP 自主勒索軟體保護使用案例與考量

自主勒索軟體防護 (ARP) 適用於從ONTAP 9.10.1 開始的 NAS 工作負載和從ONTAP 9.17.1 開始的 SAN 工作負載。在部署 ARP 之前，您應該了解其建議用途、支援的配置以及效能影響。

支援和不支援的組態

在決定使用 ARP 時、請務必確保您的磁碟區工作負載適合 ARP 、並且符合所需的系統組態。

合適的工作負載

ARP 適用於以下類型的工作負載：

- NFS 或 SAN 儲存上的資料庫
- Windows或Linux主目錄

  對於沒有 ARP/AI 的環境，使用者可能會建立一些在學習期間無法偵測到的副檔名的檔案。因此，此類工作負載中出現誤報的可能性較大。

- 影像與影片

  例如、醫療記錄和電子設計自動化（ EDA ）資料

不適當的工作負載

ARP 不適合以下類型的工作負載：

- 具有高頻率檔案建立或刪除操作的工作負載（幾秒鐘內數十萬個檔案；例如，測試/開發工作負載）。
- ARP 的威脅偵測依賴於其識別檔案建立、重新命名或刪除操作異常激增的能力。如果應用程式本身是文件活動的來源，則無法有效區分勒索軟體活動。
- 應用程式或主機加密資料的工作負載。

  ARP 依賴區分傳入資料是加密的還是未加密的。如果應用程式本身正在加密數據，則該功能的有效性會降低。但是，ARP 仍然可以根據檔案活動（刪除、覆蓋、創建，或建立檔案或使用新的檔案副檔名重新命名）和檔案類型進行工作。

支援的組態

從ONTAP 9.10.1 開始，ARP 可用於 NAS NFS 和 SMB FlexVol磁碟區。從 9.17.1 開始，ARP 可用於 iSCSI 、FC 和具有 SAN 儲存的 NVMe 的 SAN FlexVol磁碟區。

從 ONTAP 9.10.1 開始，MetroCluster 組態支援 ARP。

下列 ONTAP 版本支援其他組態和磁碟區類型：

	ONTAP 9.18.1	**ONTAP 9.17.1**	**ONTAP 9.16.1.**	**ONTAP 9.15.1.1**	**ONTAP 9.14.1.**	**ONTAP 9.13.1.12 .9.11.9.1 1.**	**ONTAP 9.12.1**	**零點9.11. 1. ONTAP**	**零點9.10. 1 ONTAP**
使用 SnapMirror 非同步保護的磁碟區	✓	✓	✓	✓	✓	✓	✓		
受 SnapMirror 非同步（ SVM 災難恢復）保護的 SVM	✓	✓	✓	✓	✓	✓	✓		
SVM資料移動性 (`vserver migrate`)	✓	✓	✓	✓	✓	✓	✓		

	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1.	ONTAP 9.15.1.1	ONTAP 9.14.1.	ONTAP 9.13.1.12 .9.11.9.1 1.	ONTAP 9.12.1	零點9.11. 1. ONTAP	零點9.10. 1 ONTAP
FlexGroup卷[1]	✓	✓	✓	✓	✓	✓			
多管理員驗證	✓	✓	✓	✓	✓				
ARP/AI提供自動更新	✓	✓	✓						
ARP/AI預設啟用[2]	✓								

[1] ONTAP 9.16.1 和 9.17.1 不提供FlexGroup卷的 ARP/AI 支援。升級到這些版本後，啟用 ARP 的FlexGroup磁碟區將繼續使用 ARP/AI 之前使用的相同 ARP 模型運行。從ONTAP 9.18.1 開始， FlexGroup磁碟區使用 ARP/AI 模型。

[2] 從 ONTAP 9.18.1 開始，AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系統均支援 ARP/AI 預設為啟用。此行為會在升級後 12 小時寬限期後自動為所有新磁碟區啟用 ARP/AI,或新 ONTAP 9.18.1 安裝的系統則立即啟用。您需要手動啟用 ARP "現有磁碟區"。

SnapMirror與ARP互通性

從ONTAP 9.12.1 開始， SnapMirror非同步目標磁碟區支援 ARP。 SnapMirrorSnapMirror同步或SnapMirror主動同步不支援 ARP。

如果SnapMirror來源磁碟區啟用了 ARP，則SnapMirror目標磁碟區會自動取得 ARP 設定狀態（例如 `dry-run` 或者 `enabled`）、ARP 訓練資料以及 ARP 建立的來源磁碟區快照。無需明確啟用。

儘管目標磁碟區包含唯讀 (RO) 快照，但其資料不會進行任何 ARP 處理。但是，當SnapMirror目標磁碟區轉換為讀寫 (RW) 時，ARP 會在已轉換為 RW 的目標磁碟區上自動啟用。除了來源磁碟區上已記錄的內容外，目標磁碟區不需要任何其他學習過程。

在ONTAP 9.10.1 和 9.11.1 中， SnapMirror不會將 ARP 設定狀態、訓練資料和快照從來源磁碟區傳送到目標磁碟區。因此，當SnapMirror目標磁碟區轉換為 RW 時，必須在轉換後在學習模式下明確啟用目標磁碟區上的 ARP。

ARP 和虛擬機器

VMware 上的虛擬機器 (VM) 支援 ARP。檢測對於虛擬機器內部和外部的變更有不同的行為。對於虛擬機器中涉及大量高度壓縮檔案（例如 7z 和 ZIP）或加密檔案（例如受密碼保護的 PDF、DOC 或 ZIP）的工作負載，不建議使用 ARP。

VM 以外的變更

如果新副檔名以加密狀態進入磁碟區或檔案副檔名發生變化，ARP 可以偵測到 VM 外部 NFS 磁碟區上的檔案副檔名變化。

VM 內部的變更

如果勒索軟體攻擊更改了虛擬機器內部的文件，而沒有更改虛擬機器外部的文件，且虛擬機器的預設熵較低（例如 .txt、.docx 或 .mp4 文件），ARP 就會偵測到威脅。對於ONTAP 9.16.1 及更早版本，ARP 會在這種情況下建立保護性快照，但不會產生威脅警報，因為虛擬機器外部的檔案副檔名未被竄改。從ONTAP 9.17.1 中的 SAN 支援開始，如果 ARP 偵測到虛擬機器內部的熵異常，也會產生威脅警報。

如果檔案預設為高熵檔案（例如 .gzip 檔案或受密碼保護的檔案），ARP 的偵測能力就會受到限制。在這種情況下，ARP 仍然可以主動拍攝快照；但是，如果檔案副檔名未被外部篡改，則不會觸發警報。

對於 SAN，ARP 在磁碟區層級分析熵統計數據，並在發現熵異常時觸發檢測。

在ONTAP 9.18.1 及更高版本中，僅FlexVol磁碟區可偵測 VM 內發生的攻擊，如果 VM 資料儲存配置在FlexGroup磁碟區上，則無法偵測 VM 內發生的攻擊。

不支援的組態

ONTAP S3 環境不支援 ARP。

ARP 不支援下列 Volume 組態：

- FlexGroup磁碟區（在ONTAP 9.10.1 至 9.12.1 中）。

  從ONTAP 9.13.1 到ONTAP 9.17.1，支援FlexGroup卷，但僅限於 ARP/AI 之前使用的 ARP 模型。 ONTAP 9.18.1 開始支援 ARP/AI 的FlexGroup磁碟區。

- FlexCache Volume （原始 FlexVol 磁碟區支援 ARP 、快取磁碟區則不支援）
- 離線磁碟區
- 資料量SnapLock
- SnapMirror 主動同步
- SnapMirror 同步
- SnapMirror非同步（在ONTAP 9.10.1 和 9.11.1 中）。從ONTAP 9.12.1 開始支援SnapMirror非同步。有關更多信息，請參閱[SnapMirror] 。
- 受限磁碟區
- 儲存VM的根磁碟區
- 已停止儲存VM的磁碟區

ARP效能和頻率考量

ARP 對系統效能（以吞吐量和峰值 IOPS 衡量）的影響極小。 ARP功能的影響取決於特定的捲工作負載。對於常見工作負載，建議採用以下配置限制：

工作負載特性	每個節點的建議**Volume**限制	當每個節點的磁碟區限制超過上限時，效能會下降[1]
讀取密集型或資料可以壓縮	150	最高IOPS的4%

工作負載特性	每個節點的建議Volume限制	當每個節點的磁碟區限制超過上限時，效能會下降[1]
寫入密集且資料無法壓縮	60	• NAS： ONTAP 9.15.1 及更早版本的最大 IOPS 的 10% • NAS：ONTAP 9.16.1 及更高版本最大 IOPS 的 5% • SAN： ONTAP 9.17.1 及更高版本的最大 IOPS 的 5%

[1] 無論添加的捲數量超過建議的限制多少，系統效能都不會下降超過這些百分比。

由於 ARP 分析按優先順序運行，因此隨著受保護磁碟區數量的增加，每個磁碟區上運行的分析頻率會降低。

預設在大量新磁碟區上啟用 ARP 可能會增加系統資源使用量。在磁碟區上啟用 ARP 時，請考慮快照等競爭程序的空間需求。

依平台的 **ARP** 磁碟區限制

從 ONTAP 9.18.1 開始、ARP 支援根據平台類型和 CPU 核心數增加磁碟區限制。

平台類型	每個節點啟用 **ARP** 的最大磁碟區數
低階（最多 20 個 CPU 核心的系統）	250
中等配置（最多 64 個 CPU 核心的系統）	500
高階（擁有超過 64 個 CPU 核心的系統）	1000

CPU 核心數適用於 2 節點 HA 對中的每個單獨節點。

使用 **ARP** 保護的磁碟區進行多重管理驗證

從 ONTAP 9.13.1 開始、您可以啟用多重管理驗證（ MAV ）、以提高 ARP 的安全性。MAV 可確保至少有兩位或多位通過驗證的系統管理員必須關閉 ARP 、暫停 ARP 、或將可疑攻擊標示為受保護磁碟區上的誤報。瞭解如何"為受 ARP 保護的磁碟區啟用 MAV"。

您需要為 MAV 群組定義系統管理員，並為您要保護的， `security anti-ransomware volume pause`和 `security anti-ransomware volume attack clear-suspect` ARP 命令建立 MAV 規則 `security anti-ransomware volume disable`。MAV 群組中的每位管理員都必須核准每個新規則要求，並"再次新增 MAV 規則"在 MAV 設定內進行。

深入瞭解 `security anti-ransomware volume disable`， `security anti-ransomware volume pause`和 `security anti-ransomware volume attack clear-suspect` "指令參考資料ONTAP"。

從ONTAP 9.14.1 開始，ARP 會在建立 ARP 快照和發現新檔案副檔名時發出警報。這些事件的警報預設為禁用狀態。警報可以在磁碟區或 SVM 層級設定。您可以使用以下命令啟用警報 `security anti-ransomware vserver event-log modify`或使用 `security anti-ransomware volume event-log modify`。

深入瞭解 `security anti-ransomware vserver event-log modify`及 `security anti-`

`ransomware volume event-log modify` "指令參考資料ONTAP"。

後續步驟

- "啟用自發勒索軟體保護"
- "為受 ARP 保護的磁碟區啟用 MAV"

啟用 ARP

在磁碟區上啟用 **ONTAP Autonomous Ransomware Protection**

從 ONTAP 9 。 10.1 開始，您可以在現有的磁碟區上啟用「自主勒索軟體保護」（ARP ），或是建立新的磁碟區，從頭開始啟用 ARP 。

關於這項工作

若要啟用 ARP，請按照與您的環境相符的步驟操作。您確保您的環境符合某些要求 ：

- 帶有FlexVol磁碟區的 NAS
- 帶有FlexGroup磁碟區的 NAS
- SAN 磁碟區

啟用 ARP 後，ARP 可能會進入過渡期，具體取決於您的環境和ONTAP版本：

Volume類型	版本**ONTAP**	啟用後的行為
NAS FlexGroup	ONTAP 9.18.1 及更高版本	ARP/AI 無需學習期即可立即生效
	ONTAP 9.13.1 至 9.17.1	ARP啟動後將進入學習模式，持續30天。
NAS FlexVol	ONTAP 9.16.1 及更新版本	ARP/AI 無需學習期即可立即生效
	ONTAP 9.10.1 至 9.15.1	ARP啟動後將進入學習模式，持續30天。
SAN 磁碟區	ONTAP 9.17.1 及更高版本	ARP/AI 立即啟動，啟動評估期，以確定合適的警報閾值，然後再從初始的保守閾值過渡。

開始之前

啟用 ARP 之前，請確保您的環境具備以下條件：

NAS 特定要求

- 啟用了 NFS 或 SMB（或兩者）協定的儲存虛擬機器 (SVM)。
- 已配置客戶端的 NAS 工作負載。
- 積極"交會路徑"就音量而言。

SAN 特定要求

- 啟用了 iSCSI、FC 或 NVMe 協定的儲存虛擬機器 (SVM)。
- 已配置客戶端的 SAN 工作負載。

一般要求

- 這"正確授權"適用於您的ONTAP版本。
- （建議）啟用多管理員驗證 (MAV)（ONTAP 9.13.1 及更高版本）。看"啟用多重管理驗證"。

在 **NAS FlexVol**磁碟區上啟用 **ARP**

您可以使用系統管理員或ONTAP CLI 在 NAS FlexVol磁碟區上啟用 ARP。具體流程會根據您的ONTAP版本而有所不同。

ONTAP 9.16.1 及更新版本

從ONTAP 9.16.1 開始，ARP/AI 可立即激活，無需學習期。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取您要保護的磁碟區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. 在「反勒索軟體」方塊中驗證磁碟區的 ARP 狀態。

   若要顯示所有磁碟區的 ARP 狀態：在 * Volumes （磁碟區） * 窗格中，選取 * Show （顯示） / Hide （隱藏） * ，然後確定已勾選 * Anti-勒索 ware* 狀態。

CLI

在現有磁碟區上啟用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

建立啟用 **ARP** 的新磁碟區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path
</path_name>
```

驗證**ARP**狀態：

```
security anti-ransomware volume show
```

如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume show`資訊，請參閱。

ONTAP 9.10.1 至 **9.15.1**

對於ONTAP 9.10.1 至 9.15.1 版本，您應該先啟用 ARP。"學習模式" （或“試運轉”狀態）。該系統透過分析工作負載來描述正常行為。以主動模式啟動可能會導致過多的誤報。

建議讓 ARP 以學習模式運作至少 30 天。從ONTAP 9.13.1 開始，ARP 會自動確定最佳學習間隔並自動切換，切換可能在 30 天之前完成。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取您要保護的磁碟區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. 在「反勒索軟體」方塊中選擇「在學習模式下啟用」。

你可以"停用關聯儲存虛擬機器上的自動學習活動模式轉換"如果您想手動控制學習模式到主動模式的轉換。

在現有的磁碟區中、學習和作用中模式僅適用於新寫入的資料、而不適用於磁碟區中現有的資料。不會掃描和分析現有資料、因為在啟用Volume以進行Arp之後、會根據新資料來假設先前一般資料流量的特性。

4. 在「反勒索軟體」方塊中驗證磁碟區的 ARP 狀態。

   若要顯示所有磁碟區的 ARP 狀態：在 * Volumes （磁碟區） * 窗格中，選取 * Show （顯示） / Hide （隱藏） * ，然後確定已勾選 * Anti-勒索 ware* 狀態。

CLI

在現有磁碟區上啟用 **ARP**：

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume dry-run`資訊，請參閱。

建立啟用 **ARP** 的新磁碟區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path
</path_name>
```

停用自動切換（可選）：

如果您已將ONTAP升級至 ONTAP 9.13.1 至ONTAP 9.15.1，並且想要手動控制所有關聯磁碟區從學習模式切換到活動模式，則可以從 SVM 執行此操作：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

驗證**ARP**狀態：

```
security anti-ransomware volume show
```

在 **NAS FlexGroup**磁碟區上啟用 **ARP**

您可以使用系統管理員或ONTAP CLI 在 NAS FlexGroup磁碟區上啟用 ARP。具體流程會根據您的ONTAP版本而有所不同。

ONTAP 9.18.1 及更高版本

從ONTAP 9.18.1 開始，ARP/AI 對FlexGroup卷立即生效，無需學習期。

系統管理員

1. 選擇“儲存 > 磁碟區”，然後選擇要保護的FlexGroup區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. 在「反勒索軟體」方塊中驗證磁碟區的 ARP 狀態。

   若要顯示所有磁碟區的 ARP 狀態：在 * Volumes （磁碟區） * 窗格中，選取 * Show （顯示） / Hide （隱藏） * ，然後確定已勾選 * Anti-勒索 ware* 狀態。

CLI

在現有**FlexGroup**磁碟區上啟用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

建立啟用 **ARP** 的新**FlexGroup**區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state enabled -junction-path </path_name>
```

驗證**ARP**狀態：

```
security anti-ransomware volume show
```

ONTAP 9.13.1 至 **9.17.1**

對於ONTAP 9.13.1 至 9.17.1 版本， FlexGroup磁碟區的起始版本為："學習模式" 。該系統透過分析工作負載來描述正常行為。

建議讓 ARP 以學習模式運作至少 30 天。ARP 會自動確定最佳學習週期間隔並自動切換，切換可能在 30 天之前發生。

系統管理員

1. 選擇“儲存 > 磁碟區”，然後選擇要保護的FlexGroup區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. 在「反勒索軟體」方塊中選擇「在學習模式下啟用」。

你可以"停用自動學習到活動模式的轉換"如果您想手動控制學習模式到主動模式的轉換。

4. 在「反勒索軟體」方塊中驗證磁碟區的 ARP 狀態。

CLI

在現有**FlexGroup**磁碟區上啟用 **ARP**：

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

建立啟用 **ARP** 的新**FlexGroup**區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state dry-run -junction-path </path_name>
```

停用自動切換（可選）：

如果您想手動控制從學習模式到活動模式的切換：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

驗證**ARP**狀態：

```
security anti-ransomware volume show
```

在**SAN**磁碟區上啟用**ARP**

從ONTAP 9.17.1 開始，您可以在 SAN 磁碟區上啟用 ARP。 ARP/AI 功能會自動啟用，並在 SAN 磁碟區維護期間立即開始主動監控和保護 SAN 磁碟區。"評估期"同時確定工作負載是否適合 ARP，並設定最佳加密偵測閾值。

您可以使用系統管理員或ONTAP CLI 在 SAN 磁碟區上啟用 ARP。

系統管理員

步驟

1. 選擇“儲存 > 磁碟區”，然後選擇要保護的 SAN 磁碟區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. ARP/AI自動進入評估期。
4. 在「反勒索軟體」方塊中驗證 ARP 狀態和評估狀態。

   若要顯示所有磁碟區的 ARP 狀態：在 * Volumes （磁碟區） * 窗格中，選取 * Show （顯示） / Hide （隱藏） * ，然後確定已勾選 * Anti-勒索 ware* 狀態。

CLI

在現有 **SAN** 磁碟區上啟用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

建立啟用 **ARP** 的新 **SAN** 磁碟區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

驗證**ARP**狀態和評估狀態：

```
security anti-ransomware volume show
```

檢查 `Block device detection status`現場監測評估期進展。

如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume show`資訊，請參閱。

相關資訊

- "在學習期間後切換至使用中模式"

在新磁碟區中，預設啟用 **ONTAP** 自主勒索軟體保護

從 ONTAP 9.10.1 開始，您可以設定儲存虛擬機器（SVM），以便預設為新磁碟區啟用自主勒索軟體防護（ARP）。您可以使用 System Manager 或 ONTAP CLI 修改此設定。

從 ONTAP 9.18.1 開始，在叢集升級或全新安裝後經過 12 小時的寬限期後，"支援的系統" 的所有新磁碟區預設會在叢集層級啟用 ARP。如果您在叢集層級停用 ARP 的自動預設啟用，仍可選擇在 SVM 層級手動為所有新磁碟區預設啟用 ARP。

對於 ONTAP 9.17.1 及更早版本，在 SVM 層級進行設定是預設在新磁碟區上啟用 ARP 的唯一方法。

關於這項工作

預設情況下，新建磁碟區的 ARP 功能是停用的。您需要啟用 ARP 功能，並將其設定為在 SVM 中建立的新磁碟區上預設為啟用。

當您變更 SVM 的預設值時，未啟用 ARP 的現有磁碟區不會自動變更 ARP 啟用狀態。本程式中所述的 SVM 設定變更僅影響新產生的磁碟區。學習如何"為現有磁碟區啟用 ARP"。

啟用 ARP 後，ARP 可能會進入過渡期，具體取決於您的環境和ONTAP版本：

Volume類型	版本**ONTAP**	啟用後的行為
NAS FlexGroup	ONTAP 9.18.1 及更高版本	ARP/AI 無需學習期即可立即生效
	ONTAP 9.13.1 至 9.17.1	ARP啟動後將進入學習模式，持續30天。
NAS FlexVol	ONTAP 9.16.1 及更新版本	ARP/AI 無需學習期即可立即生效
	ONTAP 9.10.1 至 9.15.1	ARP啟動後將進入學習模式，持續30天。
SAN 磁碟區	ONTAP 9.17.1 及更高版本	ARP/AI 立即啟動，啟動評估期，以確定合適的警報閾值，然後再從初始的保守閾值過渡。

開始之前

啟用 ARP 之前，請確保您的環境具備以下條件：

NAS 特定要求

- 啟用了 NFS 或 SMB（或兩者）協定的儲存虛擬機器 (SVM)。
- 積極"交會路徑"就音量而言。

SAN 特定要求

- 啟用了 iSCSI、FC 或 NVMe 協定的儲存虛擬機器 (SVM)。

一般要求

- 這"正確授權"適用於您的ONTAP版本。
- （建議）啟用多管理員驗證（MAV）（ONTAP 9.13.1+）。看"啟用多重管理驗證"。

步驟

您可以使用系統管理員或 ONTAP CLI 在新磁碟區上預設啟用 ARP 。

系統管理員

1. 選擇“儲存”或“叢集”（取決於您的環境），選擇“儲存虛擬機器”，然後選擇將包含要使用 ARP 保護的磁碟區的儲存虛擬機器。
2. 導航至“設定”標籤。在「安全性」下，找到「反勒索軟體」磁貼，然後選擇 。
3. 勾選此方塊以啟用反勒索軟體 (ARP)。勾選附加方塊可在儲存虛擬機器中所有符合條件的磁碟區上啟用 ARP。
4. 對於有建議學習期的ONTAP版本，請選擇「學習足夠時間後自動從學習模式切換到活動模式」。這允許 ARP 確定最佳學習間隔並自動切換到主動模式。

CLI

修改現有**SVM**，使其在新磁碟區中預設啟用**ARP**。

選擇 `dry-run`如果您的 `ARP` 版本需要學習週期。否則，請選擇 `enabled`。

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

建立一個新的**SVM**，並預設為新磁碟區啟用**ARP**。

選擇 `dry-run`如果您的 `ARP` 版本需要學習週期。否則，請選擇 `enabled`。

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

修改現有**SVM**，停用自動學習到主動模式的轉換

如果您已從ONTAP 9.13.1 升級到ONTAP 9.15.1，並且預設狀態為 `dry-run`（學習模式），啟用自適應學習，以便進行更改 `enabled`狀態（活動模式）是自動完成的。您可以停用此自動切換功能，以便手動控制所有關聯音量從學習模式切換到活動模式：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

驗證 **ARP** 狀態

```
security anti-ransomware volume show
```

相關資訊

- "在學習期間後切換至使用中模式"
- "安全反勒索軟體卷顯示"

選擇退出 **ONTAP Autonomous Ransomware Protection** 預設啟用狀態

從 ONTAP 9.18.1 開始，對於 AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系統，在升級或全新安裝後的 12 小時預熱期結束後，所有新磁碟區預設自動啟用 Autonomous Ransomware Protection（ARP），前提是已安裝 ARP 授權。您可以在 12 小時寬限期內或之後使用 System Manager 或 ONTAP CLI 選擇停用此預設功能。

現有磁碟區必須"手動啟用"用於 ARP。

關於這項工作

您可以稍後變更此程序所選擇的設定。寬限期過後，您可以隨時靈活地開啟或關閉預設啟用功能：

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false|true
```

步驟

您可以使用 System Manager 或 ONTAP CLI 來管理 ARP 預設啟用選項。

系統管理員

1. 選擇*叢集>設定*。
2. 執行下列其中一項：
   - 在作用中寬限期內停用：
     i. 在「反勒索軟體」部分，您會看到一則訊息，指示啟用 ARP 前剩餘的小時數。選取「不啟用」。
     ii. 在下一個對話方塊中選取 **Disable**，以確認已為新磁碟區關閉預設 ARP 啟用功能。
   - 寬限期過後停用：
     i. 在 **Anti-ransomware** 部分中，選取 。
     ii. 選取核取方塊，然後按一下 **Save** 以停用新磁碟區的預設 ARP 啟用功能。

CLI

1. 檢查預設啟用狀態：

   ```
   security anti-ransomware auto-enable show
   ```

2. 停用新磁碟區的預設啟用：

   ```
   security anti-ransomware auto-enable modify -new-volume-auto-enable
   false
   ```

相關資訊

- "在單一磁碟區啟用 ONTAP 自主勒索軟體防護"

在學習期間之後，在 **ONTAP ARP** 中切換至作用中模式

對於 NAS 環境，手動或自動將啟用 ARP 的磁碟區從學習模式切換到活動模式。如果您在ONTAP 9.15.1 及更早版本中使用 ARP，或在ONTAP 9.17.1 及更早版本的FlexGroup區上執行 ARP，則需要切換模式。

ARP 完成建議至少 30 天的學習模式運作後，您可以手動切換到活動模式。從ONTAP 9.13.1 開始，ARP 會自動確定最佳學習週期間隔並自動切換，切換可能在 30 天之前發生。

如果您將 ARP 與 ARP/AI 保護結合使用，則 ARP 會自動啟動。無需學習期。

> 在現有的磁碟區中、學習和作用中模式僅適用於新寫入的資料、而不適用於磁碟區中現有的資料。不會掃描和分析現有資料、因為在啟用Volume以進行Arp之後、會根據新資料來假設先前一般資料流量的特性。

在學習期間後手動切換至使用中模式

對於ONTAP 9.10.1 至 9.15.1（ONTAP 9.17.1 及更早版本，帶FlexGroup卷），學習期結束後，您可以使用系統管理器或ONTAP CLI 手動將 ARP 學習模式轉換為活動模式。

關於這項工作

本過程中所描述的學習期後手動過渡到主動模式特定於 NAS 環境。

步驟

您可以使用系統管理員或ONTAP CLI 從學習模式切換到主動模式。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取已準備好用於作用中模式的磁碟區。
2. 在 * Volumes * （卷）總覽的 * Security （安全性） * 標籤中，在 Anti-勒索 軟體方塊中選取 * Switch to active mode* （切換至作用中模式）。
3. 您可以在 * 反勒索軟體 * 方塊中驗證磁碟區的 ARP 狀態。

CLI

1. 如果尚未自動完成，則修改受保護的磁碟區以切換到活動模式：

   ```
   security anti-ransomware volume enable -volume <vol_name> -vserver
   <svm_name>
   ```

   您也可以使用modify volume命令切換至作用中模式：

   ```
   volume modify -volume <vol_name> -vserver <svm_name> -anti
   -ransomware-state enabled
   ```

2. 驗證磁碟區的ARP狀態。

   ```
   security anti-ransomware volume show
   ```

自動從學習模式切換至使用中模式

從ONTAP 9.13.1 開始，自適應學習已新增至 ARP 分析中，並且可以自動從學習模式切換到主動模式。 ARP自動從學習模式切換到主動模式的自主決策基於以下選項的配置設定：

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

如果啟用自動切換功能，即使未滿足所有條件，磁碟區也會在最多 30 天後自動切換到活動模式。此 30 天的限制是固定的，無法更改。

如需 ARP 組態選項（包括預設值）的詳細資訊、請參閱 "指令參考資料ONTAP"。

相關資訊

- "安全反勒索軟體量"

了解 SAN 磁碟區的ONTAP ARP 評估期

從ONTAP 9.17.1 開始，ARP 需要一段評估期來確定 SAN 磁碟區工作負載的熵等級是否適合勒索軟體防護。在 SAN 磁碟區上啟用 ARP 後，ARP/AI 會在評估期間主動監控並保護該磁碟區，同時確定最佳加密閾值。在評估期間，可以使用保守閾值進行檢測和發出警報，同時建立基線閾值。會區分評估後的 SAN 磁碟區中適用和不適用的工作負載，如果確定工作負載適合防護，則會根據評估期統計資料自動設定加密閾值。

理解熵評估

系統每隔 10 分鐘收集一次連續的加密統計資料。在評估期間，也會每四小時持續建立一次 ARP 定期快照。如果某個時間間隔內的加密百分比超過了為該磁碟區確定的最佳加密閾值，則會觸發警報，`Anti_ransomware_attack_backup`建立快照，並且任何定期 ARP 快照的快照保留時間都會增加。

確認評估期間有效

您可以執行下列指令，確認評估已啟動，並確認狀態為 `evaluation_period`。如果磁碟區不符合評估條件，則不會顯示評估狀態。

```
security anti-ransomware volume show -vserver <svm_name> -volume
<volume_name>
```

回應範例：

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : evaluation_period
```

監測評估期資料收集

您可以透過執行以下命令來即時監控加密偵測。該命令將傳回一個直方圖，顯示每個加密百分比範圍內的資料量。此直方圖每 10 分鐘更新一次。

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

回應範例：

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

合適的工作負荷和自適應閾值

評估以下列結果之一作結：

- 此工作負載適用於 **ARP**。 ARP會自動將自適應閾值設定為高於評估期間最大加密百分比的 10%。 ARP也會持續收集統計資料並定期建立 ARP 快照。
- 該工作負載不適合 **ARP**。 ARP會自動將自適應閾值設定為評估期間內可見的最大加密百分比。 ARP也會繼續收集統計資料並定期建立 ARP 快照，但係統最終會建議在該磁碟區上停用 ARP。

確定評估結果

評估期結束後，ARP會根據評估結果自動設定自適應閾值。

您可以透過執行以下命令來確定評估結果。卷適用性顯示在 `Block device detection status`場地：

```
security anti-ransomware volume show  -vserver <svm_name> -volume
<volume_name>
```

回應範例：

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

您也可以顯示評估結果所採用的值閾值：

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

回應範例：

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

暫停 ONTAP 自主勒索軟體保護，將工作負載事件排除在分析之外

如果您預期會發生異常的工作負載事件、可以隨時暫停並恢復自發勒索軟體保護（Arp）分析。

從 ONTAP 9.13.1 開始，您可以啟用多重管理驗證（ MAV ），以便需要兩個或多個已驗證的使用者管理員才能暫停 ARP 。

"深入瞭解MAV"。

關於這項工作

在 ARP 暫停期間， ONTAP不會記錄新寫入的事件或操作；但是，對早期日誌的分析會在背景繼續進行。

> 請勿使用 ARP 停用功能來暫停分析。這樣做會停用磁碟區上的Arp、並會遺失所有有關已學習工作負載行為的現有資訊。這需要重新啟動學習期間。

步驟

您可以使用系統管理員或 ONTAP CLI 來暫停 ARP 。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取您要暫停 ARP 的磁碟區。
2. 在卷概覽的「安全性」標籤中，選擇「反勒索軟體」方塊中的「暫停反勒索軟體」。

> 從ONTAP 9.13.1 開始，如果您使用 MAV 來保護 ARP 設置，暫停操作會提示您獲得一個或多個其他管理員的批准。"必須收到所有管理員的核准"與 MAV 審批小組相關，否則操作將會失敗。

3. 若要恢復監控，請選擇*恢復反勒索軟體*。

CLI

1. 在磁碟區上暫停ARP：

```
security anti-ransomware volume pause -vserver <svm_name> -volume
<vol_name>
```

2. 若要繼續處理、請使用 `resume` 命令：

```
security anti-ransomware volume resume -vserver <svm_name> -volume
<vol_name>
```

如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume`資訊，請參閱。

3. 如果您使用 MAV（從ONTAP 9.13.1 開始與 ARP 一起使用）來保護 ARP 設置，則暫停操作會提示您獲得一個或多個其他管理員的批准。必須獲得與 MAV 審批組相關的所有管理員的批准，否則操作將失敗。

   如果您使用的是 MAV 、而預期的暫停作業需要額外核准、則每位 MAV 群組核准者都會執行下列動作：

   a. 顯示要求：

   ```
   security multi-admin-verify request show
   ```

   b. 核准申請：

   ```
   security multi-admin-verify request approve -index[<number
   returned from show request>]
   ```

   最後一個群組核准者的回應表示該磁碟區已修改、而且 ARP 狀態已暫停。

   如果您使用的是 MAV 、而且您是 MAV 群組核准者、您可以拒絕暫停作業要求：

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

+
如"指令參考資料ONTAP"需詳細 `security multi-admin-verify request`資訊，請參閱。

管理 ONTAP 自主勒索軟體保護攻擊偵測參數

從 ONTAP 9.11.1 開始，您可以在啟用自動勒索軟體保護的特定磁碟區上修改勒索軟體偵測的參數，並將已知的激增報告為正常檔案活動。調整偵測參數有助於根據您的特定 Volume 工作負載、提高報告的準確度。

攻擊偵測的運作方式

當自主勒索軟體防護 (ARP) 處於學習或評估模式時，它會為卷宗行為制定基準值。這些基準值包括熵、檔案副檔名以及（從ONTAP 9.11.1 開始的）IOPS。這些基準用於評估勒索軟體威脅。有關這些標準的更多信息，請參閱"ARP 偵測到什麼" 。

不同的資料量和工作負載需要不同的偵測參數。例如，啟用 ARP 的磁碟區可能託管多種類型的檔案副檔名，在這種情況下，您可能需要將從未見過的檔案副檔名的閾值計數修改為大於預設值 20 的數字，或停用基於從未見過的檔案副檔名的警告。從ONTAP 9.11.1 開始，您可以修改攻擊偵測參數，使其更適應您的特定工作負載。

從 ONTAP 9.14.1 開始，您可以在 ARP 觀察到新的副檔名，以及 ARP 建立快照時，設定警示。如需更多資訊、請參閱 [modify-alerts]。

NAS 環境中的攻擊偵測

在 ONTAP 9.10.1 中、如果 ARP 偵測到下列兩種情況、就會發出警告：

- 超過 20 個檔案的副檔名先前未在磁碟區中觀察到
- 高 Entropy 資料

從 ONTAP 9.11.1 開始，如果符合 _ 僅 _ 一個條件， ARP 就會發出威脅警告。例如，如果在 24 小時內觀察到超過 20 個檔案的副檔名，而這些副檔名先前未在磁碟區中觀察到，則 ARP 會將此歸類為威脅（無論觀察到的 Entropy 為何）。24 小時和 20 個檔案值為預設值，可加以修改。

> 若要減少大量誤報，請前往“儲存”>“磁碟區”>“安全性”>“設定工作負載特性”，並停用“監控新檔案類型”。此設定在ONTAP 9.14.1 P7、9.15.1 P1、9.16.1 及更高版本中預設為停用。

SAN 環境中的攻擊偵測

從ONTAP 9.17.1 開始，如果 ARP 偵測到超過自動學習閾值的高加密速率，則會發出警告。此閾值是在"評估期"但可以修改。

修改攻擊偵測參數

根據啟用 ARP 的磁碟區的預期行為，您可能需要修改攻擊偵測參數。

步驟

1. 檢視現有的攻擊偵測參數：

```
security anti-ransomware volume attack-detection-parameters show
-vserver <svm_name> -volume <volume_name>
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                          Vserver Name : vs1
                                           Volume Name : vol1
          Block Device Auto Learned Encryption Threshold : 10
           Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                Is Detection Based on File Create Rate? : true
                Is Detection Based on File Rename Rate? : true
                Is Detection Based on File Delete Rate? : true
          Is Detection Relaxing Popular File Extensions? : true
               High Entropy Data Surge Notify Percentage : 100
                File Create Rate Surge Notify Percentage : 100
                File Rename Rate Surge Notify Percentage : 100
                File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 5
       Never Seen before File Extensions Duration in Hour : 48
```

2. 所有顯示的欄位均可使用布林值或整數值進行修改。若要修改字段，請使用 `security anti-ransomware volume attack-detection-parameters modify`命令。

   如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume attack-detection-parameters modify`資訊，請參閱。

回報已知的突波

即使在作用中， ARP 仍會繼續修改偵測參數的基準值。如果您知道 Volume 活動的突波，一次性突波或是屬於新常態特徵的突波，您應該將它們回報為安全的。手動回報這些突波的安全性、有助於提高 ARP 威脅評估的準確度。

回報一次性突波

1. 如果已知情況下發生一次性喘振、而您希望 ARP 在未來的情況下回報類似的喘振、請清除工作負載行為中的喘振：

```
security anti-ransomware volume workload-behavior clear-surge -vserver
<svm_name> -volume <volume_name>
```

   如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume workload-behavior clear-surge`資訊，請參閱。

修改基準突波

1. 如果回報的喘振應視為正常應用程式行為、請回報喘振、以修改基準喘振值。

```
security anti-ransomware volume workload-behavior update-baseline-from-
surge -vserver <svm_name> -volume <volume_name>
```

詳細了解 `security anti-ransomware volume workload-behavior update-baseline-from-surge`在"指令參考資料ONTAP" 。

設定 **ARP** 警示

從 ONTAP 9.14.1 開始， ARP 可讓您指定兩個 ARP 事件的警示：

- 觀察磁碟區上的新副檔名
- 建立 ARP 快照

這兩個事件的警示可在個別磁碟區或整個 SVM 上設定。如果您啟用 SVM 的警示、則警示設定只會由啟用警示後建立的磁碟區繼承。根據預設、警示不會在任何磁碟區上啟用。

事件警報可透過多管理員驗證進行控制。有關更多信息，請參閱"使用 ARP 保護的磁碟區進行多重管理驗證" 。

步驟

您可以使用系統管理員或ONTAP CLI 設定 ARP 事件警報。

系統管理員

設定磁碟區的警示

1. 導航到“卷”。選擇要修改設定的單一磁碟區。
2. 選擇“安全”選項卡，然後選擇“事件嚴重性設定”。
3. 若要接收「偵測到新檔案副檔名」和「已建立勒索軟體快照」的警報，請選擇「嚴重性」標題下的下拉式功能表。將設定從「不產生事件」修改為「通知」。
4. 選擇*保存*。

設定 **SVM** 的警示

1. 導覽至 儲存虛擬機器，然後選擇要啟用設定的 SVM。
2. 在「安全性」標題下，找到「反勒索軟體」標籤。選擇⋮然後*編輯勒索軟體事件嚴重性*。
3. 若要接收「偵測到新檔案副檔名」和「已建立勒索軟體快照」的警報，請選擇「嚴重性」標題下的下拉式功能表。將設定從「不產生事件」修改為「通知」。
4. 選擇*保存*。

CLI

設定磁碟區的警示

- 若要設定新副檔名的警示：

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-new-file-extension-seen true`
```

- 若要設定建立 ARP 快照的警示：

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-snapshot-copy-creation true
```

- 使用確認您的設定 `anti-ransomware volume event-log show` 命令。

設定 **SVM** 的警示

- 若要設定新副檔名的警示：

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-new-file-extension-seen true
```

- 若要設定建立 ARP 快照的警示：

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-snapshot-copy-creation true
```

- 使用確認您的設定 `security anti-ransomware vserver event-log show` 命令。

詳細了解 `security anti-ransomware vserver event-log`命令"指令參考資料ONTAP" 。

相關資訊

- "瞭解自主勒索軟體保護攻擊和自主勒索軟體保護快照"。
- "指令參考資料ONTAP"

回應 ONTAP ARP 偵測到的異常活動

當自發勒索軟體保護（Arp）偵測到受保護磁碟區中的異常活動時、就會發出警告。您應該評估通知、以判斷該活動是否可接受（誤判）、或攻擊是否看起來惡意。將攻擊分類後，您可以清除可疑檔案的警告和注意事項。

對攻擊進行分類時，ARP 快照要麼在分類作業啟動後保留一段較短的時間（ONTAP 9.16.1 及更高版本），要麼立即刪除（ONTAP 9.15.1 及更早版本）。

從ONTAP 9.11.1 開始，您可以修改"保留設定"用於 ARP 快照。

關於這項工作

當 ARP 偵測到高資料熵、包含資料加密的異常磁碟區活動以及異常檔案副檔名的任意組合時，它會顯示可疑檔案清單。從適用於 NAS 和 SAN 環境的ONTAP 9.17.1 開始，系統管理員中的「反勒索軟體」頁面也會報告熵峰值的詳細資訊。

當發出 ARP 警告通知時，透過以下兩種方式之一指定活動進行回應：

- * 誤判 *

  已識別的文件類型或熵峰值是您的工作負載中預期會出現的，可以忽略。

- * 可能的勒索軟體攻擊 *

  所識別的文件類型或熵峰值在您的工作負載中是意外的，應被視為潛在攻擊。

在您更新您的決定並清除 ARP 通知後，系統將恢復正常監控。 ARP會將您的評估記錄到威脅評估設定檔中，並使用您的選擇來監控後續的檔案活動。

如果是可疑的攻擊、您必須判斷它是否為攻擊、如果是攻擊、請回應、並在清除通知之前還原受保護的資料。 "深入瞭解如何從勒索軟體攻擊中恢復"。

如果您還原整個磁碟區、則沒有要清除的通知。

開始之前

ARP 必須主動保護卷，而不是處於學習或評估模式。

步驟

您可以使用系統管理員或 ONTAP CLI 來回應異常活動。

系統管理員

1. 當您收到「異常活動」通知時，請點擊連結。或者，導覽至「磁碟區」概覽的「安全性」標籤。

   警告會顯示在 * 事件 * 功能表的 * 總覽 * 窗格中。

2. 在「安全」標籤中，查看可疑檔案類型或熵峰值報告。
   - 對於可疑文件，請檢查「可疑文件類型」對話方塊中的每種文件類型，並分別標記。
   - 對於熵峰值，請檢查熵報告。
3. 記錄你的答案：

如果選擇此值…	請採取此行動…
誤判	a. 執行下列其中一項： ◦ 對於文件類型警告，選擇*更新並清除可疑文件類型*。 ◦ 對於熵尖峰，選擇*標記為假陽性*。 這些操作可清除有關可疑文件或活動的警告通知。 ARP隨後將恢復對磁碟區的正常監控。對於ONTAP 9.16.1 及更高版本中的 ARP/AI ，ARP 快照會在分類操作觸發的縮短保留期後自動刪除。對於ONTAP 9.15.1 及更早版本，清除可疑檔案類型後，相關的 ARP 快照會自動刪除。 從ONTAP 9.13.1 開始，如果您使用 MAV 來保護 ARP 設置，清除可疑項目操作會提示您獲得一個或多個其他管理員的批准。"必須收到所有管理員的核准"與 MAV 審批小組相關，否則操作將會失敗。
可能的勒索軟體攻擊	a. 回應攻擊： ◦ 對於文件類型警告，將選定的文件標記為*潛在勒索軟體攻擊*，並"還原受保護的資料" 。 ◦ 對於表示攻擊的熵峰值，選擇「標記為潛在勒索軟體攻擊」並"還原受保護的資料" 。 b. 資料恢復完成後，記錄您的決定並恢復正常的ARP監控： ◦ 對於文件類型警告，選擇*更新並清除可疑文件類型*。 ◦ 對於熵峰值，選擇*標記為潛在勒索軟體攻擊*並選擇*儲存並關閉*。 如果您已還原整個磁碟區，則無需清除任何可疑文件類型通知。 記錄您的決定將清除攻擊報告。對於ONTAP 9.16.1 及更高版本中的 ARP/AI ，ARP 快照會在分類操作觸發的縮短保留期後自動刪除。對於ONTAP 9.15.1 及更早版本，還原磁碟區後，ARP 快照將自動刪除。

CLI

驗證攻擊

1. 當您收到可疑勒索軟體攻擊的通知時、請確認攻擊的時間和嚴重性：

```
security anti-ransomware volume show -vserver <svm_name> -volume
<vol_name>
```

範例輸出：

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 5/12/2025 01:03:23
Number of Attacks: 1
Attack Detected By: encryption_percentage_analysis
```

您也可以檢查EMS訊息：

```
event log show -message-name callhome.arw.activity.seen
```

2. 產生攻擊報告並指定儲存位置：

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

命令範例：

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

範例輸出：

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
"vs0:vol1/"
```

3. 在管理用戶端系統上檢視報告。例如：

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

採取行動

1. 根據您對檔案副檔名或熵峰值的評估，請執行以下操作之一：

   - 誤判

     執行以下命令之一來記錄您的決定並恢復正常的自主勒索軟體防護監控：

     - 對於檔案副檔名：

       ```
       anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> [<extension_identifiers>] -false
       -positive true
       ```

       使用下列選用參數，僅將特定副檔名識別為誤報：

       - `[-extension <text>, … ]`：檔案副檔名

     - 對於熵尖峰：

       ```
       security anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
       HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
       ```

   - 可能的勒索軟體攻擊

     回應攻擊和 "從 ARP 建立的備份快照中恢復資料"。執行以下命令之一記錄您的決定並恢復正常的 ARP 監控：

     - 對於檔案副檔名：

       ```
       anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> [<extension identifiers>] -false
       -positive false
       ```

       請使用下列選用參數，僅將特定的擴充功能識別為可能的勒索軟體：

       - `[-extension <text>, … ]`：檔案副檔名

     - 對於熵尖峰：

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive
false
```

這 `clear-suspect`操作會清除攻擊報告。如果您還原了整個磁碟區，則無需清除任何可疑檔案類型通知。對於ONTAP 9.16.1 及更高版本中的 ARP/AI，ARP 快照會在分類操作觸發的縮短保留期後自動刪除。對於ONTAP 9.15.1 及更早版本，還原磁碟區或清除可疑事件後，ARP 快照會自動刪除。

2. 從 9.18.1 版本開始，您可以確定以下狀態： `clear-suspect`手術：

```
security anti-ransomware volume show -clear-suspect-status -volume
<vol_name> -vserver <svm_name>
```

MAV選項

1. 如果您使用的是 MAV 、而且是預期的 `clear-suspect` 作業需要額外核准、每位 MAV 群組核准者必須：

   a. 顯示要求：

   ```
   security multi-admin-verify request show
   ```

   b. 核准恢復正常反勒索軟體監控的要求：

   ```
   security multi-admin-verify request approve -index[<number
   returned from show request>]
   ```

   最後一個群組核准者的回應表示已修改磁碟區、並記錄誤報。

2. 如果您使用的是 MAV 、而您是 MAV 群組核准者、您也可以拒絕明確可疑的要求：

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

相關資訊

- "NetApp知識庫：了解自主勒索軟體防護攻擊與自主勒索軟體防護快照"
- "修改自動快照選項"
- "安全反勒索軟體量"
- "安全多管理員驗證請求"

在勒索軟體攻擊之後，從 **ONTAP ARP** 快照還原資料

自主勒索軟體防護 (ARP) 會建立快照來防禦潛在的勒索軟體威脅。您可以使用其中一個 ARP 快照或磁碟區的其他快照來還原資料。

關於這項工作

ARP 使用以下前綴名稱之一建立快照：

- `Anti_ransomware_periodic_backup` ：在ONTAP 9.17.1 及更高版本中用於定期建立的快照。例如，`Anti_ransomware_periodic_backup.2025-06-01_1248` 。
- `Anti_ransomware_attack_backup`：在ONTAP 9.17.1 及更高版本中用於回應異常而建立的快照。例如，`Anti_ransomware_attack_backup.2025-08-25_1248` 。
- `Anti_ransomware_backup` ：在ONTAP 9.16.1 及更早版本中，用於為應對異常而建立的快照。例如，`Anti_ransomware_backup.2022-12-20_1248` 。

要從快照中恢復， `Anti_ransomware`快照 辨識出系統攻擊後，必須先釋放ARP快照。

如果沒有報告系統攻擊，您必須先從 `Anti_ransomware`快照，然後從您選擇的快照完成磁碟區的後續還原。

如果受 ARP 保護的磁碟區屬於SnapMirror關係，則從快照還原磁碟區後，您需要手動更新該磁碟區的所有映像副本。如果跳過此步驟，鏡像副本可能會變得不可用，需要刪除並重新建立。

開始之前

"您必須將攻擊標記為潛在的勒索軟體攻擊"從快照恢復資料之前。

步驟

您可以使用System Manager或ONTAP NetApp CLI來還原資料。

系統管理員

系統攻擊後還原

1. 若要從 ARP 快照還原，請跳至步驟二。若要從較早的快照還原，您必須先釋放 ARP 快照的鎖定。
   a. 選擇*儲存>磁碟區*。
   b. 選擇 * 安全 * ，然後 * 檢視可疑的檔案類型 * 。
   c. 將檔案標記為「可能的勒索軟體攻擊」。
   d. 選擇 * 更新 * 和 * 清除可疑檔案類型 * 。
2. 在磁碟區中顯示快照：

   選擇 * 儲存 > Volumes （磁碟區） * 、然後選擇 Volume （磁碟區）和 * Snapshot Copies （ * 快照複本） * 。
3. 選取：您要還原的快照旁的 * 還原 * 。

如果未識別出系統攻擊、請進行還原

1. 在磁碟區中顯示快照：

   選擇 * 儲存 > Volumes （磁碟區） * 、然後選擇 Volume （磁碟區）和 * Snapshot Copies （ * 快照複本） * 。
2. 選擇：然後選擇 `Anti_ransomware`快照。
3. 選擇*還原*。
4. 返回 * Snapshot Copies （快照複本） * 功能表，然後選擇您要使用的快照。選擇*還原*。

CLI

系統攻擊後還原

若要從 ARP 快照還原，請跳至步驟二。若要還原舊版快照的資料，您必須釋放 ARP 快照的鎖定。

> ⓘ 如果您使用的命令如下所述，則只有在從先前的快照還原之前，才需要先釋放反勒索軟體 SnapLock `volume snapshot restore` 。如果您使用 FlexClone ，單一檔案貼齊還原或其他方法還原資料，則不需要這麼做。

1. 將攻擊標記為潛在的勒索軟體攻擊(`-false-positive false` ）並清除可疑文件(`clear-suspect`):

   ```
   anti-ransomware volume attack clear-suspect -vserver <svm_name>
   -volume <vol_name> [<extension identifiers>] -false-positive false
   ```

   使用以下參數之一來識別擴充：

   - `[-seq-no integer]` ：可疑清單中文件的序號。
   - `[-extension text, … ]` ：檔案副檔名
   - `[-start-time date_time -end-time date_time]` ：需要清除的檔案範圍的開始和結束時

間，格式為「MM/DD/YYYY HH:MM:SS」。

2. 列出磁碟區中的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

以下範例顯示中的快照 `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. 從快照還原磁碟區的內容：

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

下列範例還原的內容 `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

如果未識別出系統攻擊、請進行還原

1. 列出磁碟區中的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

以下範例顯示中的快照 `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 從快照還原磁碟區的內容：

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

下列範例還原的內容 `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

如"指令參考資料ONTAP"需詳細 `volume snapshot`資訊，請參閱。

相關資訊

- "NetApp知識庫： ONTAP中的勒索軟體預防與恢復"
- "指令參考資料ONTAP"

調整自動產生的 ARP 快照的設置

從 ONTAP 9 · 11.1 開始，您可以使用 CLI 來控制自動產生的勒索軟體保護（ ARP ）快照保留設定，以因應可疑的勒索軟體攻擊。

開始之前

您只能修改"節點SVM"而不適用於其他類型的 SVM。

步驟

1. 顯示所有目前的 ARP 快照設定：

```
options -option-name arw*
```

2. 顯示選取的目前 ARP 快照設定：

```
options -option-name <arw_setting_name>
```

3. 修改 ARP 快照設定：

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

您可以修改以下設定：

> 從ONTAP 9.17.1 開始，部分所述命令已棄用。 ONTAPONTAP中引入的指令同時支援 NAS 和 SAN 環境。

設定	說明	支援的版本
`arw.snap.max.count`	指定任意給定時間卷中可存在的 ARP 快照的最大數量。系統會刪除較舊的副本，以確保 ARP 快照的總數不會超過此指定限制。	更新版本ONTAP
`arw.snap.create.interval.hours`	指定 ARP 快照之間的間隔（以小時為單位）。當懷疑存在基於資料熵的攻擊且最近建立的 ARP 快照早於指定間隔時，將建立新的 ARP 快照。	更新版本ONTAP
`arw.snap.normal.retain.interval.hours`	指定 ARP 快照的保留時長（以小時為單位）。當 ARP 快照達到保留閾值時，將被刪除。	• ONTAP 9.11.1 升級至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已棄用
`arw.snap.max.retain.interval.days`	指定可以保留 ARP 快照的最長持續時間（以天為單位）。如果磁碟區未回報任何攻擊，則會刪除任何早於此持續時間的 ARP 快照。 > 如果偵測到中度威脅，就會忽略 ARP 快照的最大保留時間間隔。針對威脅所建立的 ARP 快照會保留，直到您回應威脅為止。當您將威脅標示為誤判時， ONTAP 會刪除該磁碟區的 ARP 快照。	• ONTAP 9.11.1 升級至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已棄用

設定	說明	支援的版本
`arw.snap.create.interval.hours.post.max.count`	當磁碟區已包含最大數量的 ARP 快照時，指定 ARP 快照之間的間隔（以小時為單位）。達到最大數量時，將刪除一個 ARP 快照，為新副本騰出空間。使用此選項可以降低新 ARP 快照的建立速度，以保留舊副本。如果磁碟區已包含最大數量的 ARP 快照，則下次建立 ARP 快照時將使用此選項中指定的間隔，而不是 `arw.snap.create.interval.hours` 。	• ONTAP 9.11.1 至 9.16.1 • 在ONTAP 9.17.1 及更高版本中已棄用
`arw.snap.low.encryption.retain.duration.hours`	指定在加密活動較少期間建立的 ARP 快照的保留時間（以小時為單位）。	• ONTAP 9.17.1 及更高版本
`arw.snap.new.extns.interval.hours`	指定偵測到新檔案副檔名時建立 ARP 快照的間隔（以小時為單位）。偵測到新檔案副檔名時會建立一個新的 ARP 快照；上一個在偵測到新檔案副檔名時所建立的快照早於此指定的間隔。在頻繁建立新檔案副檔名的工作負載上，此間隔有助於控制 ARP 快照的頻率。此選項獨立於 `arw.snap.create.interval.hours` ，指定基於資料熵的 ARP 快照的間隔。	• ONTAP 9.11.1 升級至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已棄用
`arw.snap.retain.hours.after.clear.suspect.false.alert`	指定在管理員將攻擊事件標記為誤報後，ARP 快照作為預防措施保留的時間間隔（以小時為單位）。在此預防性保留期到期後，可能會根據選項定義的標準保留期限刪除快照 `arw.snap.normal.retain.interval.hours`和 `arw.snap.max.retain.interval.days` 。	• ONTAP 9.16.1 及更新版本
`arw.snap.retain.hours.after.clear.suspect.real.attack`	指定管理員將攻擊事件標記為真實攻擊後，ARP 快照作為預防措施保留的時間間隔（以小時為單位）。在此預防性保留期到期後，可能會根據選項定義的標準保留期限刪除快照。 `arw.snap.normal.retain.interval.hours`和 `arw.snap.max.retain.interval.days` 。	• ONTAP 9.16.1 及更新版本
`arw.snap.surge.interval.days`	指定為回應 IO 突波而建立的 ARP 快照之間的間隔（以天為單位）。當 IO 流量激增且上次建立的 ARP 快照快照比此指定時間間隔還早時， ONTAP 會建立 ARP 快照突波複本。此選項也會指定 ARP 喘振快照的保留期間（以天為單位）。	更新版本ONTAP
`arw.high.encryption.alert.enabled`	啟用高級別加密警報。當此選項設定為 `on` （預設），當ONTAP百分比超過 `arw.high.encryption.percentage.threshold` 。	ONTAP 9.17.1 及更高版本
`arw.high.encryption.percentage.threshold`	指定卷的最大加密百分比。如果加密百分比超過此閾值，則ONTAP會將加密百分比的增加視為攻擊，並建立 ARP 快照。 `arw.high.encryption.alert.enabled`必須設定為 `on`以使此選項生效。	ONTAP 9.17.1 及更高版本

設定	說明	支援的版本
`arw.snap.high.encryption.retain.duration.hours`	指定在高加密閾值事件期間建立的快照的保留持續時間間隔（以小時為單位）。	ONTAP 9.17.1 及更高版本

4. 如果您在 SAN 環境中使用 ARP，您也可以修改以下評估期設定：

設定	說明	支援的版本
`arw.block_device.auto.learn.threshold.min_value`	指定區塊設備評估的自動學習階段的最小加密閾值百分比值。	ONTAP 9.17.1 及更高版本
`arw.block_device.auto.learn.threshold.max_value`	指定區塊設備評估的自動學習階段的最大加密閾值百分比值。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.min_hours`	指定在設定加密閾值之前評估階段必須運行的最小間隔（以小時為單位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.max_hours`	指定在設定加密閾值之前評估階段必須運行的最大間隔（以小時為單位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	指定在設定加密閾值之前評估階段必須提取的最小資料量（以 GB 為單位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.alert.enabled`	指定是否在區塊設備上啟用 ARP 評估階段的警報。預設值為 `True` 。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.alert.threshold`	指定區塊設備上 ARP 評估階段的閾值百分比。如果加密百分比超過此閾值，則會觸發警報。	ONTAP 9.17.1 及更高版本

相關資訊

- "威脅評估和 ARP 快照"
- "SAN熵評估期"

使用 **AI** （ **ARP/AI** ）更新 **ONTAP** 自主勒索軟體保護

為了隨時掌握最新的勒索軟體威脅防護， ARP/AI 提供在一般 ONTAP 發行時程之外自動更新。

從ONTAP 9.16.1 開始，除系統和韌體更新外，系統管理器軟體下載中還提供 ARP/AI 安全性更新。如果您的ONTAP叢集已註冊"自動系統與韌體更新" ，當 ARP/AI 安全性更新可用時，系統會自動通知您。您也可以更改您的更新偏好以便ONTAP自動安裝安全性更新。

如果您想要手動更新 ARP/AI，可以從 NetApp 支援網站下載更新，然後使用系統管理員進行安裝。

關於這項工作

您只能使用系統管理員更新 ARP/AI。

選取 **ARP/AI** 的更新偏好選項

在系統管理員中，安全文件的啟用自動更新頁面上的設定被設定為 `Show notifications`如果您已註冊自動韌體和系統更新，您可以變更更新設定以 `Automatically update`如果您希望ONTAP自動套用最新更新。如果您使用暗網或希望手動執行更新，您可以選擇顯示通知或自動關閉安全性更新。

開始之前

如需自動安全性更新，請參閱"應啟用 AutoSupport 和 AutoSupport OnDemand ，傳輸傳輸協定應設定為 HTTPS"。

步驟

1. 在 System Manager 中，按一下 * 叢集 > 設定 > 軟體更新 * 。
2. 在 * 軟體更新 * 區段中，選擇 → 。
3. 從 * 軟體更新 * 頁面，選取 * 所有其他更新 * 索引標籤。
4. 選取 * 所有其他更新 * 索引標籤，然後按一下 * 更多 * 。
5. 選取 * 編輯自動更新設定 * 。
6. 從「自動更新設定」頁面，選取 * 安全檔案 * 。
7. 指定要對安全檔案採取的行動（ ARP/AI 更新）。

   您可以選擇自動更新，顯示通知或自動關閉更新。

   若要自動更新安全性更新，應啟用 AutoSupport 和 AutoSupport OnDemand ，並將傳輸通訊協定設定為 HTTPS 。

8. 接受條款與條件、然後選取 * 儲存 * 。

使用最新的安全套件手動更新 **ARP/AI**

視您是否已向 Active IQ Unified Manager 註冊而定，請遵循適當的程序。

請務必僅安裝比目前版本更新的 ARP 更新，以免任何非預期的 ARP 降級。

ONTAP 9 。 **16.1** 及更新版本，搭配數位顧問

1. 在 System Manager 中、前往 * 儀表板 * 。

   在 * 狀況 * 區段中，如果叢集有任何建議的安全性更新，則會顯示一則訊息。

2. 按一下警示訊息。
3. 在建議更新清單中的安全性更新旁，選取 * 動作 * 。
4. 按一下 * 更新 * 立即安裝更新、或按 * 排程 * 排程稍後更新。

   如果已排程更新、您可以 * 編輯 * 或 * 取消 * 。

ONTAP 9 。 16.1 及更新版本，不含數位顧問

1. 瀏覽"NetApp 支援網站"並登入。
2. 完成提示並下載您要用來更新叢集 ARP/AI 的安全套件。
3. 將檔案複製到網路上的 HTTP 或 FTP 伺服器，或複製到可使用 ARP/AI 的叢集可存取的本機資料夾。
4. 在 System Manager 中，按一下 * 叢集 > 設定 > 軟體更新 * 。
5. 在 * 軟體更新 * 中，選取 * 所有其他更新 * 索引標籤。
6. 在 * 手動更新 * 窗格中，按一下 * 新增安全檔案 * ，然後使用下列其中一個偏好設定來新增檔案：
   - * 從伺服器下載 * ：輸入安全檔案套件的 URL 。
   - * 從本機用戶端上傳 * ：瀏覽至下載的 TGZ 檔案。

   請確定檔案名稱以開頭，並具有 `.tgz`副檔名 `ontap_security_file_arpai_`。
7. 按一下 * 新增 * 以套用更新。

驗證 **ARP/AI** 更新

若要檢視已關閉或安裝失敗的自動更新歷程記錄，請執行下列步驟：

1. 在 System Manager 中，按一下 * 叢集 > 設定 > 軟體更新 * 。
2. 在 * 軟體更新 * 區段中，選擇 → 。
3. 在 * 軟體更新 * 頁面中，選取 * 所有其他更新 * 索引標籤，然後按一下 * 更多 * 。
4. 選取 * 檢視所有自動更新 * 。

相關資訊

- "了解ARP/AI"
- "軟體更新的電子郵件訂閱"

使用 VScan 保護病毒

了解 ONTAP Vscan 的防毒配置

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

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。

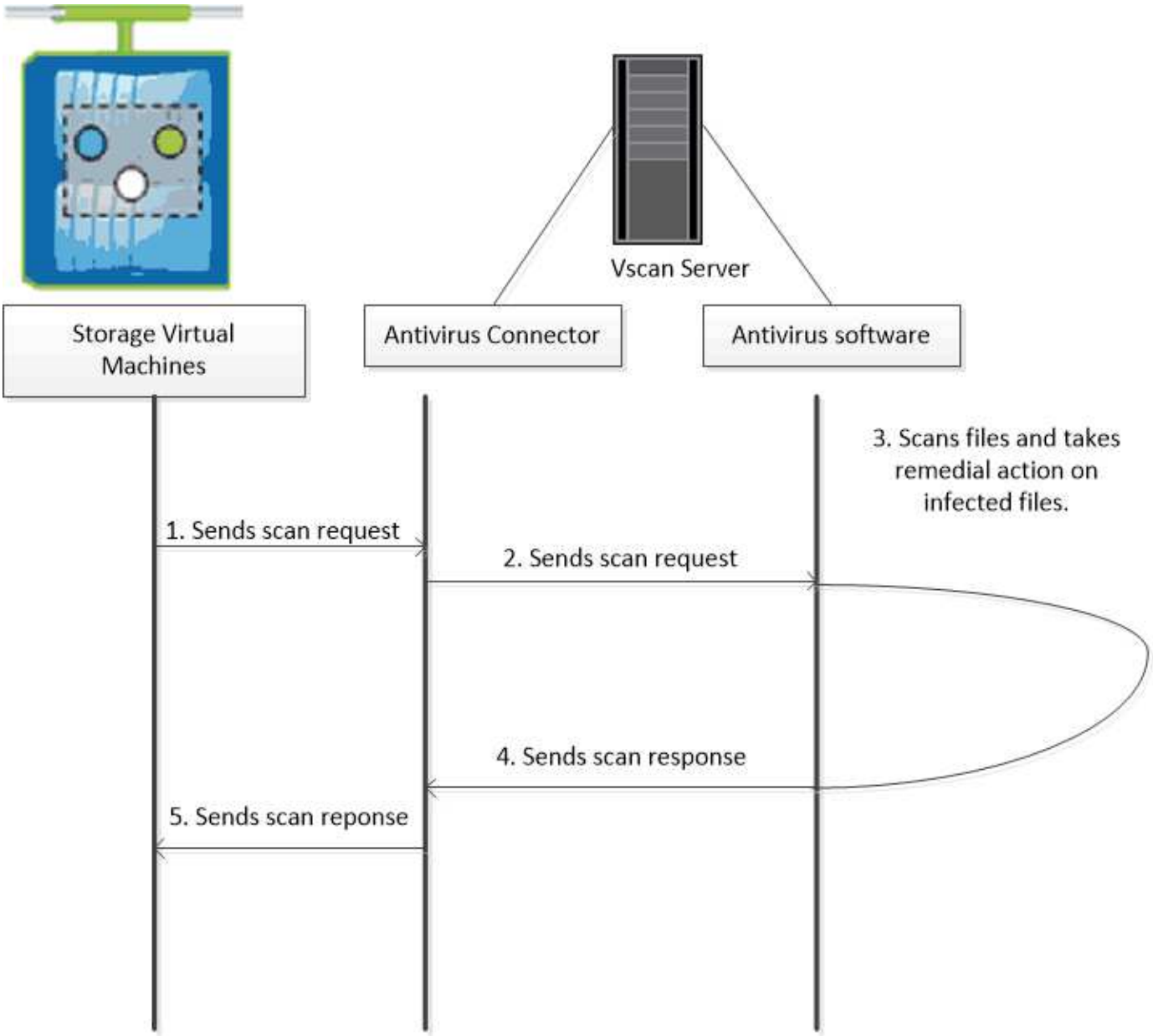
  NFS不支援存取時掃描。

- 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。

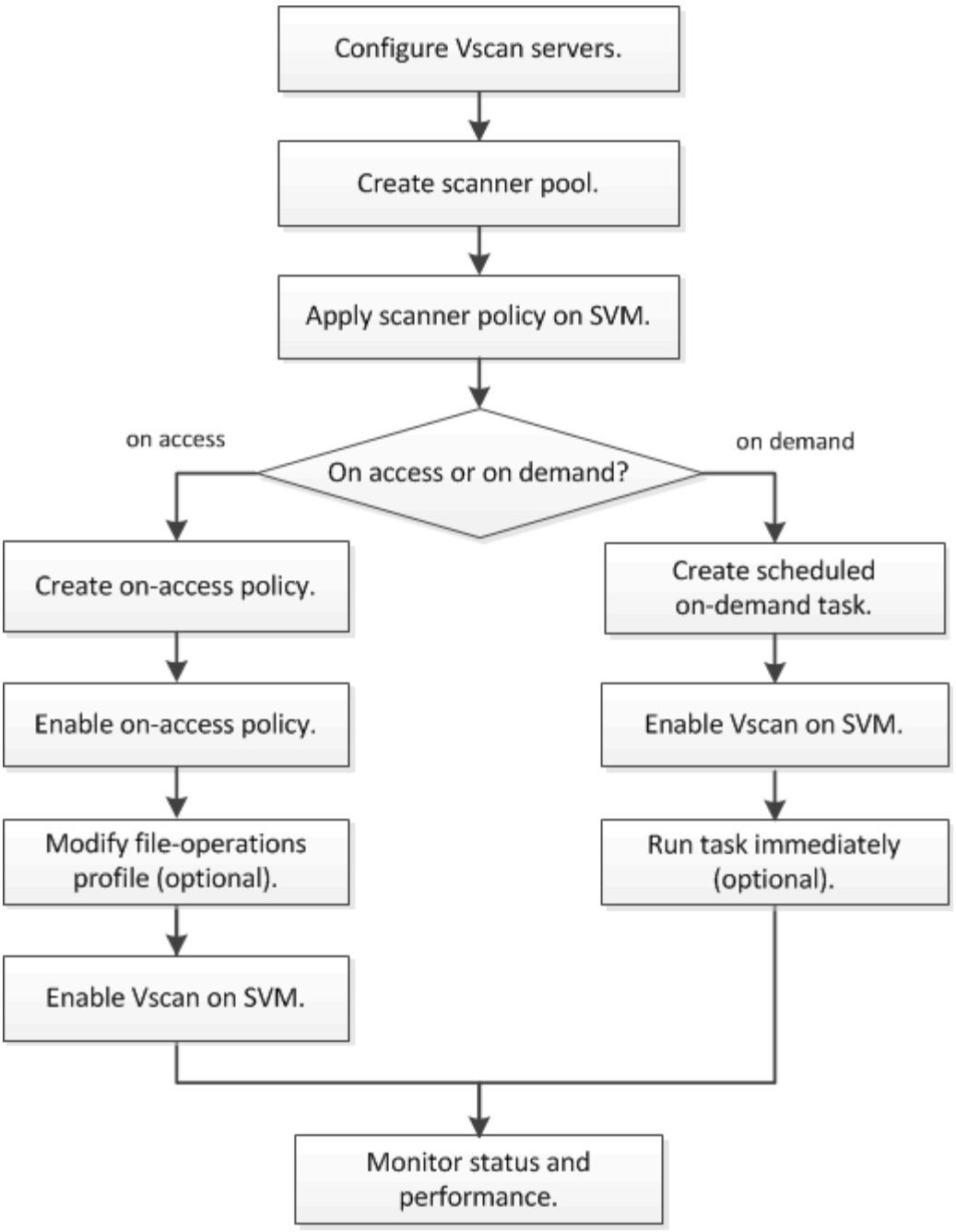
由NetApp提供並安裝在外部伺服器上的《The停止防毒連接器：處理儲存系統與防毒軟體之間的通訊。ONTAP



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。

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 和 Trend Micro 的互通性詳情已在 NetApp 互通性矩陣中列出。Trellix、Deep Instinct 和 OPSWAT 的互通性詳情也可在其合作夥伴網站上找到。Sentinel One、Symantec、Deep Instinct、OPSWAT 和其他新合作夥伴的互通性詳情將由合作夥伴在其網站上提供。

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"	"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
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

VScan伺服器安裝與組態

ONTAP Vscan 伺服器安裝與設定

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、軟體和版本資訊、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 Vscan 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

- 如"VScan 合作夥伴解決方案"需支援的通訊協定、防毒廠商軟體版本、 ONTAP 版本、互通性需求和 Windows 伺服器的相關資訊、請參閱頁面。
- 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 建議使用專用實體機器進行防毒掃描。
- 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 REST API 的角色 `/api/network/ip/interfaces`。
    - 深入瞭解 `security login role create`及 `security login create` "指令參考資料ONTAP"。

> 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"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

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」

瞭解更多關於"建立 LIF"的資訊。

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 Vscan** 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 REST API 的角色 `/api/network/ip/interfaces`。

深入瞭解 `security login role create`及 `security login create` "指令參考資料ONTAP"。

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"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

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. 確保用於簽署NetApp伺服器憑證的 CA 憑證（以及直至根 CA 的任何中間簽章機構）採用 Privacy Enhanced Mail (PEM) 格式，並命名為「Ontap_CA.pem」。將其放置在防毒軟體連接器的安裝目錄中。在ONTAP系統上，將用於在「ONTAP」上為防毒連接器簽署用戶端憑證的 CA 憑證（以及任何中間簽章機構，直到根 CA）安裝為「client-ca」類型的憑證。

設定掃描器資源池

了解如何設定 ONTAP Vscan 掃描器池

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 ONTAP Vscan 掃描器池

掃描器集區會定義VScan伺服器和可連線至SVM的授權使用者。

開始之前

- SVM和VScan伺服器必須位於同一個網域或信任的網域中。
- 使用叢集管理 LIF 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 的網域和使用者名稱。
- 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 cluster_admin_SVM -scanner-pool
   scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 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"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool create`資訊，請參閱。

2. 確認已建立掃描器集區：

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

   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 cluster_admin_SVM
-scanner-pool SP

                                    Vserver: cluster_admin_SVM
                                Scanner Pool: SP
                              Applied Policy: idle
                              Current Status: off
          Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: cluster
        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`命令來檢視叢集上的所有掃描器集區。如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool show`資訊，請參閱。

在 **MetroCluster** 配置中建立 **ONTAP Vscan** 掃描器池

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。

開始之前

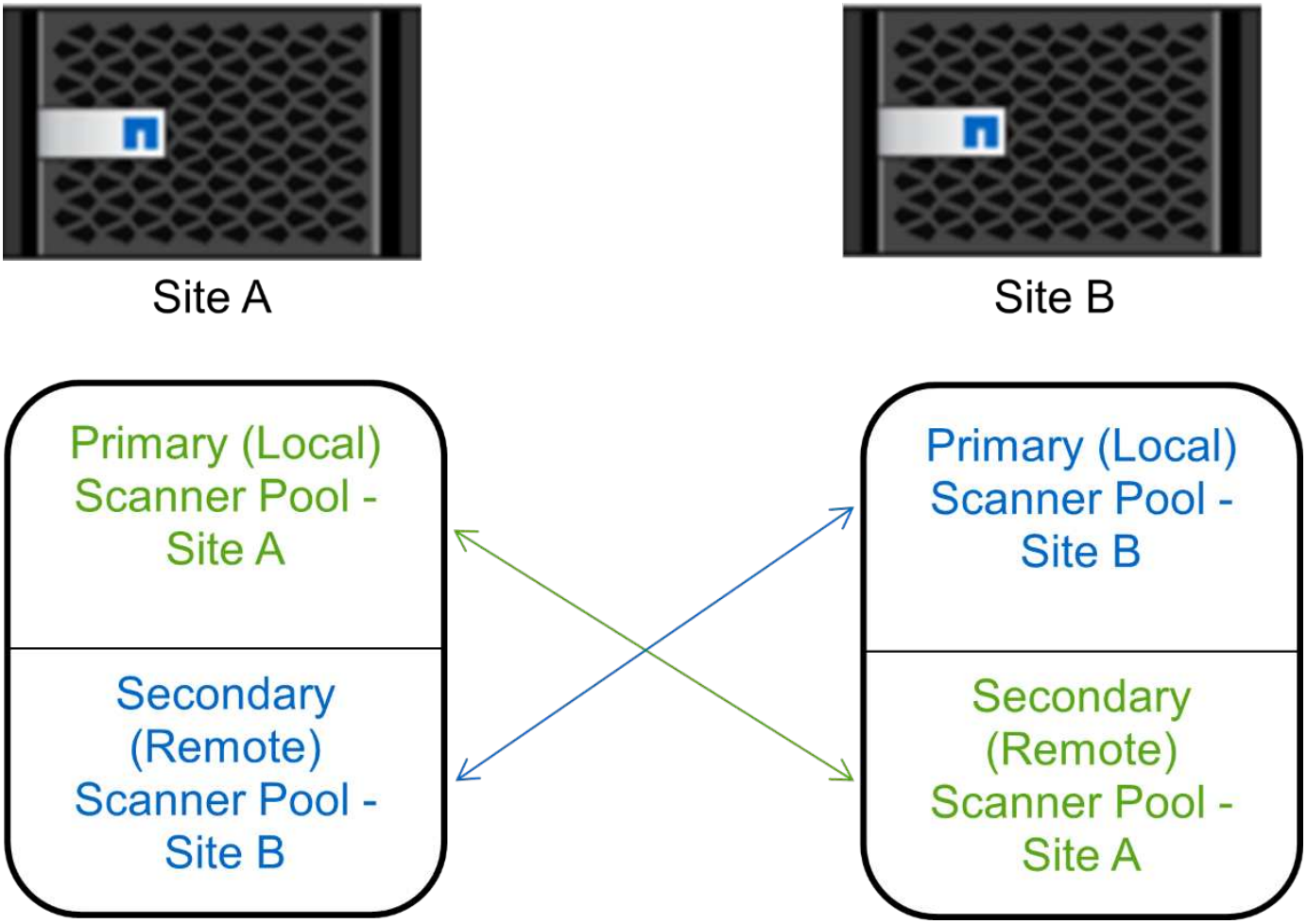
- SVM和VScan伺服器必須位於同一個網域或信任的網域中。
- 針對為個別 SVM 定義的掃描器集區、您必須使用 SVM 管理 LIF 或 SVM 資料 LIF 來設定 ONTAP 防毒連接器。
- 針對叢集中所有 SVM 定義的掃描器集區、您必須使用叢集管理 LIF 來設定 ONTAP 防毒連接器。
- 授權使用者清單必須包含VScan伺服器用來連線至SVM的網域使用者帳戶。
- 設定掃描器集區後、請檢查伺服器的連線狀態。

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"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool create`資訊，請參閱。

   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`*

   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`命令來檢視 SVM 上的所有掃描器集區。如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool show`資訊，請參閱。

使用 **ONTAP Vscan** 在單一叢集上套用掃描器策略

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
   ```

   如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

   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`命令來檢視 SVM 上的作用中掃描器集區。如"指令參

考資料ONTAP"需詳細 `vserver vscan scanner-pool show-active`資訊，請參閱。

在 **MetroCluster ONTAP Vscan** 設定中套用掃描器策略

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
   ```

   如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool apply-policy`資訊，請參閱。

   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"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool show`資訊，請參閱。

   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`命令來檢視 SVM 上的作用中掃描器集區。如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool show-active`資訊，請參閱。

用於管理 **Vscan** 中的掃描器池的 **ONTAP** 指令

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`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

設定存取時掃描

建立 ONTAP Vscan 依存取策略

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。
  - 從 ONTAP 9.14.1 開始、您可以使用萬用字元來指定要排除的存取路徑和副檔名。
- 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"指令參考資料ONTAP"需詳細 `vserver vscan on-access-policy`資訊，請參閱。

   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 **ONTAP Vscan** 依存取策略

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"指令參考資料ONTAP"需詳細 `vserver vscan on-access-policy show`資訊，請參閱。

   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** 共享的 **ONTAP Vscan** 檔案操作設定文件

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

   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
   ```

用於管理按存取原則的 **ONTAP Vscan** 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`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

設定隨需掃描

了解如何設定 **ONTAP Vscan** 按需掃描

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。

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。

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。

使用 **ONTAP Vscan** 建立按需任務

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。
- 從 ONTAP 9.14.1 開始、您可以使用萬用字元來指定要排除的隨需路徑和檔案副檔名。

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"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task create`資訊，請參閱。

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`命令來檢視工作的狀態。您可以使用 `job pause`和 `job resume`命令暫停和重新啟動工作，或使用 `job stop`命令結束工作。如"指令參考資料ONTAP"需詳細 `job`資訊，請參閱。

2. 確認已建立隨選工作：

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

   如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task show`資訊，請參閱。

   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。

使用 **ONTAP Vscan** 安排按需任務

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.
```

如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task schedule`資訊，請參閱。

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；命令會終止工作 `job stop`。如"指令參考資料ONTAP"需詳細 `job`資訊，請參閱。

2. 確認隨選工作已排程：

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

   如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task show`資訊，請參閱。

   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 ONTAP Vscan 按需任務

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.
```

如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task run`資訊，請參閱。

> 您可以使用 `job show`命令來檢視工作的狀態。您可以使用 `job pause`和 `job resume`命令暫停和重新啟動工作，或使用 `job stop`命令結束工作。如"指令參考資料ONTAP"需詳細 `job`資訊，請參閱。

用於管理按需任務的 **ONTAP Vscan** 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`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

在 **ONTAP Vscan** 中配置機外防毒功能的最佳實踐

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"VScan 合作夥伴解決方案"的最佳實務做法、請參閱。

在 SVM ONTAP Vscan 上啟用病毒掃描

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
   ```

   如"指令參考資料ONTAP"需詳細 `vserver vscan enable`資訊，請參閱。

   > 如有必要，您可以使用 `vserver vscan disable`命令來停用病毒掃描。如"指令參考資料ONTAP"需詳細 `vserver vscan disable`資訊，請參閱。

   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"指令參考資料ONTAP"需詳細 `vserver vscan show`資訊，請參閱。

   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 ONTAP Vscan 掃描檔的狀態

有時候，您可能會想要重設 SVM 上已成功掃描檔案的掃描狀態，方法是使用 `vserver vscan reset`命令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。如"指令參考資料ONTAP"需詳細 `vserver vscan reset`資訊，請參閱。

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
   ```

   如"指令參考資料ONTAP"需詳細 `set -privilege advanced`資訊，請參閱。

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
   ```

使用 ONTAP 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
   ```

   如"指令參考資料ONTAP"需詳細 `set`資訊，請參閱。

2. 檢視VScan事件記錄資訊：

```
vserver vscan show-events
```

如"指令參考資料ONTAP"需詳細 `vserver vscan show-events`資訊，請參閱。

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

涉及掃描強制選項的潛在 **ONTAP Vscan** 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。

如"指令參考資料ONTAP"需詳細 `vserver vscan connection-status show`資訊，請參閱。

用於查看 **Vscan** 伺服器連線狀態的 **ONTAP** 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"指令參考資料ONTAP"需詳細 `vserver vscan connection-status show`資訊，請參閱。

排除病毒 **ONTAP Vscan** 掃描故障

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。

相關資訊

- "Vserver vscan掃描程式集區顯示"
- "Vserver vscan存取時原則顯示"

監控 ONTAP Vscan 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"指令參考資料ONTAP"需詳細 `vserver vscan connection-status show`資訊，請參閱。

檢視 VScan 伺服器統計資料

您可以查看 Vscan 伺服器特定的統計信息，以監控效能並診斷與病毒掃描相關的問題。您必須先收集資料樣本，然後才能使用 `statistics show`命令顯示 Vscan 伺服器統計資料。

如"指令參考資料ONTAP"需詳細 `statistics show`資訊，請參閱。

若要完成資料範例、請完成下列步驟：

步驟

1. 執行 `statistics start`命令和選用命令 `statistics stop`。

   詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

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. 使用下列計數器執行 `statistics show -object offbox_vscan –instance SVM`命令：

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
---------------------------------------------------------------
```

相關資訊

- "指令參考資料ONTAP"

稽核SVM上的NAS事件

瞭解如何針對 SMB 和 NFS 傳輸協定使用 ONTAP 來稽核檔案存取

您可以搭配ONTAP 使用適用於SMB和NFS傳輸協定的檔案存取稽核功能、例如使用FPolicy進行原生稽核和檔案原則管理。

在下列情況下、您應該設計及實作SMB與NFS檔案存取事件的稽核：

- 已設定基本的SMB和NFS傳輸協定檔案存取。
- 您想要使用下列其中一種方法來建立及維護稽核組態：
  - 原生ONTAP 的功能
  - 外部FPolicy伺服器

稽核SVM上的NAS事件

稽核NAS事件是一項安全性措施、可讓您追蹤及記錄儲存虛擬機器（SVM）上的特定SMB和NFS事件。這有助於您追蹤潛在的安全問題、並提供任何安全漏洞的證據。您也可以登錄及稽核Active Directory集中存取原則、以瞭解實作原則的結果。

SMB 活動

您可以稽核下列事件：

- SMB檔案與資料夾存取事件

  您可以稽核儲存在FlexVol 包含啟用稽核功能之SVM的物件上的SMB檔案和資料夾存取事件。

- SMB登入和登出事件

  您可以稽核SVM上SMB伺服器的SMB登入和登出事件。

- 集中存取原則執行事件

  您可以使用透過建議的集中存取原則套用的權限、來稽核SMB伺服器上物件的有效存取。透過集中存取原則的暫存進行稽核、可讓您在部署中央存取原則之前、先瞭解其影響。

  使用Active Directory GPO設定集中存取原則暫存稽核；不過、SVM稽核組態必須設定為稽核集中存取原則暫存事件。

  雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。

NFS 事件

您可以利用NFSv4 ACL來稽核儲存在SVM上的物件、以稽核檔案和目錄事件。

稽核的運作方式

瞭解 ONTAP 的基本稽核概念

若要瞭解ONTAP 功能性稽核、您應該瞭解一些基本的稽核概念。

- 暫存檔案

  在合併與轉換之前、會儲存稽核記錄的個別節點上的中間二進位檔案。暫存檔案包含在暫存磁碟區中。

- 暫存磁碟區

  由支援儲存暫存檔案的功能所建立的專屬Volume ONTAP 。每個Aggregate有一個接移磁碟區。執行磁碟區由所有啟用稽核的儲存虛擬機器（SVM）共享、以儲存資料磁碟區在該特定集合體中的資料存取稽核記錄。每個SVM的稽核記錄都儲存在暫存磁碟區內的個別目錄中。

  叢集管理員可以檢視暫存磁碟區的相關資訊、但不允許執行其他大部分的Volume作業。只ONTAP 有能夠建立暫存磁碟區。自動為暫存磁碟區指派名稱。ONTAP所有暫存磁碟區名稱都以開頭 `MDV_aud_` 接著是包含該暫存磁碟區的集合的 UUID （例如： `MDV_aud_1d0131843d4811e296fc123478563412`）

- 系統磁碟區

  包含特殊中繼資料（例如檔案服務稽核記錄的中繼資料）的Some Volume。FlexVol管理SVM擁有整個叢集可見的系統磁碟區。接移磁碟區是一種系統磁碟區。

- 整合工作

  啟用稽核時建立的工作。這項在每個SVM上長期執行的工作、會將稽核記錄從SVM成員節點上的暫存檔案中

移出。此工作會依照時間順序合併稽核記錄、然後將其轉換成稽核組態中指定的使用者可讀取事件記錄格式（無論是evtx或XML檔案格式）。轉換後的事件記錄會儲存在SVM稽核組態中指定的稽核事件記錄目錄中。

瞭解 **ONTAP** 稽核程序的功能

這個不一樣的稽核程序與Microsoft稽核程序不同。ONTAP在您設定稽核之前、您應該先瞭解ONTAP 不稽核程序的運作方式。

稽核記錄一開始會儲存在個別節點上的二進位暫存檔案中。如果在SVM上啟用稽核、則每個成員節點都會維護該SVM的暫存檔案。這些記錄會定期整合並轉換成使用者可讀取的事件記錄、這些記錄會儲存在SVM的稽核事件記錄目錄中。

在**SVM**上啟用稽核的程序

稽核只能在SVM上啟用。當儲存管理員在SVM上啟用稽核時、稽核子系統會檢查暫存磁碟區是否存在。每個包含SVM擁有之資料磁碟區的Aggregate都必須存在暫存Volume。稽核子系統會建立任何必要的暫存磁碟區（如果不存在）。

稽核子系統也會在啟用稽核之前完成其他必要工作：

- 稽核子系統會驗證記錄目錄路徑是否可用、而且不包含symlink。

  記錄目錄必須已存在於SVM命名空間內的路徑中。建議您建立新的Volume或qtree來保存稽核記錄檔。稽核子系統不會指派預設的記錄檔位置。如果稽核組態中指定的記錄目錄路徑不是有效路徑、則稽核組態建立會失敗 `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` 錯誤。

  如果目錄存在但包含symlink、則組態建立會失敗。

- 稽核會排程整合工作。

  排程此工作之後、就會啟用稽核。SVM稽核組態和記錄檔會在重新開機時持續存在、或者NFS或SMB伺服器會停止或重新啟動。

事件記錄整合

記錄整合是一項排程工作、會在停用稽核之前、定期執行。停用稽核時、整合工作會驗證是否已合併所有剩餘的記錄。

保證稽核

依預設、稽核是保證的。此功能可確保記錄所有可稽核的檔案存取事件（如設定的稽核原則ACL所指定）、即使節點無法使用亦然。ONTAP在將該作業的稽核記錄儲存至持續儲存設備上的暫存磁碟區之前、無法完成要求的檔案作業。如果稽核記錄無法提交至暫存檔案中的磁碟、無論是因為空間不足或其他問題、用戶端作業都會遭到拒絕。

系統管理員或具有權限層級存取權的帳戶使用者、可以使用NetApp Manageability SDK或REST API來略過檔案稽核記錄作業。您可以檢閱儲存在中的命令記錄檔、判斷是否已使用 NetApp Manageability SDK 或 REST API 執行任何檔案動作 `audit.log` 檔案：

如需命令歷程記錄稽核記錄的詳細資訊、請參閱中的「管理管理管理活動的稽核記錄」一節 "系統管理"。

節點無法使用時的整合程序

如果包含屬於已啟用稽核之SVM的磁碟區的節點無法使用、則稽核整合工作的行為取決於節點的儲存容錯移轉（SFO）合作夥伴（或是雙節點叢集的HA合作夥伴）是否可用：

- 如果接移磁碟區可透過SFO合作夥伴取得、則會掃描上次從節點回報的接移磁碟區、並正常進行整合。
- 如果無法取得SFO合作夥伴、工作會建立部分記錄檔。

  當節點無法連線時、整合工作會整合該SVM其他可用節點的稽核記錄。為了識別尚未完成、工作會新增後置字元 `.partial` 合併的檔案名稱。

- 當無法使用的節點可用之後、該節點中的稽核記錄會與當時來自其他節點的稽核記錄合併。
- 所有稽核記錄都會保留下來。

事件記錄檔循環

稽核事件記錄檔會在達到設定的臨界值記錄大小或已設定的排程時進行旋轉。當事件記錄檔旋轉時、排程的整合工作會先將作用中的轉換檔重新命名為具有時間戳記的歸檔檔檔、然後建立新的作用中轉換事件記錄檔。

在**SVM**上停用稽核的程序

在SVM上停用稽核時、整合工作會最後觸發一次。所有未處理、記錄的稽核記錄都會以使用者可讀取的格式記錄。在SVM上停用稽核且可供檢視時、不會刪除儲存在事件記錄目錄中的現有事件記錄。

合併該SVM的所有現有暫存檔案之後、整合工作就會從排程中移除。停用SVM的稽核組態不會移除稽核組態。儲存管理員可以隨時重新啟用稽核。

稽核整合工作會在啟用稽核時建立、可監控整合工作、並在整合工作因錯誤而結束時重新建立。使用者無法刪除稽核整合工作。

ONTAP 稽核的必要條件

在儲存虛擬機器（SVM）上設定及啟用稽核之前、您必須瞭解特定的需求和考量。

- NFS 和 S3 稽核啟用 SVM 的合併限制取決於您的 ONTAP 版本：

版本ONTAP	最大值
9.8 及更早版本	50
9.9.1及更新版本	400

- 稽核不受限於SMB或NFS授權。

即使叢集上未安裝SMB與NFS授權、您仍可設定及啟用稽核。

- NFS稽核支援安全性ACE（類型U）。
- 對於NFS稽核、模式位元與稽核ACE之間沒有對應關係。

  將ACL轉換為模式位元時、會跳過稽核ACE。將模式位元轉換為ACL時、不會產生稽核ACE。

- 稽核組態中指定的目錄必須存在。

  如果不存在、建立稽核組態的命令就會失敗。

- 稽核組態中指定的目錄必須符合下列需求：
  - 目錄不得包含符號連結。

    如果稽核組態中指定的目錄包含符號連結、建立稽核組態的命令就會失敗。

  - 您必須使用絕對路徑來指定目錄。

    您不應指定相對路徑、例如 `/vs1/../`。

- 稽核取決於暫存磁碟區中是否有可用空間。

  您必須瞭解並制定計畫、確保集合體中含有稽核磁碟區的暫存磁碟區有足夠的空間。

- 稽核取決於磁碟區中是否有可用空間、其中包含儲存轉換事件記錄的目錄。

  您必須注意並制定計畫、確保用於儲存事件記錄的磁碟區有足夠的空間。您可以使用指定要保留在稽核目錄中的事件記錄數目 `-rotate-limit` 建立稽核組態時的參數、有助於確保磁碟區中有足夠的可用空間用於事件記錄。

- 雖然您可以在稽核組態中啟用集中存取原則接移、而不需在SMB伺服器上啟用動態存取控制、但必須啟用動態存取控制、才能產生集中存取原則接移事件。

  預設不會啟用動態存取控制。

啟用稽核時的**Aggregate space**考量

建立稽核組態並在叢集中至少一個儲存虛擬機器（SVM）上啟用稽核時、稽核子系統會在所有現有的集合體和所有建立的新集合體上建立暫存磁碟區。在叢集上啟用稽核時、您必須注意特定的Aggregate空間考量。

由於Aggregate中的空間不可用、所以暫存磁碟區建立可能會失敗。如果您建立稽核組態、而現有的Aggregate沒有足夠的空間來容納接移磁碟區、就可能發生這種情況。

在SVM上啟用稽核之前、您應該先確定現有集合體上有足夠的空間可用於暫存磁碟區。

限制 **ONTAP** 稽核記錄的暫存檔案大小

暫存檔案上的稽核記錄大小不得大於32 KB。

發生大型稽核記錄時

在下列其中一種情況下、在管理稽核期間可能會發生大量的稽核記錄：

- 新增或刪除具有大量使用者之群組的使用者。
- 新增或刪除檔案共用區上的檔案共用存取控制清單（ACL）、以供大量的檔案共用使用者使用。
- 其他案例。

停用管理稽核以避免此問題。若要這麼做、請修改稽核組態、並從稽核事件類型清單中移除下列項目：

- 檔案共用
- 使用者帳戶
- 安全性群組
- 授權原則變更

  移除之後、檔案服務稽核子系統不會稽核這些檔案。

稽核記錄過大的影響

- 如果稽核記錄的大小過大（超過32 KB）、則不會建立稽核記錄、稽核子系統會產生類似下列的事件管理系統（EMS）訊息：

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  如果保證稽核、則檔案作業會因為無法建立稽核記錄而失敗。

- 如果稽核記錄的大小超過9、999個位元組、則會顯示與上述相同的EMS訊息。系統會建立部分稽核記錄、但缺少較大的金鑰值。
- 如果稽核記錄超過2、000個字元、則會顯示下列錯誤訊息、而非實際值：

  ```
  The value of this field was too long to display.
  ```

瞭解 ONTAP 稽核事件記錄的支援格式

已轉換的稽核事件記錄檔支援的檔案格式為 EVTX 和 XML 檔案格式。

您可以在建立稽核組態時指定檔案格式的類型。根據預設、 ONTAP 會將二進位記錄轉換成 EVTX 檔案格式。

檢視及處理 ONTAP 稽核事件記錄

您可以使用稽核事件記錄來判斷是否有足夠的檔案安全性、以及是否有不當的檔案和資料夾存取嘗試。您可以檢視及處理儲存在中的稽核事件記錄 EVTX 或 XML 檔案格式。

- EVTX 檔案格式

您可以開啟已轉換的 EVTX 使用 Microsoft 事件檢視器將事件記錄稽核為儲存的檔案。

使用「事件檢視器」檢視事件記錄時、您可以使用兩種選項：

- 一般檢視

  所有事件的通用資訊都會顯示在事件記錄中。在此版本ONTAP 的資訊不顯示事件記錄的事件特定資料。您可以使用詳細檢視來顯示特定事件的資料。

- 詳細檢視

  提供友善的檢視和XML檢視。易記檢視和XML檢視會同時顯示所有事件通用的資訊、以及事件記錄的事件特定資料。

- XML 檔案格式

  您可以檢視及處理 XML 稽核支援的協力廠商應用程式上的事件記錄 XML 檔案格式。XML檢視工具可用於檢視稽核記錄、前提是您必須具備XML架構和XML欄位定義的相關資訊。如需XML架構和定義的詳細資訊、請參閱 "《稽核架構參考》ONTAP"。

使用事件檢視器檢視作用中稽核記錄的方式

如果稽核整合程序正在叢集上執行、則整合程序會將新記錄附加到啟用稽核的儲存虛擬機器（SVM）作用中稽核記錄檔。此作用中稽核記錄可透過Microsoft事件檢視器中的SMB共用區存取及開啟。

除了檢視現有的稽核記錄之外、「事件檢視器」還提供重新整理選項、可讓您重新整理主控台視窗中的內容。新附加的記錄是否可在事件檢視器中檢視、取決於是否在用來存取作用中稽核記錄的共用區上啟用oplocks。

共享區上的oplocks設定	行為
已啟用	「事件檢視器」會開啟記錄、其中包含寫入到該時間點的事件。重新整理作業不會以合併程序附加的新事件來重新整理記錄。
已停用	「事件檢視器」會開啟記錄、其中包含寫入到該時間點的事件。重新整理作業會以合併程序附加的新事件來重新整理記錄。

此資訊僅適用於 EVTX 事件記錄。 XML 事件記錄可以透過 SMB 瀏覽器或 NFS 、使用任何 XML 編輯器或檢視器來檢視。

可稽核的SMB事件

瞭解 **ONTAP** 可稽核以解讀結果的 **SMB** 事件

可稽核特定的SMB事件、包括特定檔案和資料夾存取事件、特定登入和登出事件、以及集中存取原則暫存事件。ONTAP瞭解哪些存取事件可以稽核、有助於解讀事件記錄的結果。

可以審核以下附加 SMB 事件：

事件ID（EVT/evtx）	活動	說明	類別

4670	物件權限已變更	物件存取：權限已變更。	檔案存取
4907	物件稽核設定已變更	物件存取：稽核設定已變更。	檔案存取
4913.	物件中心存取原則已變更	物件存取：CAP已變更。	檔案存取

下列SMB事件ONTAP 可在下列版本中透過下列功能進行稽核：

事件ID（EVT/evtx）	活動	說明	類別
540/4624	帳戶已成功登入	登入/登出：網路（SMB）登入。	登入與登出
598/4625	帳戶無法登入	登入/登出：不明的使用者名稱或錯誤的密碼。	登入與登出
530/4625	帳戶無法登入	登入/登出：帳戶登入時間限制。	登入與登出
531/4625	帳戶無法登入	登入/登出：帳戶目前已停用。	登入與登出
532/4625	帳戶無法登入	登入/登出：使用者帳戶已過期。	登入與登出
533/4625	帳戶無法登入	登入/登出：使用者無法登入此電腦。	登入與登出
534/4625	帳戶無法登入	登入/登出：使用者未在此授予登入類型。	登入與登出
535/4625	帳戶無法登入	登入/登出：使用者密碼已過期。	登入與登出
537-4625	帳戶無法登入	登入/登出：登入失敗的原因並非上述原因。	登入與登出
5310/4625	帳戶無法登入	登入/登出：帳戶已鎖定。	登入與登出
538/4634	帳戶已登出	登入/登出：本機或網路使用者登出。	登入與登出
560/ 4656	開啟物件/建立物件	物件存取：物件（檔案或目錄）開啟。	檔案存取
563/4659	開啟要刪除的物件	物件存取：要求物件（檔案或目錄）的控點、目的是刪除。	檔案存取

564/4660	刪除物件	物件存取：刪除物件（檔案或目錄）。當Windows用戶端嘗試刪除物件（檔案或目錄）時、會產生此事件。ONTAP	檔案存取
567/4663	讀取物件/寫入物件/取得物件屬性/設定物件屬性	物件存取：物件存取嘗試（讀取、寫入、取得屬性、設定屬性）。 附註： ONTAP 針對此活動、僅針對物件上的第一個SMB讀取和第一個SMB寫入作業（成功或失敗）進行不稽核。這可防止ONTAP 在單一用戶端開啟物件並對同一個物件執行多次連續的讀取或寫入作業時、造成過多的記錄項目。	檔案存取
NA/4664	硬式連結	物件存取：嘗試建立硬式連結。	檔案存取
NA/4818	建議的集中存取原則並未授予與目前集中存取原則相同的存取權限	物件存取：集中存取原則Staging。	檔案存取
NA/ NA Data ONTAP 不適用事件ID 9999	重新命名物件	物件存取：物件已重新命名。這是一個不確定的事件。ONTAPWindows目前不支援將它當成單一事件。	檔案存取
NA/ NA Data ONTAP 不景事件ID 9998	取消連結物件	物件存取：物件未連結。這是一個不確定的事件。ONTAPWindows目前不支援將它當成單一事件。	檔案存取

活動**4656**的其他相關資訊

。 `HandleID` 稽核中的標記 `XML` 事件包含所存取物件（檔案或目錄）的處理方式。。 `HandleID` evtx 4656 事件的標記包含不同的資訊、取決於開啟的事件是用於建立新物件或開啟現有物件：

- 如果開啟的事件是建立新物件（檔案或目錄）的開放式要求、則 `HandleID` 稽核 XML 事件中的標記顯示為空白 `HandleID` （例如： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>` ）。

  。 `HandleID` 為空白、因為在實際物件建立之前和處理代碼存在之前、會先稽核開啟（用於建立新物件）的要求。相同物件的後續稽核事件在中具有適當的物件控點 `HandleID` 標記。

- 如果開啟的事件是開啟現有物件的開放式要求、則稽核事件會在中指派該物件的處理代碼 `HandleID` 標記（例如： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>` ）。

決定 **ONTAP** 稽核物件的完整路徑

列印在中的物件路徑 `<ObjectName>` 稽核記錄的標記包含磁碟區名稱（以括弧括住）、以及包含磁碟區根目錄的相對路徑。如果您想要判斷稽核物件的完整路徑（包括交會路徑

）、您必須採取某些步驟。

步驟

1. 請查看、判斷哪些磁碟區名稱和受稽核物件的相對路徑 `<ObjectName>` 稽核事件中的標記。

   在此範例中、磁碟區名稱為「 data1 」、檔案的相對路徑為 `/dir1/file.txt`：

   ```
   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
   ```

2. 使用上一步驟所決定的磁碟區名稱、判斷包含稽核物件之磁碟區的交會路徑：

   在此範例中、磁碟區名稱為「 data1 」、而包含稽核物件之磁碟區的交會路徑為 `/data/data1`：

   ```
   volume show -junction -volume data1
   ```

   ```
                                  Junction                       Junction
   Vserver   Volume       Language Active    Junction Path      Path Source
   --------- ------------ -------- --------  ------------------ -----------
   vs1       data1        en_US.UTF-8
                                  true      /data/data1        RW_volume
   ```

3. 附加在中找到的相對路徑、以決定稽核物件的完整路徑 `<ObjectName>` 標記為磁碟區的交會路徑。

   在此範例中、磁碟區的交會路徑為：

   ```
   /data/data1/dir1/file.text
   ```

瞭解 **ONTAP** 對符號連結和硬式連結的稽核

稽核symlink和硬式連結時、必須謹記某些考量事項。

稽核記錄包含所稽核物件的相關資訊、包括中所識別的已稽核物件路徑 `ObjectName` 標記。您應該瞭解 symlinks 和硬式連結的路徑如何記錄在中 `ObjectName` 標記。

symlinks

symlink是一個具有獨立inode的檔案、其中包含指向目的地物件（稱為目標）位置的指標。透過symlink存取物件時ONTAP 、流通會自動解譯symlink、並遵循實際規範的非規範傳輸協定路徑、前往磁碟區中的目標物件。

在下列範例輸出中、有兩個 symlink 、兩者都指向一個名為的檔案 `target.txt`。其中一個symlink是相對symlink、一個是絕對symlink。如果稽核其中任一符號連結、則為 `ObjectName` 稽核事件中的標記包含檔案路徑 `target.txt`：

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

硬式連結

硬式連結是指將名稱與檔案系統上現有檔案相關聯的目錄項目。硬式連結指向原始檔案的inode位置。如同用什麼方式解譯symlinks、它會解譯硬式連結、並遵循實際規範路徑前往Volume中的目標物件。ONTAP ONTAP稽核硬式連結物件的存取時、稽核事件會在中記錄這條絕對規範路徑 `ObjectName` 標記而非硬連結路徑。

瞭解替代 **NTFS** 資料串流的 **ONTAP** 稽核

在使用NTFS替代資料流稽核檔案時、您必須謹記某些考量事項。

要稽核的物件位置會使用兩個標籤（即）記錄在事件記錄中 `ObjectName` 標記（路徑）和 `HandleID` 標記（控點）。若要正確識別正在記錄的串流要求、您必須知道ONTAP 這些欄位中有哪些資料流是NTFS替代資料串流的佐證記錄：

- evtxID：4656個事件（開啟並建立稽核事件）
  - 替代資料串流的路徑會記錄在中 `ObjectName` 標記。
  - 替代資料串流的處理方式會記錄在中 `HandleID` 標記。
- evtxID：4663個事件（所有其他稽核事件、例如讀取、寫入、getattr等）
  - 基礎檔案的路徑、而非替代資料串流、會記錄在中 `ObjectName` 標記。
  - 替代資料串流的處理方式會記錄在中 `HandleID` 標記。

範例

下列範例說明如何使用識別 evtx ID ： 4663 個事件以用於替代資料串流 `HandleID` 標記。即使是 `ObjectName` 在讀取稽核事件中記錄的標記（路徑）位於基礎檔案路徑 `HandleID` 標記可用於將事件識別為替代資料串流的稽核記錄。

串流檔案名稱採用格式 `base_file_name:stream_name`。在此範例中 `dir1` 目錄包含基礎檔案、具有下列路徑的替代資料串流：

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

下列事件範例中的輸出會如所示被刪減；輸出不會顯示事件的所有可用輸出標記。

對於 evtx ID 4656 （開放式稽核事件）、替代資料串流的稽核記錄輸出會在中記錄替代資料串流名稱 `ObjectName` 標記：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

對於 evtx ID 4663 （讀取稽核事件）、相同替代資料串流的稽核記錄輸出會在中記錄基礎檔案名稱 `ObjectName` 標記；不過、中的控點 `HandleID` 標記是替代資料串流的處理方式、可用於將此事件與替代資料串流建立關聯：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

瞭解 **ONTAP** 對 **NFS** 檔案和目錄存取事件的稽核

可以稽核某些NFS檔案和目錄存取事件。ONTAP瞭解哪些存取事件可稽核、有助於解讀轉換後的稽核事件記錄結果。

您可以稽核下列NFS檔案和目錄存取事件：

- 讀取
- 開啟
- 關閉
- readdir
- 寫入
- 設定
- 建立
- 連結
- OPENATTR
- 移除
- GetAttr
- 驗證
- n驗證
- 重新命名

若要可靠地稽核NFS重新命名事件、您應該在目錄上設定稽核ACE、而不要在檔案上設定、因為如果目錄權限足夠、就不會檢查檔案權限來執行重新命名作業。

規劃 **ONTAP VM** 上的稽核組態

在儲存虛擬機器（SVM）上設定稽核之前、您必須先瞭解可用的組態選項、並針對每個選項規劃您要設定的值。此資訊可協助您設定稽核組態、以滿足您的業務需求。

所有稽核組態都有一些通用的組態參數。

此外、您也可以使用某些參數來指定在旋轉合併和轉換的稽核記錄時使用哪些方法。您可以在設定稽核時指定下列三種方法之一：

- 根據記錄大小來旋轉記錄

  這是用來旋轉記錄的預設方法。

- 根據排程來旋轉記錄
- 根據記錄大小和排程來旋轉記錄（以先發生的事件為準）

至少應設定一種記錄輪調方法。

所有稽核組態的通用參數

建立稽核組態時、必須指定兩個必要參數。您也可以指定三個選用參數：

資訊類型	選項	必要	包括	您的價值

*SVM*名稱 要在其中建立稽核組態的SVM名稱。SVM必須已經存在。	`-vserver vserver_name`	是的	是的	
記錄目的地路徑 指定儲存已轉換稽核記錄的目錄、通常是專屬磁碟區或qtree。路徑必須已存在於SVM命名空間中。 路徑長度最多可達864個字元、且必須具有讀寫權限。 如果路徑無效、稽核組態命令就會失敗。 如果SVM是SVM災難恢復來源、則記錄目的地路徑無法位於根磁碟區上。這是因為根磁碟區內容並未複寫到災難恢復目的地。 您無法將FlexCache 無法使用的功能區當成記錄目的地ONTAP （例如、更新版本的更新版本）。	`-destination text`	是的	是的	

要稽核的事件類別_ 指定要稽核的事件類別。您可以稽核下列事件類別： • 檔案存取事件（SMB和NFSv4） • SMB登入和登出事件 • 集中存取原則執行事件 從 Windows 2012 Active Directory 網域開始、就可以使用中央存取原則的移位事件。 • 非同步刪除 • 檔案共用類別事件 • 稽核原則變更事件 • 本機使用者帳戶管理事件 • 安全性群組管理事件 • 授權原則變更事件 預設為稽核檔案存取和SMB登入及登出事件。 • 備註： * 您可以先指定 `cap-staging` 在事件類別中、 SVM 上必須存在 SMB 伺服器。雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。	`-events{file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change`	`async-delete}`

否			記錄檔案輸出格式 決定稽核記錄的輸出格式。輸出格式可以是ONTAP專用格式XML或Microsoft Windows EVTX記錄格式。依預設、輸出格式為EVTX。	-format {xml
evtx}	否			記錄檔案旋轉限制 決定要保留多少稽核記錄檔、然後再將最舊的記錄檔轉出。例如、如果您輸入的值5，最後五個記錄檔會保留。 的值0表示保留所有記錄檔。預設值為0。

用於判斷何時旋轉稽核事件記錄的參數

根據記錄大小旋轉記錄

預設值是根據大小來旋轉稽核記錄。

- 預設記錄大小為100 MB
- 如果您要使用預設的記錄檔旋轉方法和預設的記錄檔大小、則不需要設定任何特定的記錄檔旋轉參數。

- 如果您想要根據記錄檔大小來旋轉稽核記錄檔、請使用下列命令來取消設定 `-rotate-schedule-minute` 參數： `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

如果您不想使用預設記錄大小、可以設定 `-rotate-size` 指定自訂記錄大小的參數：

資訊類型	選項	必要	包括	您的價值
記錄檔案大小限制 決定稽核記錄檔大小限制。	`-rotate-size {integer[kb`	MB	GB	TB

根據排程旋轉記錄

如果您選擇根據排程來旋轉稽核記錄、您可以使用任何組合的時間型旋轉參數來排程記錄輪調。

- 如果您使用時間型旋轉、則會使用 `-rotate-schedule-minute` 參數為必填。
- 所有其他的時間型旋轉參數都是選用的。
- 旋轉排程是使用所有與時間相關的值來計算。

  例如、如果您只指定 `-rotate-schedule-minute` 參數時、稽核記錄檔會根據一週中所有天所指定的分鐘數、在一年中所有月份的所有小時內進行旋轉。

- 如果只指定一或兩個時間型旋轉參數（例如、 `-rotate-schedule-month` 和 `-rotate-schedule -minutes`）、記錄檔會根據您在一週的所有天、所有時間、但僅在指定的月份內所指定的分鐘值來旋轉。

  例如、您可以指定稽核日誌在一月、三月和八月的所有週一、週三和週六上午10：30進行輪調

- 如果您同時指定兩者的值 `-rotate-schedule-dayofweek` 和 `-rotate-schedule-day`的問題。

  例如、如果您指定 `-rotate-schedule-dayofweek` 星期五和 `-rotate-schedule-day` 截至 13 日、稽核記錄將會在每週五和指定月份的第 13 天、而不只是在每週五的第 13 天輪調。

- 如果您想要根據排程來旋轉稽核記錄檔、請使用下列命令來取消設定 `-rotate-size` 參數： `vserver audit modify -vserver vs0 -destination / -rotate-size -`

您可以使用下列可用稽核參數清單、來決定要使用哪些值來設定稽核事件記錄輪調的排程：

資訊類型	選項	必要	包括	您的價值
記錄輪調排程：月 決定每月循環稽核記錄的排程。 有效值為 `January` 透過 `December`和 `all`。例如、您可以指定稽核日誌在1月、3月和8月期間輪調。	`-rotate-schedule-month chron_month`	否		

記錄輪調排程：週中日 決定每日（一週中的某天）排程以循環稽核記錄。 有效值為 `Sunday` 透過 `Saturday`和 `all`。例如、您可以指定稽核日誌在週二和週五、或一週中的所有日子循環顯示。	`-rotate-schedule -dayofweek chron_dayofweek`	否		
記錄輪調排程：天 決定每月的日期排程、以循環稽核記錄。 有效值範圍從 `1` 透過 `31`。例如、您可以指定稽核日誌在每月的第10天和第20天、或每月的所有天進行旋轉。	`-rotate-schedule-day chron_dayofmonth`	否		
_記錄輪調排程：hour _ 決定每小時循環稽核記錄的排程。 有效值範圍從 `0` （午夜）至 `23` （下午 11 ： 00 ）。指定 `all` 每小時輪換稽核記錄。例如、您可以指定稽核日誌的旋轉時間為6（上午6點）和18（下午6點）。	`-rotate-schedule-hour chron_hour`	否		
記錄輪調排程：分 決定稽核日誌的分鐘排程。 有效值範圍從 `0` 至 `59`。例如、您可以指定稽核日誌在30分鐘內旋轉。	`-rotate-schedule-minute chron_minute`	是、如果設定排程型記錄輪調、則為否		

根據記錄大小和排程來旋轉記錄

您可以選擇根據記錄大小和排程來旋轉記錄檔、方法是同時設定 `-rotate-size` 參數和時間型旋轉參數。例如：IF `-rotate-size` 設為 10 MB 、且 `-rotate-schedule-minute` 設為 15 、當記錄檔大小達到 10 MB 或每小時 15 分鐘（以先發生的事件為準）時、記錄檔會旋轉。

在**SVM**上建立檔案和目錄稽核組態

在 **ONTAP VM** 上建立檔案和目錄稽核組態

在儲存虛擬機器（SVM）上建立檔案和目錄稽核組態、包括瞭解可用的組態選項、規劃組態、然後設定和啟用組態。然後您可以顯示稽核組態的相關資訊、以確認所產生的組態為所需的組態。

在開始稽核檔案和目錄事件之前、您必須先在儲存虛擬機器（SVM）上建立稽核組態。

開始之前

如果您打算建立稽核組態以進行集中存取原則暫存、則SVM上必須有SMB伺服器。

- 雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。

  動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。

- 如果命令中某個欄位的引數無效、例如欄位的輸入無效、項目重複、以及項目不存在、則命令會在稽核階段之前失敗。

  此類失敗不會產生稽核記錄。

關於這項工作

如果SVM是SVM災難恢復來源、則目的地路徑無法位於根磁碟區上。

步驟

1. 使用規劃工作表中的資訊、建立稽核組態、根據記錄大小或排程來旋轉稽核記錄：

如果您想要以下列方式來旋轉稽核記錄…	輸入…
記錄檔大小	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
排程	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

範例

下列範例會建立稽核組態、以大小為基礎的旋轉方式來稽核檔案作業和SMB登入及登出事件（預設值）。記錄格式為 `EVTX` （預設）。記錄會儲存在中 `/audit_log` 目錄。記錄檔大小限制為 `200 MB`。當記錄大小達到200 MB時、就會進行旋轉：

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

下列範例會建立稽核組態、以大小為基礎的旋轉方式來稽核檔案作業和SMB登入及登出事件（預設值）。記錄格式為 `EVTX` （預設）。記錄會儲存在中 `/cifs_event_logs` 目錄。記錄檔大小限制為 `100 MB` （預設值）、且記錄輪調限制為 `5`：

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

下列範例建立稽核組態、以稽核檔案作業、CIFS登入和登出事件、以及使用時間型輪調的集中存取原則暫存事件。記錄格式為 `EVTX` （預設）。稽核記錄會每月於下午12：30循環一次一週中的所有天。日誌輪轉限制為 `5`：

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

相關資訊

- "在SVM上啟用稽核"
- "驗證稽核組態"

在設定稽核組態之後，啟用 **ONTAP SVM** 的稽核

完成稽核組態的設定之後、您必須在儲存虛擬機器（SVM）上啟用稽核。

開始之前

SVM稽核組態必須已經存在。

關於這項工作

當SVM災難恢復ID捨棄組態第一次啟動（完成SnapMirror初始化之後）且SVM具有稽核組態時ONTAP 、無法自動停用稽核組態。在唯讀SVM上停用稽核、以防止執行磁碟區填滿。只有在SnapMirror關係中斷且SVM為讀寫時、才能啟用稽核。

步驟

1. 在SVM上啟用稽核：

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

相關資訊

- "建立稽核組態"
- "驗證稽核組態"

驗證 **ONTAP** 稽核組態

完成稽核組態之後、您應該確認稽核設定正確且已啟用。

步驟

1. 驗證稽核組態：

   ```
   vserver audit show -instance -vserver vserver_name
   ```

   下列命令會以清單形式顯示儲存虛擬機器（SVM）VS1的所有稽核組態資訊：

   ```
   vserver audit show -instance -vserver vs1
   ```

   ```
                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                           Log Format: evtx
                  Log File Size Limit: 200MB
        Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
   ```

相關資訊

- "建立稽核組態"
- "在SVM上啟用稽核"

設定檔案和資料夾稽核原則

啟用 **ONTAP SVM** 上的稽核組態，並設定檔案和資料夾稽核原則

在檔案和資料夾存取事件上實作稽核是兩步驟的程序。首先、您必須在儲存虛擬機器（SVM）上建立並啟用稽核組態。其次、您必須在要監控的檔案和資料夾上設定稽核原則。您可以設定稽核原則、以監控成功和失敗的存取嘗試。

您可以設定SMB和NFS稽核原則。SMB與NFS稽核原則具有不同的組態需求與稽核功能。

如果已設定適當的稽核原則、ONTAP 僅當SMB或NFS伺服器正在執行時、才會監控稽核原則中指定的SMB和NFS存取事件。

在 **NTFS** 安全性樣式的檔案和目錄上設定 **ONTAP** 稽核原則

在稽核檔案和目錄作業之前、您必須先在要收集稽核資訊的檔案和目錄上設定稽核原則。這是設定及啟用稽核組態的附加功能。您可以使用Windows安全性索引標籤或ONTAP 使用CLI來設定NTFS稽核原則。

使用**Windows**安全性索引標籤設定**NTFS**稽核原則

您可以使用「Windows內容」視窗中的「* Windows安全性*」索引標籤、在檔案和目錄上設定NTFS稽核原則。這是在Windows用戶端上設定資料稽核原則時所使用的相同方法、讓您能夠使用慣用的GUI介面。

開始之前

稽核必須在儲存虛擬機器（SVM）上設定、其中包含您要套用系統存取控制清單（SACL）的資料。

關於這項工作

若要設定NTFS稽核原則、請將項目新增至與NTFS安全性描述元相關聯的NTFS SACL。然後將安全性描述元套用至NTFS檔案和目錄。這些工作會由Windows GUI自動處理。安全性描述元可包含用於套用檔案和資料夾存取權限的判別存取控制清單（DACL）、用於檔案和資料夾稽核的SACL、或同時套用SACL和DACL。

若要使用Windows安全性索引標籤設定NTFS稽核原則、請在Windows主機上完成下列步驟：

步驟

1. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
2. 填寫*對應網路磁碟機*方塊：

   a. 選取*磁碟機*字母。

   b. 在「資料夾」方塊中、輸入包含共用區的SMB伺服器名稱、其中包含您要稽核的資料及共用區名稱。

      您可以指定 SMB 伺服器的資料介面 IP 位址、而非 SMB 伺服器名稱。

      如果您的 SMB 伺服器名稱為「 ShMB_Server 」、而您的共用名稱為「 shahre1 」、則您應該輸入 `\\SMB_SERVER\share1`。

   c. 單擊*完成*。

   您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

3. 選取您要啟用稽核存取的檔案或目錄。
4. 以滑鼠右鍵按一下檔案或目錄、然後選取*內容*。
5. 選取*安全性*索引標籤。
6. 按一下*進階*。
7. 選取*稽核*索引標籤。
8. 執行所需的動作：

如果你想…	請執行下列動作

設定新使用者或群組的稽核	a. 按一下「 * 新增 * 」。 b. 在「輸入要選取的物件名稱」方塊中、輸入您要新增的使用者或群組名稱。 c. 按一下「確定」。
移除使用者或群組的稽核	a. 在「輸入要選取的物件名稱」方塊中、選取您要移除的使用者或群組。 b. 按一下「移除」。 c. 按一下「確定」。 d. 跳過此程序的其餘部分。
變更使用者或群組的稽核	a. 在「輸入要選取的物件名稱」方塊中、選取您要變更的使用者或群組。 b. 按一下 * 編輯 * 。 c. 按一下「確定」。

如果您要在使用者或群組上設定稽核、或是變更現有使用者或群組的稽核、就會開啟「<object>的稽核項目」方塊。

9. 在「套用至」方塊中、選取您要套用此稽核項目的方式。

   您可以選擇下列其中一項：

   - 此資料夾、子資料夾及檔案
   - 此資料夾及子資料夾
   - 僅此資料夾
   - 此資料夾與檔案
   - 僅限子資料夾與檔案
   - 僅子資料夾
   - * 僅檔案 *
     如果您要在單一檔案上設定稽核、則「 * 套用至 * 」方塊不會啟用。「套用至」方塊設定預設為*僅此物件*。

   由於稽核需要SVM資源、因此請僅選取提供稽核事件的最低層級、以符合您的安全需求。

10. 在「存取」方塊中、選取您要稽核的項目、以及是否要稽核成功的事件、失敗事件或兩者。
    - 若要稽核成功的事件、請選取「成功」方塊。
    - 若要稽核失敗事件、請選取「失敗」方塊。

      只選取您需要監控的動作、以符合安全性需求。如需這些可稽核事件的詳細資訊、請參閱Windows文件。您可以稽核下列事件：

- 完全控制
- 周遊資料夾/執行檔案
- 列出資料夾/讀取資料
- 讀取屬性
- 讀取延伸屬性
- 建立檔案/寫入資料
- 建立資料夾/附加資料
- 寫入屬性
- 寫入延伸屬性
- 刪除子資料夾與檔案
- 刪除
- 讀取權限
- 變更權限
- 取得所有權

11. 如果不希望稽核設定傳播到原始容器的後續檔案和資料夾、請選取「僅將這些稽核項目套用至此容器內的物件和（或）容器*」方塊。
12. 按一下「 * 套用 * 」。
13. 完成新增、移除或編輯稽核項目之後、請按一下*確定*。

    「<object>的稽核項目」方塊隨即關閉。

14. 在「稽核」方塊中、選取此資料夾的繼承設定。

    只選取提供稽核事件的最低層級、以符合您的安全需求。您可以選擇下列其中一項：

    - 選取[包含來自此物件父物件的可繼承稽核項目]方塊。
    - 選取「使用此物件的可繼承稽核項目來取代所有子系上所有現有的可繼承稽核項目」方塊。
    - 選取兩個方塊。
    - 請選取兩個方塊。
      如果您要在單一檔案上設定SACL，則[稽核]方塊中不會出現[以這個物件的可繼承稽核項目取代所有子系上所有現有的可繼承稽核項目]方塊。

15. 按一下「確定」。

    稽核方塊隨即關閉。

使用**ONTAP CLI**設定**NTFS**稽核原則

您可以使用ONTAP CLI在檔案和資料夾上設定稽核原則。這可讓您設定NTFS稽核原則、而不需要使用Windows用戶端上的SMB共用區連線至資料。

您可以使用設定 NTFS 稽核原則 `vserver security file-directory` 命令系列。

您只能使用CLI設定NTFS SACL。此支援的不支援NFSv4 SACL系列。ONTAP深入瞭解如何使用這些命令來設定 NTFS SACL "指令參考資料ONTAP"，並將其新增至中的檔案和資料夾。

設定 **UNIX** 安全性樣式檔案和目錄的 **ONTAP** 稽核

您可以將稽核ACE新增至NFSv4.x ACL、以設定UNIX安全樣式檔案和目錄的稽核。這可讓您監控特定NFS檔案和目錄存取事件、以確保安全。

關於這項工作

對於NFSv4.x、可自由判斷的ACE和系統的ACE都儲存在相同的ACL中。它們不會儲存在個別的DACL和SACL中。因此、在將稽核ACE新增至現有ACL時、您必須謹慎小心、以免覆寫及遺失現有ACL。將稽核ACE新增至現有ACL的順序並不重要。

步驟

1. 使用擷取檔案或目錄的現有 ACL `nfs4_getfacl` 或等效命令。

   如"指令參考資料ONTAP"需有關操作 ACL 的詳細資訊，請參閱。

2. 附加所需的稽核ACE。
3. 使用將更新的 ACL 套用至檔案或目錄 `nfs4_setfacl` 或等效命令。

顯示套用至檔案和目錄的稽核原則相關資訊

存取 **Windows** 安全性索引標籤，即可檢視 **ONTAP** 稽核原則資訊

您可以使用「Windows內容」視窗中的「安全性」索引標籤、顯示已套用至檔案和目錄的稽核原則相關資訊。這種方法與存放在Windows伺服器上的資料相同、可讓客戶使用慣用的GUI介面。

關於這項工作

顯示套用至檔案和目錄的稽核原則相關資訊、可讓您驗證是否已在指定的檔案和資料夾上設定適當的系統存取控制清單（SACL）。

若要顯示已套用至NTFS檔案和資料夾的SACL相關資訊、請在Windows主機上完成下列步驟。

步驟

1. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
2. 完成*對應網路磁碟機*對話方塊：

   a. 選取*磁碟機*字母。

   b. 在「資料夾」方塊中、輸入儲存虛擬機器（SVM）的IP位址或SMB伺服器名稱、其中包含要稽核的資料及共用名稱。

      如果您的 SMB 伺服器名稱為「 ShMB_Server 」、而您的共用名稱為「 shahre1 」、則您應該輸入 `\\SMB_SERVER\share1`。

      您可以指定 SMB 伺服器的資料介面 IP 位址、而非 SMB 伺服器名稱。

c. 單擊*完成*。

您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

3. 選取您要顯示稽核資訊的檔案或目錄。
4. 在檔案或目錄上按一下滑鼠右鍵、然後選取*內容*。
5. 選取*安全性*索引標籤。
6. 按一下*進階*。
7. 選取*稽核*索引標籤。
8. 按一下 * 繼續 * 。

稽核方塊隨即開啟。「稽核項目」方塊會顯示套用SACL的使用者和群組摘要。

9. 在「稽核項目」方塊中、選取您要顯示其SACL項目的使用者或群組。
10. 按一下 * 編輯 * 。

隨即開啟<object>的稽核項目方塊。

11. 在「存取」方塊中、檢視套用至所選物件的目前SACL。
12. 按一下*取消*以關閉*稽核項目*方塊。
13. 單擊*取消*關閉*稽核*方塊。

顯示 **ONTAP FlexVol** 磁碟區上 **NTFS** 稽核原則的相關資訊

您可以在FlexVol 功能區上顯示NTFS稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單的相關資訊。您可以使用這些資訊來驗證安全性組態或疑難排解稽核問題。

關於這項工作

顯示套用至檔案和目錄的稽核原則相關資訊、可讓您驗證是否已在指定的檔案和資料夾上設定適當的系統存取控制清單（SACL）。

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或資料夾路徑。您可以以摘要形式或詳細清單來顯示輸出。

- NTFS安全型磁碟區和qtree僅使用NTFS系統存取控制清單（SACL）來執行稽核原則。
- 在具有NTFS有效安全性的混合式安全型磁碟區中、檔案和資料夾可以套用NTFS稽核原則。

  混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。

- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS有效安全性、而且可能包含或不包含NTFS SACL。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般檔案和資料夾NFSv4 SACL、以及儲存層級存取保護NTFS SACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則輸出也會顯示動態存取控制ACE的相關資訊（

如果已針對指定的檔案或目錄路徑設定動態存取控制）。

- 在顯示具有NTFS有效安全性的檔案和資料夾的安全性資訊時、UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。

  NTFS安全型檔案和資料夾在決定檔案存取權限時、僅使用NTFS檔案權限、Windows使用者和群組。

- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄稽核原則設定：

如果您想要顯示資訊…	輸入下列命令…
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
詳細清單	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

下列範例顯示路徑的稽核原則資訊 `/corp` 在 SVM VS1 中。路徑具有NTFS有效安全性。NTFS安全性描述元包含成功和成功/失敗SACL項目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

下列範例顯示路徑的稽核原則資訊 `/datavol1` 在 SVM VS1 中。路徑包含一般檔案和資料夾SACL、以及儲存層級存取保護SACL。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

使用萬用字元顯示 **ONTAP** 檔案安全性和稽核原則的相關資訊

您可以使用萬用字元（*）來顯示特定路徑或根磁碟區下所有檔案和目錄的檔案安全性和稽核原則相關資訊。

萬用字元（*）可做為指定目錄路徑的最後一個子元件、您可以在該子元件下方顯示所有檔案和目錄的資訊。

如果您想要顯示名為「*」的特定檔案或目錄資訊、則必須在雙引號（「」）內提供完整路徑。

範例

下列含有萬用字元的命令會顯示路徑下方所有檔案和目錄的相關資訊 `/1/` SVM VS1 ：

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
           Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
           Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

下列命令會顯示路徑下名為「 * 」的檔案資訊 `/vol1/a` SVM VS1 的路徑會以雙引號（""）括住。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

可稽核的CLI變更事件

瞭解可稽核的 **ONTAP CLI** 變更事件

可稽核某些CLI變更事件、包括特定SMB共用事件、特定稽核原則事件、特定本機安全性群組事件、本機使用者群組事件、以及授權原則事件。ONTAP瞭解哪些變更事件可稽核、有助於解讀事件記錄的結果。

您可以手動旋轉稽核記錄、啟用或停用稽核、顯示稽核變更事件的相關資訊、修改稽核變更事件、以及刪除稽核變更事件、藉此管理儲存虛擬機器（SVM）稽核CLI變更事件。

身為系統管理員、如果您執行任何命令來變更SMB共用區、本機使用者群組、本機安全性群組、授權原則及稽核原則事件的相關組態、 產生記錄並稽核相應的事件：

稽核類別	活動	事件ID	執行此命令…
主機稽核	原則變更	[4719]稽核組態已變更	`vserver audit disable
enable	modify`	檔案共用	已新增[5142]網路共用

`vserver cifs share create`	[5143]網路共用區已修改	`vserver cifs share modify` `vserver cifs share create`	modify
delete` `vserver cifs share add	remove`	[5144]網路共用區已刪除	`vserver cifs share delete`
稽核	使用者帳戶	[4720]本機使用者已建立	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722]本機使用者已啟用	`vserver cifs users-and-groups local-user create	modify`	[4724]本機使用者密碼重設
`vserver cifs users-and-groups local-user set-password`	[4725]本機使用者已停用	`vserver cifs users-and-groups local-user create	modify`
[4726]本機使用者已刪除	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738]本機使用者變更	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781]本機使用者重新命名	`vserver cifs users-and-groups local-user rename`	安全性群組	[4731]已建立本機安全性群組
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734]本機安全性群組已刪除	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735]本機安全性群組已修改
`vserver cifs users-and-groups local-group rename`	modify` `vserver services name-service unix-group modify`	[4732]使用者已新增至本機群組	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`

[4733]使用者已從本機群組中移除	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	授權原則變更	[4704]已指派使用者權限
`vserver cifs users-and-groups privilege add-privilege`	[4705]使用者權限已移除	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

相關資訊

- "Vserver"

管理檔案共用 **ONTAP** 事件

為儲存虛擬機器（SVM）設定檔案共用事件並啟用稽核時、就會產生稽核事件。使用修改 SMB 網路共用時、會產生檔案共用事件 `vserver cifs share` 相關命令。

新增、修改或刪除SVM的SMB網路共用時、會產生事件ID為5142、5143和5144的檔案共用事件。SMB 網路共用組態是使用修改的 `cifs share access control create|modify|delete` 命令。

下列範例顯示建立名為「稽核目的地」的共用物件時、會產生ID為5143的檔案共用事件：

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

管理稽核原則變更 **ONTAP** 事件

當為儲存虛擬機器（SVM）設定稽核原則變更事件並啟用稽核時、就會產生稽核事件。使用修改稽核原則時、會產生稽核原則變更事件 `vserver audit` 相關命令。

每當停用、啟用或修改稽核原則時、就會產生事件ID 4719的稽核原則變更事件、並有助於識別使用者嘗試停用稽核以涵蓋追蹤的時間。此設定預設為設定、需要診斷權限才能停用。

下列範例顯示稽核原則變更事件、並在停用稽核時產生ID 4719：

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

管理使用者帳戶 **ONTAP** 事件

當儲存虛擬機器（SVM）的使用者帳戶事件設定為啟用稽核時、就會產生稽核事件。

事件ID為4720、4722、4724、4725、4726、 當本機SMB或NFS使用者從系統建立或刪除、本機使用者帳戶啟用、停用或修改、以及本機SMB使用者密碼重設或變更時、就會產生4738和4781。使用修改使用者帳戶時、會產生使用者帳戶事件 `vserver cifs users-and-groups <local user>` 和 `vserver services name-service <unix user>` 命令。

下列範例顯示建立本機SMB使用者時產生ID 4720的使用者帳戶事件：

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

下列範例顯示在先前範例中建立的本機SMB使用者重新命名時、產生ID為4781的使用者帳戶事件：

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

管理安全性群組 **ONTAP** 事件

當儲存虛擬機器（SVM）的安全性群組事件設定為啟用稽核時、就會產生稽核事件。

從系統建立或刪除本機SMB或NFS群組、並從群組新增或移除本機使用者時、會產生事件ID為4731、4732、4733、4734和4735的安全性群組事件。當使用修改使用者帳戶時、就會產生安全性群組事件 `vserver cifs users-and-groups <local-group>` 和 `vserver services name-service <unix-group>` 命令。

下列範例顯示建立本機UNIX安全性群組時、產生ID 4731的安全性群組事件：

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

管理授權原則變更 **ONTAP** 事件

當儲存虛擬機器（SVM）的授權原則變更事件設定為啟用稽核時、就會產生稽核事件。

每當SMB使用者和SMB群組的授權權限被授予或撤銷時、就會產生事件ID為4704和4705的授權原則變更事件。當使用指派或撤銷授權權限時、就會產生授權原則變更事件 `vserver cifs users-and-groups privilege` 相關命令。

下列範例顯示指派SMB使用者群組授權權限時、產生ID 4704的授權原則事件：

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

管理稽核組態

手動旋轉稽核事件記錄檔，以檢視特定的 ONTAP SVM 事件記錄

您必須先將記錄轉換成使用者可讀取的格式、才能檢視稽核事件記錄。如果您想要先檢視特定儲存虛擬機器（SVM）的事件記錄、再ONTAP 由SVM自動旋轉記錄、您可以手動旋轉SVM上的稽核事件記錄。

步驟

1. 使用旋轉稽核事件記錄 `vserver audit rotate-log` 命令。

   ```
   vserver audit rotate-log -vserver vs1
   ```

   稽核事件記錄會以稽核組態指定的格式儲存在 SVM 稽核事件記錄目錄中 (`XML` 或 `EVTX`）、並可使用適當的應用程式來檢視。

啟用或停用 ONTAP SVM 上的稽核

您可以在儲存虛擬機器（SVM）上啟用或停用稽核。您可能想要停用稽核功能、暫時停止檔案和目錄稽核。您可以隨時啟用稽核（如果存在稽核組態）。

開始之前

在SVM上啟用稽核之前、SVM的稽核組態必須已經存在。

"建立稽核組態"

關於這項工作

停用稽核不會刪除稽核組態。

步驟

1. 執行適當的命令：

如果您想要稽核...	輸入命令...
已啟用	`vserver audit enable -vserver vserver_name`
已停用	`vserver audit disable -vserver vserver_name`

2. 確認稽核處於所需狀態：

   `vserver audit show -vserver vserver_name`

範例

下列範例可啟用SVM VS1的稽核：

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

cluster1::> vserver audit show -vserver vs1

                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

下列範例停用SVM VS1的稽核：

```
cluster1::> vserver audit disable -vserver vs1

                                Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

顯示 **ONTAP** 稽核組態的相關資訊

您可以顯示稽核組態的相關資訊。這些資訊可協助您判斷每個SVM的組態是否符合您的需求。顯示的資訊也可讓您驗證是否已啟用稽核組態。

關於這項工作

您可以在所有SVM上顯示稽核組態的詳細資訊、也可以指定選用參數來自訂輸出中顯示的資訊。如果您未指定任何選用參數、則會顯示下列項目：

- 稽核組態套用至的SVM名稱
- 稽核狀態、可以是 `true` 或 `false`

  如果稽核狀態為 `true`，已啟用稽核。如果稽核狀態為 `false`，稽核已停用。

- 要稽核的事件類別
- 稽核記錄格式
- 稽核子系統儲存合併及轉換稽核記錄的目標目錄

步驟

1. 使用顯示稽核組態的相關資訊 `vserver audit show` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver audit show`資訊，請參閱。

範例

下列範例顯示所有SVM稽核組態的摘要：

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

下列範例以清單形式顯示所有SVM的所有稽核組態資訊：

```
cluster1::> vserver audit show -instance

                            Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
```

用於修改稽核組態的 **ONTAP** 命令

如果您想要變更稽核設定、可以隨時修改目前的組態、包括修改記錄路徑目的地和記錄格式、修改要稽核的事件類別、如何自動儲存記錄檔、以及指定要儲存的記錄檔數目上限。

如果您想要...	使用此命令...
修改記錄目的地路徑	`vserver audit modify` 使用 `-destination` 參數
修改要稽核的事件類別	`vserver audit modify` 使用 `-events` 參數 若要稽核集中存取原則暫存事件、必須在儲存虛擬機器（SVM）上啟用動態存取控制（DAC）SMB伺服器選項。
修改記錄格式	`vserver audit modify` 使用 `-format` 參數
根據內部記錄檔大小啟用自動儲存	`vserver audit modify` 使用 `-rotate-size` 參數

根據時間間隔啟用自動儲存	`vserver audit modify` 使用 `-rotate-schedule-month`、`-rotate-schedule-dayofweek`、`-rotate-schedule-day`、`-rotate-schedule-hour`和 `-rotate-schedule-minute` 參數
指定儲存的記錄檔數目上限	`vserver audit modify` 使用 `-rotate-limit` 參數

刪除 ONTAP SVM 上的稽核組態

如果您不想再稽核儲存虛擬機器（SVM）上的檔案和目錄事件、也不想在SVM上維護稽核組態、可以刪除稽核組態。

步驟

1. 停用稽核組態：

```
vserver audit disable -vserver vserver_name

vserver audit disable -vserver vs1
```

2. 刪除稽核組態：

```
vserver audit delete -vserver vserver_name

vserver audit delete -vserver vs1
```

瞭解還原稽核 ONTAP 叢集的影響

如果您打算還原叢集、ONTAP 當叢集中有啟用稽核的儲存虛擬機器（SVM）時、您應該注意下列還原程序。您必須先採取特定行動、才能恢復。

還原ONTAP 至不支援SMB登入和登出事件稽核、以及集中存取原則執行事件的版本

支援SMB登入和登出事件的稽核、以及集中存取原則執行事件、從叢集Data ONTAP 式的版本資訊8.3開始。如果您要回復ONTAP 到不支援這些事件類型的版本、而且您有監控這些事件類型的稽核組態、則必須在還原之前變更這些啟用稽核的SVM的稽核組態。您必須修改組態、以便只稽核檔案作業事件。

疑難排解 ONTAP 稽核和暫存磁碟區空間問題

當暫存磁碟區或包含稽核事件記錄的磁碟區空間不足時、可能會發生問題。如果空間不足、就無法建立新的稽核記錄、這會使用戶端無法存取資料、而且存取要求也會失敗。您應該知道如何疑難排解及解決這些磁碟區空間問題。

疑難排解與事件記錄磁碟區相關的空間問題

如果包含事件記錄檔的磁碟區空間不足、稽核將無法將記錄轉換成記錄檔。這會導致用戶端存取失敗。您必須知道如何疑難排解與事件記錄磁碟區相關的空間問題。

- 儲存虛擬機器（ SVM ）和叢集管理員可以顯示有關 Volume 和 Aggregate 使用率和組態的資訊、藉此判斷是否有足夠的磁碟區空間。
- 如果包含事件記錄的磁碟區空間不足、SVM和叢集管理員可以移除部分事件記錄檔、或是增加磁碟區的大小、來解決空間問題。

> ⓘ 如果包含事件記錄磁碟區的Aggregate已滿、則必須先增加Aggregate的大小、才能增加磁碟區的大小。只有叢集管理員可以增加集合體的大小。

- 事件記錄檔的目的地路徑可透過修改稽核組態、變更為另一個磁碟區上的目錄。

> ⓘ 在下列情況下、資料存取遭拒：
>
> ◦ 目的地目錄即會刪除。
>
> ◦ 主控目的地目錄的磁碟區上的檔案限制達到其最大層級。

深入瞭解：

- "如何檢視磁碟區的相關資訊、以及增加磁碟區大小"。
- "如何檢視有關集合體與管理集合體的資訊"。

疑難排解與接移磁碟區相關的空間問題

如果任何包含儲存虛擬機器（SVM）暫存檔案的磁碟區空間不足、稽核將無法將記錄寫入暫存檔案。這會導致用戶端存取失敗。若要疑難排解此問題、您必須顯示磁碟區使用量的相關資訊、以判斷SVM中使用的任何暫存磁碟區是否已滿。

如果包含合併事件記錄檔的磁碟區有足夠空間、但由於空間不足、仍有用戶端存取失敗、則暫存磁碟區可能空間不足。SVM管理員必須聯絡您、以判斷內含SVM暫存檔案的暫存磁碟區是否空間不足。如果因暫存磁碟區空間不足而無法產生稽核事件、則稽核子系統會產生EMS事件。畫面會顯示下列訊息： `No space left on device`。只有您可以檢視暫存磁碟區的相關資訊、SVM管理員無法檢視。

所有暫存磁碟區名稱都以開頭 `MDV_aud_` 接著是包含該暫存磁碟區的集合的 UUID 。以下範例顯示管理SVM上的四個系統磁碟區、這些磁碟區是在為叢集中的資料SVM建立檔案服務稽核組態時自動建立的：

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

如果暫存磁碟區空間不足、您可以增加磁碟區的大小來解決空間問題。

如果包含暫存磁碟區的Aggregate已滿、則必須先增加Aggregate的大小、才能增加磁碟區的大小。只有您可以增加Aggregate的大小、SVM管理員才能增加。

如果一個或多個集合體的可用空間小於 2GB （在 ONTAP 9.14.1 及更早版本中）或 5GB （從 ONTAP 9.15.1 開始）、則 SVM 稽核建立會失敗。當SVM稽核建立失敗時、所建立的暫存磁碟區會被刪除。

在SVM上使用FPolicy進行檔案監控與管理

瞭解 FPolicy

了解ONTAP FPolicy 解決方案

FPolicy 是檔案存取通知架構、可用來透過合作夥伴解決方案監控及管理儲存虛擬機器（ SVM ）上的檔案存取事件。合作夥伴解決方案可協助您處理各種使用案例、例如資料治理與法規遵循、勒索軟體保護及資料移動性。

合作夥伴解決方案包括 NetApp 支援的第三方解決方案，以及 NetApp 產品工作負載安全性和雲端資料感測。

FPolicy解決方案有兩個部分。ONTAP FPolicy 架構可管理叢集上的活動、並傳送通知給合作夥伴應用程式（也稱為外部 FPolicy 伺服器）。外部 FPolicy 伺服器會處理 ONTAP FPolicy 傳送的通知、以履行客戶使用案例。

此解決方案可建立及維護FPolicy組態、監控檔案事件、並將通知傳送至外部FPolicy伺服器。ONTAP支援內部基礎架構、可在外部FPolicy伺服器與儲存虛擬機器（SVM）節點之間進行通訊。ONTAP

FPolicy架構會連線至外部FPolicy伺服器、並在用戶端存取導致這些事件發生時、將特定檔案系統事件的通知傳

送至FPolicy伺服器。外部FPolicy伺服器會處理通知、並將回應傳回節點。通知處理的結果取決於應用程式、以及節點與外部伺服器之間的通訊是否為非同步或同步。

ONTAP FPolicy 同步與非同步通知

FPolicy會透過FPolicy介面將通知傳送至外部FPolicy伺服器。通知會以同步或非同步模式傳送。通知模式會決定ONTAP 將通知傳送至FPolicy伺服器後的功能。

- 非同步通知

  藉由非同步通知、節點不會等待FPolicy伺服器的回應、進而提升系統的整體處理量。這類通知適用於FPolicy伺服器不需要在通知評估後採取任何行動的應用程式。例如、當儲存虛擬機器（SVM）管理員想要監控和稽核檔案存取活動時、就會使用非同步通知。

  如果以非同步模式運作的FPolicy伺服器發生網路中斷、則中斷期間產生的FPolicy通知會儲存在儲存節點上。當FPolicy伺服器重新連線時、系統會警示已儲存的通知、並從儲存節點擷取通知。在停機期間可儲存通知的時間長度可設定為10分鐘。

  從 ONTAP 9.14.1 開始、 FPolicy 可讓您設定持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。不支援同步（強制或非強制）和非同步強制組態。

- 同步通知

  設定為以同步模式執行時、FPolicy伺服器必須先確認每個通知、才能繼續執行用戶端作業。此類型的通知會在根據通知評估結果需要採取行動時使用。例如、當SVM管理員想要根據外部FPolicy伺服器上指定的條件來允許或拒絕要求時、就會使用同步通知。

同步與非同步應用程式

FPolicy應用程式有許多可能的用途、包括非同步和同步。

非同步應用程式是指外部FPolicy伺服器不會改變存取儲存虛擬機器（SVM）上檔案或目錄或修改資料的方式。例如：

- 檔案存取與稽核記錄
- 儲存資源管理

同步應用程式是指資料存取遭竄改或資料遭外部FPolicy伺服器修改的應用程式。例如：

- 配額管理
- 檔案存取封鎖
- 檔案歸檔與階層式儲存管理
- 加密與解密服務
- 壓縮與解壓縮服務

ONTAP FPolicy 持久存儲

持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。從

ONTAP 9.14.1 開始、您可以設定 FPolicy 持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。不支援同步（強制或非強制）和非同步強制組態。

此功能僅適用於 FPolicy 外部模式。您使用的合作夥伴應用程式需要支援此功能。您應與合作夥伴合作、確保支援此 FPolicy 組態。

從 ONTAP 9.15.1 開始、 FPolicy 永續性儲存區組態已簡化。。 `persistent-store create` 命令可自動建立 SVM 的 Volume 、並使用持續儲存區最佳實務做法來設定 Volume 。

如需持續儲存最佳實務做法的詳細資訊、請參閱 "設定FPolicy的需求、考量及最佳實務做法"。

如需新增持續儲存區的相關資訊、請參閱 "建立持續儲存區"。

ONTAP FPolicy 配置類型

有兩種基本的FPolicy組態類型。其中一個組態使用外部FPolicy伺服器來處理通知並根據通知採取行動。另一個組態不使用外部FPolicy伺服器、而是使用ONTAP 內部的、原生的FPolicy伺服器、根據副檔名來進行簡單的檔案封鎖。

- 外部**FPolicy**伺服器組態

  通知會傳送至FPolicy伺服器、該伺服器會篩選要求並套用規則、以判斷節點是否應允許要求的檔案操作。對於同步原則、FPolicy伺服器接著會傳送回應給節點、以允許或封鎖要求的檔案作業。

- 原生**FPolicy**伺服器組態

  通知會在內部篩選。根據在FPolicy範圍中設定的副檔名設定、允許或拒絕要求。

  附註：不記錄被拒絕的副檔名要求。

何時建立原生**FPolicy**組態

原生FPolicy組態使用ONTAP 內部的FPolicy引擎、根據檔案副檔名來監控及封鎖檔案作業。此解決方案不需要外部FPolicy伺服器（FPolicy伺服器）。當這個簡單的解決方案只是需要的時候、使用原生檔案封鎖組態是適當的做法。

原生檔案封鎖功能可讓您監控符合設定作業和篩選事件的任何檔案作業、然後拒絕存取具有特定副檔名的檔案。這是預設組態。

此組態可讓您僅根據檔案副檔名來封鎖檔案存取。例如、封鎖包含的檔案 `mp3` 副檔名時、您可以設定原則、為目標副檔名為的特定作業提供通知 `mp3`。原則設定為拒絕 `mp3` 產生通知之作業的檔案要求。

下列項目適用於原生FPolicy組態：

- FPolicy伺服器型檔案篩選所支援的相同篩選器和傳輸協定集、也支援原生檔案封鎖。
- 您可以同時設定原生檔案封鎖和FPolicy伺服器型檔案篩選應用程式。

  若要這麼做、您可以針對儲存虛擬機器（SVM）設定兩個獨立的FPolicy原則、其中一個設定為原生檔案封鎖、另一個設定為FPolicy伺服器型檔案篩選。

- 原生檔案封鎖功能只會根據副檔名而非檔案內容來篩選檔案。

- 在符號連結的情況下、原生檔案封鎖會使用根檔案的副檔名。

深入瞭解 "FPolicy：原生檔案封鎖"。

何時建立使用外部**FPolicy**伺服器的組態

使用外部FPolicy伺服器來處理及管理通知的FPolicy組態、可針對需要根據副檔名進行簡單檔案封鎖的使用案例、提供健全的解決方案。

當您想要執行監控及記錄檔案存取事件、提供配額服務、根據簡單副檔名以外的條件執行檔案封鎖、使用階層式儲存管理應用程式提供資料移轉服務等作業時、應建立使用外部FPolicy伺服器的組態、 或是提供一組精細的原則、僅監控儲存虛擬機器（SVM）中的資料子集。

ONTAP FPolicy 實作中的叢集元件角色

叢集、內含的儲存虛擬機器（SVM）和資料生命量、都在FPolicy實作中扮演著重要角色。

- 叢集

  叢集包含FPolicy管理架構、並維護及管理叢集中所有FPolicy組態的相關資訊。

- * SVM*

  FPolicy組態是在SVM層級定義。組態的範圍是SVM、它只能在SVM資源上運作。某個SVM組態無法監控及傳送針對位於另一個SVM上的資料所提出的檔案存取要求通知。

  可在管理SVM上定義FPolicy組態。在管理SVM上定義組態之後、即可在所有SVM中看到及使用這些組態。

- 資料生命量

  連接至FPolicy伺服器的方式是透過屬於SVM的資料LIF與FPolicy組態。這些連線所使用的資料生命量、可能會像一般用戶端存取所使用的資料生命量一樣進行容錯移轉。

ONTAP FPolicy 如何與外部 **FPolicy** 伺服器搭配使用

在儲存虛擬機器（SVM）上設定並啟用FPolicy之後、FPolicy會在SVM所參與的每個節點上執行。FPolicy負責建立及維護與外部FPolicy伺服器（FPolicy伺服器）的連線、通知處理、以及管理與FPolicy伺服器之間的通知訊息。

此外、在連線管理中、FPolicy有下列責任：

- 確保檔案通知會透過正確的LIF傳送到FPolicy伺服器。
- 確保當多個FPolicy伺服器與某個原則相關聯時、會在傳送通知給FPolicy伺服器時完成負載平衡。
- 當與FPolicy伺服器的連線中斷時、嘗試重新建立連線。
- 透過驗證的工作階段將通知傳送至FPolicy伺服器。
- 管理FPolicy伺服器所建立的Passthrough-read資料連線、以便在啟用passe-read時、為用戶端要求提供服務。

控制通道如何用於**FPolicy**通訊

FPolicy會從儲存虛擬機器（SVM）上每個節點的資料生命期、啟動與外部FPolicy伺服器的控制通道連線。FPolicy使用控制通道來傳輸檔案通知、因此FPolicy伺服器可能會根據SVM拓撲看到多個控制通道連線。

特殊權限資料存取通道如何用於同步通訊

在同步使用案例中、FPolicy伺服器會透過特殊權限的資料存取路徑、存取儲存虛擬機器（SVM）上的資料。透過權限路徑存取時、會將完整的檔案系統公開給FPolicy伺服器。它可以存取資料檔案來收集資訊、掃描檔案、讀取檔案或寫入檔案。

由於外部FPolicy伺服器可透過特殊權限的資料通道、從SVM的根目錄存取整個檔案系統、因此具有特殊權限的資料通道連線必須安全無虞。

如何將**FPolicy**連線認證用於特殊權限的資料存取通道

FPolicy伺服器會使用與FPolicy組態一起儲存的特定Windows使用者認證、建立與叢集節點的授權資料存取連線。SMB是唯一支援的傳輸協定、可用來建立特殊權限資料存取通道連線。

如果FPolicy伺服器需要存取授權資料、則必須符合下列條件：

- 必須在叢集上啟用SMB授權。
- FPolicy伺服器必須在FPolicy組態中設定的認證下執行。

建立資料通道連線時、FPolicy會使用指定Windows使用者名稱的認證資料。資料存取是透過管理共用ONTAP_admin$進行。

授與超級使用者認證以進行授權資料存取的意義

使用FPolicy組態中設定的IP位址和使用者認證組合、將超級使用者認證授予FPolicy伺服器。ONTAP

當FPolicy伺服器存取資料時、超級使用者狀態會授予下列權限：

- 避免進行權限檢查

  使用者無需檢查檔案和目錄存取。

- 特殊鎖定權限

  支援讀取、寫入或修改任何檔案的存取權限、無論現有的鎖定為何。ONTAP如果FPolicy伺服器對檔案進行位元組範圍鎖定、則會立即移除檔案上現有的鎖定。

- 略過任何FPolicy檢查

  存取不會產生任何FPolicy通知。

FPolicy如何管理原則處理

可能有多個FPolicy原則指派給您的儲存虛擬機器（SVM）、每個原則的優先順序各不相同。若要在SVM上建立適當的FPolicy組態、請務必瞭解FPolicy如何管理原則處理。

每個檔案存取要求都會經過初始評估、以判斷哪些原則正在監控此事件。如果是受監控的事件、則監控事件的相

關資訊以及相關的原則都會傳送到FPolicy、並在FPolicy中進行評估。每個原則都會依照指派的優先順序進行評估。

在設定原則時、您應考慮下列建議：

- 當您想要在其他原則之前一律先評估原則時、請以較高的優先順序設定該原則。
- 如果所要求的檔案存取作業在受監控事件上成功、是根據其他原則評估檔案要求的先決條件、請將控制第一個檔案作業成功或失敗的原則設定為較高的優先順序。

  例如、如果一個原則管理FPolicy檔案歸檔與還原功能、而另一個原則管理線上檔案的檔案存取作業、 管理檔案還原的原則必須具有較高的優先順序、才能在第二個原則所管理的作業之前還原檔案。

- 如果您想要評估所有可能套用至檔案存取作業的原則、請將同步原則的優先順序降低。

您可以修改原則順序編號、重新排列現有原則的原則優先順序。不過、若要讓FPolicy根據修改後的優先順序來評估原則、您必須停用並重新啟用具有修改順序編號的原則。

節點到外部 **ONTAP FPolicy** 伺服器通訊過程

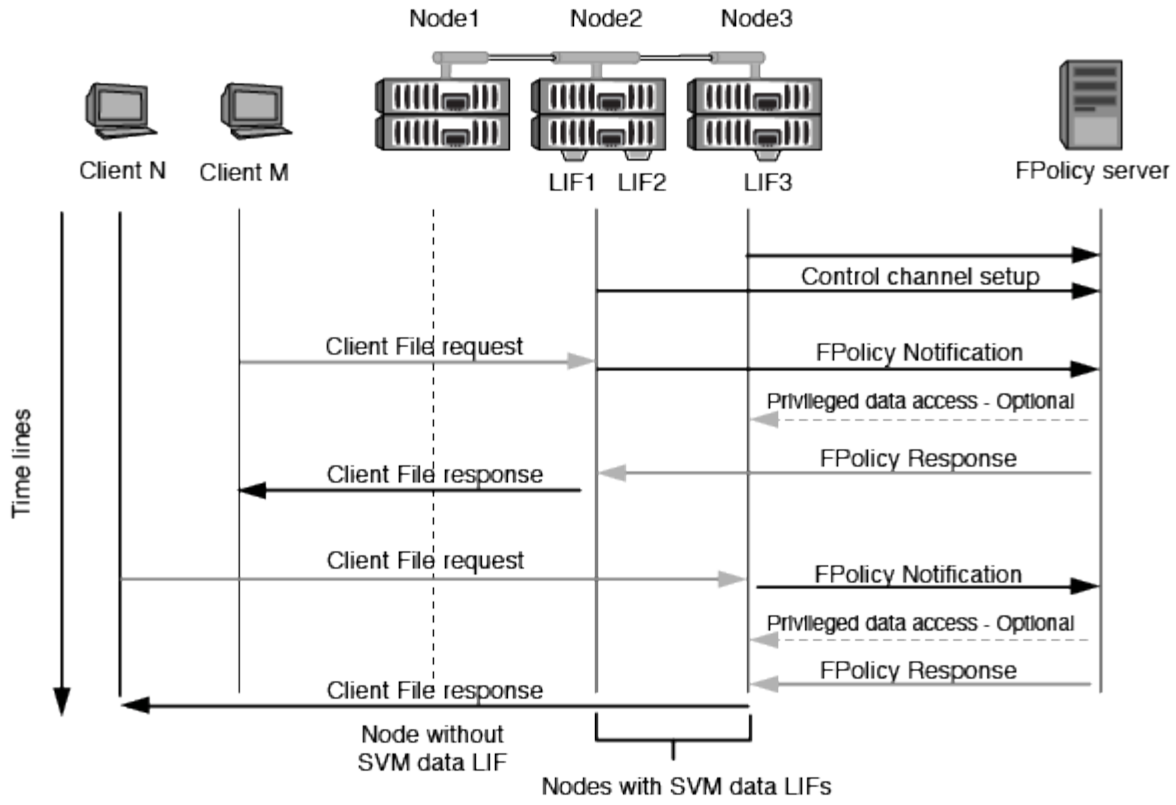
若要正確規劃FPolicy組態、您應該瞭解節點對外部FPolicy伺服器的通訊程序為何。

每個參與每個儲存虛擬機器（SVM）的節點、都會使用TCP/IP來啟動與外部FPolicy伺服器（FPolicy伺服器）的連線。與FPolicy伺服器的連線是使用節點資料LIF設定、因此只有當節點具有SVM的作業資料LIF時、參與的節點才能設定連線。

啟用原則時、參與節點上的每個FPolicy程序都會嘗試建立與FPolicy伺服器的連線。它使用原則組態中指定的FPolicy外部引擎IP位址和連接埠。

此連線會透過資料LIF、從每個SVM上的每個節點建立一個控制通道、以連接至FPolicy伺服器。此外、如果同一個參與節點上有IPV4和IPV6資料LIF位址、FPolicy會嘗試建立連線、以便同時連線至IPV4和IPV6。因此、在SVM延伸到多個節點上的案例中、或是同時存在IPV4和IPV6位址時、FPolicy伺服器必須在SVM上啟用FPolicy原則之後、為叢集的多個控制通道設定要求做好準備。

例如、如果叢集有三個節點（節點1、節點2和節點3）、而SVM資料LIF僅散佈於節點2和節點3、則控制通道只會從節點2和節點3啟動、無論資料磁碟區的分佈為何。說明Node2有兩個屬於SVM的資料生命期、分別是LIF1和LIF2、而且初始連線來自於LIF1。如果LIF1失敗、FPolicy會嘗試從LIF2建立控制通道。



FPolicy如何在**LIF**移轉或容錯移轉期間管理外部通訊

資料生命期可移轉至同一個節點的資料連接埠、或移轉至遠端節點的資料連接埠。

當資料LIF容錯移轉或移轉時、會建立新的控制通道連線至FPolicy伺服器。然後FPolicy可以重試逾時的SMB和NFS用戶端要求、並將新通知傳送至外部FPolicy伺服器。節點會拒絕FPolicy伺服器對原始、逾時SMB和NFS要求的回應。

FPolicy如何在節點容錯移轉期間管理外部通訊

如果裝載用於FPolicy通訊之資料連接埠的叢集節點故障、ONTAP 則無法中斷FPolicy伺服器與節點之間的連線。

透過設定容錯移轉原則、將 FPolicy 通訊中使用的資料連接埠移轉至另一個作用中節點、可減輕叢集容錯移轉至 FPolicy 伺服器的影響。移轉完成後、會使用新的資料連接埠建立新的連線。

如果未將容錯移轉原則設定為移轉資料連接埠、 FPolicy 伺服器必須等待故障節點啟動。節點啟動後、會使用新的工作階段ID從該節點啟動新的連線。

FPolicy伺服器會使用「保持作用中」傳輸協定訊息來偵測中斷的連線。清除工作階段ID的逾時是在設定FPolicy時決定。預設的「保持作用中」逾時為兩分鐘。

了解跨 **SVM** 命名空間的 **ONTAP FPolicy** 服務

提供統一化儲存虛擬機器（SVM）命名空間。ONTAP叢集內的磁碟區會透過連接點連接在一起、以提供單一的邏輯檔案系統。FPolicy伺服器知道命名空間拓撲、並在命名空間中提供FPolicy服務。

命名空間是特定於SVM並包含在SVM中、因此您只能從SVM內容中查看命名空間。命名空間具有下列特性：

- 每個SVM中都有一個命名空間、命名空間的根目錄為根磁碟區、在命名空間中以斜槓（/）表示。
- 所有其他磁碟區的交會點均低於根（/）。
- Volume交會對用戶端而言是透明的。
- 單一NFS匯出可提供完整命名空間的存取權、否則匯出原則可匯出特定磁碟區。
- SMB共用可在磁碟區或磁碟區內的qtree上建立、或是在命名空間內的任何目錄上建立。
- 命名空間架構具有彈性。

  典型命名空間架構的範例如下：

  - 具有根目錄外單一分支的命名空間
  - 具有多個根目錄分支的命名空間
  - 一個命名空間、其根部有多個未分支的磁碟區

ONTAP FPolicy 直通讀取如何增強分層儲存管理的可用性

Passthsthro-read可讓FPolicy伺服器（做為階層式儲存管理（HSM）伺服器）提供離線檔案的讀取存取權限、而不需要從次要儲存系統將檔案重新叫用至主要儲存系統。

當FPolicy伺服器設定為提供HSM給SMB伺服器上的檔案時、會發生原則型檔案移轉、檔案會離線儲存在次要儲存設備上、而且只有存根檔案保留在主要儲存設備上。雖然存根檔案對用戶端而言是正常檔案、但實際上是與原始檔案大小相同的稀疏檔案。該檔案設有SMB離線位元、並指向已移轉至次要儲存設備的實際檔案。

一般而言、當收到離線檔案的讀取要求時、必須將要求的內容重新叫用回主要儲存設備、然後再透過主要儲存設備存取。需要將資料重新叫用回主儲存設備、會產生幾種不良影響。其中不良的影響包括：回應要求前必須回收內容、導致用戶端要求延遲增加、以及主儲存設備上已回收檔案所需的空間使用量增加。

FPolicy Passthrough-read可讓HSM伺服器（FPolicy伺服器）提供移轉離線檔案的讀取存取權、而不需要從次要儲存系統將檔案重新叫用至主要儲存系統。讀取要求可直接從次要儲存設備處理、而非將檔案重新叫用回主要儲存設備。

FPolicy pass-read作業不支援複本卸載（ODX）。

Passthsther-read提供下列優點、可增強使用性：

- 即使主儲存設備沒有足夠空間可將要求的資料回收回主儲存設備、仍可處理讀取要求。
- 當發生大量的資料回收時（例如指令碼或備份解決方案需要存取許多離線檔案）、容量和效能管理會更好。
- 您可以處理快照中離線檔案的讀取要求。

  由於快照是唯讀的，因此如果存根檔案位於快照中， FPolicy 伺服器就無法還原原始檔案。使用Passthrough-read可消除此問題。

- 您可以設定原則、以控制何時透過存取次要儲存設備上的檔案來處理讀取要求、以及何時應將離線檔案重新叫用至主要儲存設備。

  例如、您可以在HSM伺服器上建立原則、指定在檔案移轉回主要儲存設備之前、於指定時間段內存取離線檔

案的次數。這類原則可避免重呼很少存取的檔案。

啟用**FPolicy Passthrough-read**時、如何管理讀取要求

您應該瞭解啟用FPolicy pass-read時如何管理讀取要求、以便最佳設定儲存虛擬機器（SVM）與FPolicy伺服器之間的連線。

啟用FPolicy Passthrough-read且SVM收到離線檔案的要求時、FPolicy會透過標準連線通道傳送通知給FPolicy伺服器（HSM伺服器）。

收到通知後、FPolicy伺服器會從通知中傳送的檔案路徑讀取資料、並透過SVM與FPolicy伺服器之間建立的Passthrough-read權限資料連線、將要求的資料傳送至SVM。

傳送資料後、FPolicy伺服器會以允許或拒絕的形式回應讀取要求。根據讀取要求是允許還是拒絕、ONTAP 所以無法傳送要求的資訊或傳送錯誤訊息給用戶端。

規劃**FPolicy**組態

配置 **ONTAP FPolicy** 的要求、注意事項和最佳實踐

在儲存虛擬機器（SVM）上建立及設定FPolicy組態之前、您必須瞭解設定FPolicy的特定需求、考量事項及最佳實務做法。

FPolicy 功能可透過命令列介面（ CLI ）或 REST API 進行設定。

設定**FPolicy**的需求

在儲存虛擬機器（SVM）上設定及啟用FPolicy之前、您必須先瞭解特定需求。

- 叢集中的所有節點都必須執行ONTAP 支援FPolicy的版本的功能。
- 如果您不使用ONTAP 本機的FPolicy引擎、則必須安裝外部FPolicy伺服器（FPolicy伺服器）。
- FPolicy伺服器必須安裝在可從啟用FPolicy原則的SVM資料生命區存取的伺服器上。

> 從 ONTAP 9 8 開始、 ONTAP 提供用戶端 LIF 服務 `data-fpolicy-client`、用於外傳 FPolicy 連線、並新增服務。"深入瞭解生命與服務原則"。

- FPolicy伺服器的IP位址必須在FPolicy原則外部引擎組態中設定為主要或次要伺服器。
- 如果FPolicy伺服器透過特殊權限的資料通道存取資料、則必須滿足下列額外需求：
  - SMB必須在叢集上獲得授權。

    特殊權限資料存取是使用SMB連線來完成。
  - 必須設定使用者認證、才能透過權限資料通道存取檔案。
  - FPolicy伺服器必須在FPolicy組態中設定的認證下執行。
  - 用於與 FPolicy 伺服器通訊的所有資料生命都必須設定為具有 `cifs` 作為其中一種允許的通訊協定。

    這包括用於傳遞讀取連線的lifs。

在儲存虛擬機器（ SVM ）上設定 FPolicy 時、請熟悉一般組態最佳實務做法和建議、以確保 FPolicy 組態能提供強大的監控效能和符合您需求的結果。

如需效能、規模調整及組態的特定準則、請與 FPolicy 合作夥伴應用程式合作。

持續儲存區

從 ONTAP 9.14.1 開始、 FPolicy 可讓您設定持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。不支援同步（強制或非強制）和非同步強制組態。

- 在使用持續儲存功能之前、請確保您的合作夥伴應用程式支援此組態。
- 每個啟用 FPolicy 的 SVM 都需要一個持續儲存區。
  - 每個 SVM 只能設定一個持續儲存區。此單一持續儲存區必須用於該 SVM 上的所有 FPolicy 組態、即使這些原則來自不同的合作夥伴。
- ONTAP 9.15.1 或更新版本：
  - 當您建立持續儲存區時、會自動處理持續儲存區、其磁碟區及其磁碟區組態。
- ONTAP 9.14.1 ：
  - 持續儲存區、其磁碟區及其磁碟區組態是手動處理的。
- 在節點上建立持續儲存區磁碟區、其中包含預期由 FPolicy 監控的最大流量。
  - ONTAP 9.15.1 或更新版本：磁碟區會在持續儲存區建立期間自動建立及設定。
  - ONTAP 9.14.1 ：叢集管理員必須在啟用 FPolicy 的每個 SVM 上建立及設定持續儲存區的磁碟區。
- 如果持續儲存區中累積的通知超過已配置的磁碟區大小、 FPolicy 就會開始以適當的 EMS 訊息來丟棄傳入通知。
  - ONTAP 9.15.1 或更新版本：除了 `size` 參數 `autosize-mode` 參數可協助磁碟區隨使用空間量而增加或縮小。
  - ONTAP 9.14.1 `size` 在磁碟區建立期間設定參數、以提供最大限制。
- 將 Snapshot 原則設為 `none` 用於永久儲存區 Volume 、而非 `default`。這是為了確保不會意外還原快照而導致目前事件遺失、並防止可能的重複事件處理。
  - ONTAP 9.15.1 或更新版本 `snapshot-policy` 在持續儲存區建立期間、參數會自動設定為無。
  - ONTAP 9.14.1 `snapshot-policy` 參數設定為 `none` 在磁碟區建立期間。
- 讓外部使用者傳輸協定存取（ CIFS/NFS ）無法存取持續儲存區磁碟區、以避免意外毀損或刪除持續存在的事件記錄。
  - ONTAP 9.15.1 或更新版本： ONTAP 會在持續儲存區建立期間、自動封鎖磁碟區、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。
  - ONTAP 9.14.1 ：啟用 FPolicy 之後、請在 ONTAP 中卸載 Volume 以移除連接路徑。這使得外部使用者傳輸協定存取（ CIFS/NFS ）無法存取。

如需詳細資訊、請參閱 "FPolicy 永續性儲存區" 和 "建立持續儲存區"。

持續儲存區容錯移轉和恢復

持續儲存區會維持上次收到事件、發生非預期的重新開機、或是停用 FPolicy 並再次啟用時的狀態。在接管作業之後、新事件會由合作夥伴節點儲存和處理。恢復作業完成後、持續儲存區會繼續處理任何未處理的事件、這些事件可能會在節點接管發生時保留。即時事件將優先於未處理的事件。

如果持久性儲存磁碟區從同一 SVM 中的一個節點移至另一個節點，則尚未處理的通知也會移至新節點。您需要重新運行 `fpolicy persistent-store create`移動磁碟區後，在任一節點上執行指令，以確保待處理的通知傳遞到外部伺服器。

詳細了解 `fpolicy persistent-store create`在"指令參考資料ONTAP" 。

原則組態

設定 FPolicy 外部引擎、事件和 SVM 範圍、可改善您的整體體驗和安全性。

- 設定 SVM 的 FPolicy 外部引擎：
  - 提供額外的安全性需要付出效能成本。啟用安全通訊端層（ SSL ）通訊對存取共用具有效能影響。
  - FPolicy 外部引擎應設定多個 FPolicy 伺服器、以提供 FPolicy 伺服器通知處理的恢復能力和高可用度。
- 設定 SVM 的 FPolicy 事件：

  監控檔案作業會影響您的整體體驗。例如、在儲存端篩選不想要的檔案作業、可改善您的使用體驗。NetApp 建議設定下列組態：

  - 監控檔案作業的最小類型、並在不中斷使用案例的情況下啟用最大篩選器數量。
  - 使用篩選器執行 getattr 、讀取、寫入、開啟及關閉作業。SMB 和 NFS 主目錄環境在這些作業中所佔的比例很高。
- SVM 的 FPolicy 範圍組態：

  將原則的範圍限制在相關的儲存物件上、例如共用、磁碟區和匯出、而非在整個 SVM 中啟用這些物件。NetApp 建議您檢查目錄副檔名。如果是 `is-file-extension-check-on-directories-enabled` 參數設定為 `true`，目錄物件會受到與一般檔案相同的副檔名檢查。

網路組態

FPolicy 伺服器與控制器之間的網路連線應為低延遲。NetApp 建議使用私有網路來分隔 FPolicy 流量與用戶端流量。

此外、您應該將外部 FPolicy 伺服器（ FPolicy 伺服器）放置在離具有高頻寬連線能力的叢集近的位置、以提供最小的延遲和高頻寬連線能力。

> 如果將 FPolicy 流量的 LIF 設定在與 LIF 不同的連接埠上、以進行用戶端流量、則 FPolicy LIF 可能會因為連接埠故障而容錯移轉至其他節點。因此、 FPolicy 伺服器無法從節點連線、導致 FPolicy 通知節點上的檔案作業失敗。若要避免此問題、請確認可透過節點上至少一個 LIF 來連線 FPolicy 伺服器、以處理在該節點上執行檔案作業的 FPolicy 要求。

硬體組態

您可以在實體伺服器或虛擬伺服器上使用 FPolicy 伺服器。如果 FPolicy 伺服器位於虛擬環境中、您應該將專用

資源（ CPU 、網路和記憶體）分配給虛擬伺服器。

叢集節點對FPolicy伺服器比率應最佳化、以確保FPolicy伺服器不會過載、這可能會在SVM回應用戶端要求時產生延遲。最佳比率取決於使用 FPolicy 伺服器的合作夥伴應用程式。NetApp 建議與合作夥伴合作、以確定適當的價值。

多原則組態

無論序號為何、原生封鎖的 FPolicy 原則都具有最高優先順序、而變更決策原則的優先順序比其他原則高。原則優先順序取決於使用案例。NetApp 建議與合作夥伴合作、以決定適當的優先順序。

規模考量

FPolicy 會執行 SMB 和 NFS 作業的即時監控、傳送通知給外部伺服器、並根據外部引擎通訊模式（同步或非同步）等待回應。此程序會影響 SMB 和 NFS 存取和 CPU 資源的效能。

為了減輕任何問題、 NetApp 建議您在啟用 FPolicy 之前、先與合作夥伴合作、評估環境並調整其規模。效能受到多種因素影響、包括使用者數量、工作負載特性、例如每位使用者的作業次數和資料大小、網路延遲、故障或伺服器速度緩慢。

監控效能

FPolicy 是以通知為基礎的系統。通知會傳送至外部伺服器以進行處理、並產生回覆 ONTAP 的回應。此往返程序會增加用戶端存取的延遲。

監控 FPolicy 伺服器和 ONTAP 中的效能計數器、可讓您識別解決方案中的瓶頸、並視需要調整參數、以獲得最佳解決方案。例如、 FPolicy 延遲增加會對 SMB 和 NFS 存取延遲造成串聯影響。因此、您應該同時監控工作負載（ SMB 和 NFS ）和 FPolicy 延遲。此外、您可以在 ONTAP 中使用服務品質原則、為每個啟用 FPolicy 的 Volume 或 SVM 設定工作負載。

NetApp 建議您執行 `statistics show -object workload` 顯示工作負載統計資料的命令。此外、您應該監控下列參數：

- 平均、讀取和寫入延遲
- 作業總數
- 讀寫計數器

您可以使用下列 FPolicy 計數器來監控 FPolicy 子系統的效能。

您必須處於診斷模式、才能收集與 FPolicy 相關的統計資料。

步驟

1. 收集 FPolicy 計數器：
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. 顯示 FPolicy 計數器：
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`

b. `statistics show -object fpolicy_server -instance <instance_name> -sample-id <ID>`

   ◦ `fpolicy` 和 `fpolicy_server` Counters 提供下表所述數種效能參數的相關資訊。

計數器	說明
*fpolicy 計數器 *	aborted_requests
在 SVM 上中止處理的畫面要求數	event_count
導致通知的事件清單	max_requent_l滯
最大螢幕要求延遲時間	未處理的要求
處理中的畫面要求總數	Processed_requests
在 SVM 上執行 fpolicy 處理的畫面要求總數	requy_histure_hist
畫面要求延遲長條圖	Requests_Dispatched_Rate
每秒發出的畫面要求數	Requests_receiped_rate
每秒接收的畫面要求數	*fpolicy_server counters *
max_requent_l滯	畫面要求的最大延遲
未處理的要求	等待回應的畫面要求總數
requy_l滯	畫面要求的平均延遲
requy_histure_hist	畫面要求延遲長條圖
requy_sent_rate	每秒傳送至 FPolicy 伺服器的畫面要求數
RESPONY_REATE_RATE	每秒從 FPolicy 伺服器收到的畫面回應數

深入瞭解 `statistics start`及 `statistics show` "指令參考資料ONTAP"。

管理 **FPolicy** 工作流程、並仰賴其他技術

NetApp 建議您先停用 FPolicy 原則、再進行任何組態變更。例如、如果您想要新增或修改為啟用原則設定的外部引擎中的 IP 位址、請先停用原則。

如果您將 FPolicy 設定為監控 NetApp FlexCache 磁碟區、 NetApp 建議您不要設定 FPolicy 來監控讀取和 getattr 檔案作業。在 ONTAP 中監控這些作業需要擷取 inode 到路徑（ I2P ）資料。由於 I2P 資料無法從 FlexCache 磁碟區擷取、因此必須從原始磁碟區擷取。因此、監控這些作業可免除 FlexCache 所能提供的效能效益。

當同時部署 FPolicy 和隨裝即用的防毒解決方案時、防毒解決方案會先收到通知。FPolicy 處理只會在防毒掃描完成後才會開始。請務必正確設定防毒解決方案的大小、因為慢速防毒掃描程式可能會影響整體效能。

Passthsther-read升級與還原考量

在升級ONTAP 至支援Passthrough-read的版本之前、或在回復至不支援passe-read的版本之前、您必須瞭解某些升級與還原考量事項。

升級

將所有節點升級至ONTAP 支援FPolicy Passthrough-read的版本後、叢集就能使用Passthrough-read功能；不過、在現有的FPolicy組態上、依預設會停用pass-read。若要在現有的FPolicy組態上使用passThrough讀取、您必須停用FPolicy原則並修改組態、然後重新啟用組態。

還原

還原至不支援 FPolicy Passthrough-read 的 ONTAP 版本之前、您必須符合下列條件：

- 使用 Passthrough-read 停用所有原則、然後修改受影響的組態、使其不使用 passthrough Read 。
- 停用叢集上的每個 FPolicy 原則、以停用叢集上的 FPolicy 功能。

在還原至不支援持續儲存區的 ONTAP 版本之前、請確定 FPolicy 原則中沒有任何一個具有設定的持續儲存區。如果設定持續儲存區、還原將會失敗。

相關資訊

- "統計數據顯示"
- "統計開始"

設定 **ONTAP FPolicy** 配置

在FPolicy能夠監控檔案存取之前、必須先在需要FPolicy服務的儲存虛擬機器（SVM）上建立並啟用FPolicy組態。

在SVM上設定及啟用FPolicy組態的步驟如下：

1. 建立FPolicy外部引擎。

   FPolicy外部引擎可識別與特定FPolicy組態相關聯的外部FPolicy伺服器（FPolicy伺服器）。如果使用內部的「原生」FPolicy引擎來建立原生檔案封鎖組態、則不需要建立FPolicy外部引擎。

   從 ONTAP 9.15.1 開始、您可以使用 `protobuf` 引擎格式。設定為時 `protobuf`、通知訊息會使用Google Prototbuf以二進位格式編碼。將引擎格式設定為之前 `protobuf`，請確保 FPolicy 伺服器也支援 `protobuf` 反序列化。如需詳細資訊、請參閱 "規劃FPolicy外部引擎組態"

2. 建立FPolicy事件。

   FPolicy事件說明FPolicy原則應監控的項目。事件包括要監控的傳輸協定和檔案作業、並可包含篩選器清單。事件使用篩選器來縮小FPolicy外部引擎必須傳送通知的受監控事件清單。事件也會指定原則是否監控Volume作業。

3. 建立 FPolicy 持續儲存區（選用）。

   從 ONTAP 9.14.1 開始、 FPolicy 可讓您進行設定 "持續儲存區" 擷取 SVM 中非強制性非非同步原則的檔案存取事件。不支援同步（強制或非強制）和非同步強制組態。

持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。

從 ONTAP 9.15.1 開始、 FPolicy 永續性儲存區組態已簡化。。 `persistent-store-create` 命令可自動建立 SVM 的 Volume 、並設定持續儲存區的 Volume 。

4. 建立FPolicy原則。

   FPolicy原則負責將需要監控的一組事件與適當範圍相關聯、以及哪些受監控的事件通知必須傳送至指定的FPolicy伺服器（若未設定FPolicy伺服器、則會傳送至原生引擎）。該原則也定義是否允許FPolicy伺服器以權限存取其接收通知的資料。如果伺服器需要存取資料、FPolicy伺服器就需要存取權限。需要存取權限的典型使用案例包括檔案封鎖、配額管理及階層式儲存管理。您可以在原則中指定此原則的組態是使用FPolicy伺服器、還是使用內部的「原生」FPolicy伺服器。

   原則會指定是否必須篩選。如果篩選是強制性的、且所有FPolicy伺服器都關閉、或在定義的逾時期間內、未從FPolicy伺服器收到任何回應、則檔案存取將遭拒。

   原則的界限是SVM。原則無法套用至多個SVM。不過、特定SVM可以有多個FPolicy原則、每個原則的範圍、事件和外部伺服器組態組合相同或不同。

5. 設定原則範圍。

   FPolicy範圍決定原則在哪些磁碟區、共享區或匯出原則上執行、或排除在監控範圍之外。範圍也會決定哪些副檔名應納入或排除在FPolicy監控範圍之外。

   排除清單優先於包含清單。

6. 啟用FPolicy原則。

   啟用原則時、會連接控制通道和（可選）特殊權限資料通道。SVM參與之節點上的FPolicy程序會開始監控檔案和資料夾存取、若事件符合設定的條件、則會將通知傳送至FPolicy伺服器（若未設定FPolicy伺服器、則會傳送至原生引擎）。

如果原則使用原生檔案封鎖、則不會設定外部引擎、也不會與原則建立關聯。

規劃**FPolicy**外部引擎組態

規劃 **ONTAP FPolicy** 外部引擎配置

設定 FPolicy 外部引擎之前、您必須先瞭解建立外部引擎的意義、以及哪些組態參數可供使用。此資訊可協助您判斷要為每個參數設定哪些值。

建立**FPolicy**外部引擎時所定義的資訊

外部引擎組態定義 FPolicy 需要建立及管理外部 FPolicy 伺服器連線的資訊、包括：

- SVM名稱
- 引擎名稱
- 主要和次要FPolicy伺服器的IP位址、以及連接至FPolicy伺服器時要使用的TCP連接埠號碼
- 引擎類型為非同步或同步

- 引擎格式是否為 `xml` 或 `protobuf`

  從 ONTAP 9.15.1 開始、您可以使用 `protobuf` 引擎格式。設定為時 `protobuf`、通知訊息會使用Google Prototbuf以二進位格式編碼。將引擎格式設定為之前 `protobuf`，請確保 FPolicy 伺服器也支援 `protobuf` 反序列化。

  由於支援的 probuf 格式從 ONTAP 9.15.1 開始、因此您必須先考慮外部引擎格式、才能還原至舊版 ONTAP 。如果您恢復為 ONTAP 9.15.1 之前的版本、請與 FPolicy 合作夥伴合作、以：

  - 從變更每個引擎格式 `protobuf` 至 `xml`
  - 刪除引擎格式為的引擎 `protobuf`

- 如何驗證節點與FPolicy伺服器之間的連線

  如果您選擇設定相互SSL驗證、則也必須設定提供SSL憑證資訊的參數。

- 如何使用各種進階權限設定來管理連線

  這包括定義逾時值、重試值、保持活動值、最大要求值、傳送和接收緩衝區大小值、以及工作階段逾時值等項目的參數。

。 `vserver fpolicy policy external-engine create` 命令用於建立 FPolicy 外部引擎。

基本的外部引擎參數是什麼

您可以使用下表的基本FPolicy組態參數來協助規劃組態：

資訊類型	選項
SVM 指定您要與此外部引擎建立關聯的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`

引擎名稱_ 指定要指派給外部引擎組態的名稱。之後建立FPolicy原則時、您必須指定外部引擎名稱。這會將外部引擎與原則建立關聯。 名稱最長可達256個字元。 如果在MetroCluster 一個還原或SVM災難恢復組態中設定外部引擎名稱、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • “_” 、 “-”, and “.”	`-engine-name engine_name`
主要*FPolicy*伺服器 指定節點傳送特定FPolicy原則通知的主要FPolicy伺服器。此值會指定為以逗號分隔的IP位址清單。 如果指定多個主要伺服器IP位址、則SVM參與的每個節點都會在原則啟用時、建立每個指定主要FPolicy伺服器的控制連線。如果您設定多個主要FPolicy伺服器、通知會以循環配置資源的方式傳送至FPolicy伺服器。 如果外部引擎用於MetroCluster SVM災難恢復組態、您應該將來源站台FPolicy伺服器的IP位址指定為主要伺服器。目的地站台FPolicy伺服器的IP位址應指定為次要伺服器。	`-primary-servers IP_address、 ...`
連接埠號碼_ 指定FPolicy服務的連接埠號碼。	`-port integer`
次要FPolicy伺服器_ 指定次要FPolicy伺服器、以便針對指定的FPolicy原則傳送檔案存取事件。此值會指定為以逗號分隔的IP位址清單。 次要伺服器只會在無法連線到任何一部主要伺服器時使用。當原則啟用時、就會建立次要伺服器的連線、但只有在所有主要伺服器都無法連線時、才會將通知傳送到次要伺服器。如果您設定多個次要伺服器、通知會以循環配置資源的方式傳送至FPolicy伺服器。	`-secondary-servers IP_address、 ...`

外部引擎類型_ 指定外部引擎是以同步或非同步模式運作。根據預設、FPolicy會以同步模式運作。 設定為時 `synchronous`、檔案要求處理會傳送通知給 FPolicy 伺服器、但在收到 FPolicy 伺服器的回應之後才會繼續。此時、視FPolicy伺服器的回應是否允許要求的動作而定、要求流程會繼續或處理會導致拒絕。 設定為時 `asynchronous`、檔案要求處理會傳送通知給 FPolicy 伺服器、然後繼續。	`-extern-engine-type external_engine_type` 此參數的值可以是下列其中一項： • `synchronous` • `asynchronous`
外部引擎格式_ 指定外部引擎格式是 XML 還是 protobuf 。 從 ONTAP 9.15.1 開始、您可以使用原型引擎格式。設為 probuf 時、通知訊息會使用 Google Prototbuf 以二進位格式編碼。在將引擎格式設定為 protobuf 之前、請確定 FPolicy 伺服器也支援 protobuf 反序列化。	`- extern-engine-format {protobuf 或 xml}`
與FPolicy server_通訊的_SSL選項 指定與FPolicy伺服器通訊的SSL選項。這是必要的參數。您可以根據下列資訊選擇其中一個選項： • 設定為時 `no-auth`、不進行驗證。 通訊連結是透過TCP建立。 • 設定為時 `server-auth`， SVM 使用 SSL 伺服器驗證來驗證 FPolicy 伺服器。 • 設定為時 `mutual-auth`、在 SVM 和 FPolicy 伺服器之間進行相互驗證；SVM 驗證 FPolicy 伺服器、 FPolicy 伺服器驗證 SVM 。 如果您選擇設定相互 SSL 驗證、則也必須設定 `-certificate -common-name`、 `-certificate-serial`和 `-certifcate-ca` 參數。	`-ssl-option {no-auth`
`server-auth`	`mutual-auth}`
憑證*FQDN*或自訂通用名稱 指定在SVM與FPolicy伺服器之間設定SSL驗證時所使用的憑證名稱。您可以將憑證名稱指定為FQDN或自訂通用名稱。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-common-name` 參數。	`-certificate-common -name text`

憑證序號 指定在SVM與FPolicy伺服器之間設定SSL驗證時、用於驗證的憑證序號。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-serial` 參數。	`-certificate-serial text`
憑證授權單位 指定在SVM與FPolicy伺服器之間設定SSL驗證時、用於驗證的憑證CA名稱。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-ca` 參數。	`-certificate-ca text`

進階的外部引擎選項是什麼

您可以在規劃是否使用進階參數自訂組態時、使用下表的進階FPolicy組態參數。您可以使用這些參數來修改叢集節點與FPolicy伺服器之間的通訊行為：

資訊類型	選項
取消要求的逾時_ 指定時間間隔（小時） (`h`）、分鐘 (`m`）或秒 (`s`）節點等待 FPolicy 伺服器的回應。 如果逾時時間間隔超過、節點會將取消要求傳送至FPolicy伺服器。然後、節點會將通知傳送至替代的FPolicy伺服器。此逾時有助於處理無回應的FPolicy伺服器、進而改善SMB/NFS用戶端回應。此外、在逾時期間之後取消要求、也有助於釋出系統資源、因為通知要求會從停機/不良的FPolicy伺服器移至替代的FPolicy伺服器。 此值的範圍為 `0` 透過 `100`。如果值設為 `0`，此選項已停用，取消要求訊息不會傳送至 FPolicy 伺服器。預設值為 `20s`。	`-reqs-cancel-timeout integer`[h
m	s]
中止要求的逾時_ 指定逾時（以小時為單位） (`h`）、分鐘 (`m`）或秒 (`s`）以中止要求。 此值的範圍為 `0` 透過 `200`。	`-reqs-abort-timeout ` `integer`[h
m	s]

傳送狀態要求的時間間隔 指定以小時為單位的時間間隔 (h）、分鐘 (m）或秒 (s）之後、狀態要求會傳送至 FPolicy 伺服器。 此值的範圍為 0 透過 50。如果值設為 0、選項已停用、狀態要求訊息不會傳送至 FPolicy 伺服器。預設值為 10s。	`-status-req-interval integer`[h
m	s]
*FPolicy*伺服器上未處理的要求上限 指定可在FPolicy伺服器上排入佇列的未處理要求數目上限。 此值的範圍為 1 透過 10000。預設值為 500。	`-max-server-reqs integer`
中斷無回應的*FPolicy*伺服器連線逾時 指定時間間隔（小時）(h）、分鐘 (m）或秒 (s）之後、會終止與 FPolicy 伺服器的連線。 只有FPolicy伺服器的佇列包含允許的最大要求數、且在逾時期間內未收到任何回應時、才會在逾時期間之後終止連線。允許的最大要求數為其中之一 50（預設）或指定的號碼 `max-server-reqs-` 參數。 此值的範圍為 1 透過 100。預設值為 60s。	`-server-progress -timeout integer`[h
m	s]
_將保持活動訊息傳送至FPolicy server_的時間間隔 指定時間間隔（小時）(h）、分鐘 (m）或秒 (s）將保持活動的訊息傳送到 FPolicy 伺服器。 「保持連線」訊息會偵測半開啟的連線。 此值的範圍為 10 透過 600。如果值設為 0，此選項會停用，並防止將持續作用的訊息傳送至 FPolicy 伺服器。預設值為 120s。	`-keep-alive-interval- integer`[h
m	s]
最大重新連線嘗試次數_ 指定SVM在連線中斷後嘗試重新連線至FPolicy伺服器的最大次數。 此值的範圍為 0 透過 20。預設值為 5。	`-max-connection-retries integer`

接收緩衝區大小_ 指定FPolicy伺服器之連接插槽的接收緩衝區大小。 預設值設為256 KB。當值設定為0時、接收緩衝區的大小會設定為系統定義的值。 例如、如果套接字的預設接收緩衝區大小為65536位元組、將可調值設為0、則套接字緩衝區大小會設為65536位元組。您可以使用任何非預設值來設定接收緩衝區的大小（以位元組為單位）。	`-recv-buffer-size integer`
傳送緩衝區大小 指定FPolicy伺服器之連線通訊端的傳送緩衝區大小。 預設值設為256 KB。當值設定為0時、傳送緩衝區的大小會設定為系統定義的值。 例如、如果套接字的預設傳送緩衝區大小設為65536位元組、將可調值設為0、則套接字緩衝區大小會設為65536位元組。您可以使用任何非預設值來設定傳送緩衝區的大小（以位元組為單位）。	`-send-buffer-size integer`
重新連線期間清除工作階段*ID*逾時 指定以小時為單位的時間間隔 (`h`）、分鐘 (`m`）或秒 (`s`）之後、新的工作階段 ID 會在重新連線嘗試期間傳送至 FPolicy 伺服器。 如果儲存控制器與FPolicy伺服器之間的連線終止、並在中進行重新連線 `-session-timeout` 時間間隔時、舊的工作階段ID會傳送至FPolicy伺服器、以便傳送舊通知的回應。 預設值設為 10 秒。	`-session-timeout [integerh][integerM][integers]`

有關配置 **ONTAP FPolicy** 外部引擎以使用 **SSL** 身份驗證連接的其他信息

如果您想要設定FPolicy外部引擎、以便在連線至FPolicy伺服器時使用SSL、您需要知道一些其他資訊。

SSL伺服器驗證

如果您選擇將FPolicy外部引擎設定為SSL伺服器驗證、則在建立外部引擎之前、必須先安裝簽署FPolicy伺服器憑證的憑證授權單位（CA）的公開憑證。

相互驗證

如果您將FPolicy外部引擎設定為在將儲存虛擬機器（SVM）資料LIF連線至外部FPolicy伺服器時使用SSL相互驗證、則在建立外部引擎之前、 您必須安裝簽署FPolicy伺服器憑證的CA公開憑證、以及用於驗證SVM的公開憑證和金鑰檔。當任何 FPolicy 原則使用已安裝的憑證時，請勿刪除此憑證。

如果在FPolicy連線至外部FPolicy伺服器時、憑證被刪除、則無法重新啟用使用該憑證的停用FPolicy原則。在這

種情況下、即使在SVM上建立並安裝了具有相同設定的新憑證、也無法重新啟用FPolicy原則。

如果憑證已刪除、您需要安裝新的憑證、建立使用新憑證的新FPolicy外部引擎、並透過修改FPolicy原則、將新的外部引擎與您要重新啟用的FPolicy原則建立關聯。

安裝**SSL**憑證

用來簽署 FPolicy 伺服器憑證的 CA 公用憑證是使用安裝 `security certificate install` 命令 `-type` 參數設為 `client-ca`。使用安裝驗證 SVM 所需的私密金鑰和公開憑證 `security certificate install` 命令 `-type` 參數設為 `server`。

相關資訊

- "安全性憑證安裝"

ONTAP FPolicy 憑證不會在具有非 **ID** 保留配置的 **SVM** 災難復原關係中複製

連線至FPolicy伺服器時用於SSL驗證的安全性憑證、不會以非ID-preserve組態複寫至SVM災難恢復目的地。雖然已複寫SVM上的FPolicy外部引擎組態、但不會複寫安全性憑證。您必須在目的地上手動安裝安全性憑證。

當您設定 SVM 災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、所有 FPolicy 組態詳細資料都會複寫、包括安全性憑證資訊。只有當您將選項設定為時、才必須在目的地上安裝安全性憑證 `false` （非 ID-Preserve ）。

相關資訊

- "SnapMirror建立"

具有 **MetroCluster** 和 **SVM** 災難復原配置的叢集範圍 **ONTAP FPolicy** 外部引擎的限制

您可以將叢集儲存虛擬機器（SVM）指派給外部引擎、藉此建立叢集範圍內的FPolicy外部引擎。然而、在MetroCluster 使用叢集或SVM災難恢復組態建立以叢集為範圍的外部引擎時、選擇SVM用於與FPolicy伺服器進行外部通訊的驗證方法時、會有某些限制。

建立外部FPolicy伺服器時、您可以選擇三種驗證選項：無驗證、SSL伺服器驗證和SSL相互驗證。雖然在選擇驗證選項時沒有任何限制、但如果將外部FPolicy伺服器指派給資料SVM、則在建立叢集範圍的FPolicy外部引擎時仍有限制：

組態	是否允許？
不含驗證的SVM災難恢復和叢集範圍的FPolicy外部引擎（未設定SSL）MetroCluster	是的
包含SSL伺服器或SSL相互驗證的SVM災難恢復、以及叢集範圍的FPolicy外部引擎MetroCluster	否

- 如果存在具有SSL驗證的叢集範圍FPolicy外部引擎、而您想要建立MetroCluster 一套支援還原或SVM災難恢復的組態、您必須先修改此外部引擎、使其不使用驗證、或是移除外部引擎、才能建立MetroCluster 還原

或SVM災難恢復組態。

- 如果MetroCluster 已存在支援功能的不支援功能或SVM災難恢復組態、ONTAP 則無法使用SSL驗證來建立叢集範圍的FPolicy外部引擎。

完成 **ONTAP FPolicy** 外部引擎設定工作表

您可以使用這份工作表來記錄FPolicy外部引擎組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的使用值、再設定外部引擎。

基本外部引擎組態資訊

您應該記錄是否要在外部引擎組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
引擎名稱	是的	是的	
主要FPolicy伺服器	是的	是的	
連接埠號碼	是的	是的	
次要FPolicy伺服器	否		
外部引擎類型	否		
用於與外部FPolicy伺服器通訊的SSL選項	是的	是的	
憑證FQDN或自訂通用名稱	否		
憑證序號	否		
憑證授權單位	否		

進階外部引擎參數資訊

若要使用進階參數設定外部引擎、您必須在進階權限模式下輸入組態命令。

資訊類型	必要	包括	您的價值
取消要求逾時	否		
中止要求的逾時	否		

傳送狀態要求的時間間隔	否		
FPolicy伺服器上未處理的要求上限	否		
中斷無回應的FPolicy伺服器連線逾時	否		
將「保持作用中」訊息傳送至FPolicy伺服器的時間間隔	否		
最大重新連線嘗試次數	否		
接收緩衝區大小	否		
傳送緩衝區大小	否		
重新連線期間清除工作階段ID的逾時	否		

規劃**FPolicy**事件組態

瞭解 **ONTAP FPolicy** 事件組態

在設定FPolicy事件之前、您必須先瞭解建立FPolicy事件的意義。您必須決定要監控事件的傳輸協定、要監控的事件、以及要使用的事件篩選器。此資訊可協助您規劃要設定的值。

建立**FPolicy**事件的意義

建立FPolicy事件是指定義FPolicy程序所需的資訊、以決定要監控的檔案存取作業、以及應將哪些受監控事件通知傳送至外部FPolicy伺服器。FPolicy事件組態定義下列組態資訊：

- 儲存虛擬機器（SVM）名稱
- 事件名稱
- 要監控的傳輸協定

  FPolicy 可監控 SMB ， NFSv3 ， NFSv4 ，以及從 ONTAP 9.15.1 開始的 NFSv4.1 檔案存取作業。

- 要監控的檔案作業

  並非所有檔案作業都適用於每個傳輸協定。

- 要設定哪些檔案篩選器

  只有特定的檔案作業與篩選組合有效。每個傳輸協定都有自己的一組支援組合。

- 是否要監控磁碟區掛載和卸載作業

其中三個參數有相依性 (`-protocol`、 `-file-operations`、 `-filters`）。下列組合對三個參數有效：

- 您可以指定 `-protocol` 和 `-file-operations` 參數。
- 您可以指定全部三個參數。
- 您不能指定任何參數。

FPolicy事件組態包含的內容

您可以使用下列可用的FPolicy事件組態參數清單來協助規劃組態：

資訊類型	選項
SVM 指定您要與此FPolicy事件相關聯的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`
事件名稱_ 指定要指派給FPolicy事件的名稱。當您建立FPolicy原則時、會使用事件名稱將FPolicy事件與原則建立關聯。 名稱最長可達256個字元。 如果在MetroCluster 還原或SVM災難恢復組態中設定事件、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • "_"、"-`", and “.”	`-event-name event_name`

傳輸協定 指定要為FPolicy事件設定的傳輸協定。的清單 `-protocol` 可以包含下列其中一個值： • `cifs` • `nfsv3` • `nfsv4` 如果您指定 `-protocol`、然後您必須在中指定有效值 `-file-operations` 參數。隨著傳輸協定版本變更、有效值可能會變更。 從 ONTAP 9.15.1 開始， NFSv4 可讓您擷取 NFSv4.0 和 NFSv4.1 事件。	`-protocol protocol`

_File operations _ 指定FPolicy事件的檔案作業清單。 事件會使用中指定的通訊協定、從所有用戶端要求檢查此清單中指定的作業 `-protocol` 參數。您可以使用以逗號分隔的清單來列出一或多個檔案作業。的清單 `-file-operations` 可以包含下列一或多個值： • `close` 用於檔案關閉作業 • `create` 用於檔案建立作業 • `create-dir` 用於目錄建立作業 • `delete` 用於檔案刪除作業 • `delete_dir` 用於目錄刪除作業 • `getattr` 以取得屬性作業 • `link` 用於連結作業 • `lookup` 用於查詢作業 • `open` 適用於檔案開啟作業 • `read` 檔案讀取作業 • `write` 適用於檔案寫入作業 • `rename` 用於檔案重新命名作業 • `rename_dir` 用於目錄重新命名作業 • `setattr` 用於 Set 屬性作業 • `symlink` 用於符號連結作業 如果您指定 `-file-operations`、然後您必須在中指定有效的傳輸協定 `-protocol` 參數。	`-file-operations file_operations、 ...`

篩選 指定指定傳輸協定之特定檔案作業的篩選器清單。中的值 `-filters` 參數用於篩選用戶端要求。清單可包含下列一項或多項內容： 如果您指定 `-filters` 參數、您也必須為指定有效值 `-file-operations` 和 `-protocol` 參數。 • `monitor-ads` 用於篩選用戶端要求的替代資料串流選項。 • `close-with-modification` 篩選用戶端要求以進行修改以關閉的選項。 • `close-without-modification` 篩選用戶端要求以關閉而不修改的選項。 • `first-read` 篩選用戶端要求以進行第一讀取的選項。 • `first-write` 篩選用戶端要求進行第一次寫入的選項。 • `offline-bit` 用於篩選用戶端離線位元集要求的選項。 設定此篩選器後、FPolicy伺服器只會在存取離線檔案時收到通知。 • `open-with-delete-intent` 用於篩選用戶端要求以進行「刪除目的」開啟的選項。 設定此篩選器後、FPolicy伺服器只會在嘗試開啟檔案以刪除檔案時收到通知。檔案系統會在使用時使用此功能 `FILE_DELETE_ON_CLOSE` 已指定旗標。 • `open-with-write-intent` 篩選用戶端要求以進行寫入目的開啟的選項。 設定此篩選器後、FPolicy伺服器只會在嘗試開啟檔案時收到通知、以便在其中寫入內容。 • `write-with-size-change` 選項可篩選用戶端寫入要求、並變更大小。 • `setattr-with-owner-change` 用於篩選用戶端設定檔要求以變更檔案或目錄擁有者的選項。 • `setattr-with-group-change` 用於篩選用戶端集點要求以變更檔案或目錄群組的選項。 • `setattr-with-sacl-change` 用於篩選用戶端集點要求以變更檔案或目錄上的 SACL 的選項。 此篩選器僅適用於SMB和NFSv4傳輸協定。 • `setattr-with-dacl-change` 用於篩選用戶端集點要求以變更檔案或目錄上的 DACL 的選項。 此篩選器僅適用於SMB和NFSv4傳輸協定。 `setattr-with-modify-time-change` 用於篩選用戶端 setattr 要求以變更檔案或目錄的修改時間的選項。 `setattr-with-access-time-change` 用於篩選用戶端 setattr 要求	`-filters filter、 ...`

需要磁碟區作業 指定磁碟區掛載和卸載作業是否需要監控。預設值為 `false`。	`-volume-operation {true`

`false}`
 	
`-filters filter、 ...`
	_FPolicy 存取遭拒通知 _
	
	從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。這些通知對於安全性、勒索軟體保護和治理來說非常重要。由於缺乏權限、將會產生檔案作業失敗的通知、其中包括：
	
	• NTFS 權限導致的失敗。
	• 因 Unix 模式位元而發生故障。
	• NFSv4 ACL 導致故障。

`-monitor-fileop-failure {true`	`false}`

ONTAP FPolicy 監控 **SMB** 支援的檔案操作和過濾器組合

設定FPolicy事件時、您必須注意、監控SMB檔案存取作業時、僅支援特定的檔案作業和篩選器組合。

下表提供了用於監控SMB檔案存取事件的FPolicy支援檔案操作和篩選器組合清單：

支援的檔案作業	支援的篩選器
關閉	監控廣告、離線位元、近距離修改、近距離不需修改、近距離讀取、 exclude目錄
建立	監控廣告、離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	監控廣告、離線位元
刪除目錄	目前此檔案作業不支援篩選器。
GetAttr	離線位元、exclude目錄
開啟	監控廣告、離線位元、開放刪除意圖、開放寫入目的、排除目錄

讀取	監控廣告、離線位元、第一讀取
寫入	監控廣告、離線位元、第一寫入、大小變更寫入
重新命名	監控廣告、離線位元
重新命名目錄	目前此檔案作業不支援篩選器。
設定	監控廣告、離線位元、設定ATtr_with _Owner_change、設定ATr_with _group_change、設定ATtr_with _mode_change、 setattr_with _SACL_change、setattr_with _dacl_change、setattr_with _dmodify_time_change、setattr_with _access_time_change、setattr_with creation_time_change、 setattr_with _size_change、setattr_with _all撥款_size_change、exclude目錄

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的存取遭拒檔案作業清單、以及 FPolicy 監控 SMB 檔案存取事件的篩選器組合：

支援的存取遭拒檔案作業	支援的篩選器
開啟	不適用

ONTAP FPolicy 為 **NFSv3** 監控的支援的檔案操作和過濾器組合

當您設定 FPolicy 事件時、您必須注意、只有特定的檔案作業和篩選器組合才支援監控 NFSv3 檔案存取作業。

下表提供支援的檔案作業清單、以及 FPolicy 監控 NFSv3 檔案存取事件的篩選組合：

支援的檔案作業	支援的篩選器
建立	離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	離線位元
刪除目錄	目前此檔案作業不支援篩選器。
連結	離線位元
查詢	離線位元、exclude目錄
讀取	離線位元、第一讀取

寫入	離線位元、第一寫入、大小變更寫入
重新命名	離線位元
重新命名目錄	目前此檔案作業不支援篩選器。
設定	離線位元、設定attr_with _Owner_change、設定attr_with _group變更、設定attr_with模式變更、設定ATtr_with修改時間變更、 setattr_with存取時間變更、setattr_with _size_change、exclude目錄
symlink	離線位元

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的拒絕存取檔案作業清單、以及 FPolicy 監控 NFSv3 檔案存取事件的篩選組合：

支援的存取遭拒檔案作業	支援的篩選器
存取	不適用
建立	不適用
create_dir	不適用
刪除	不適用
刪除目錄	不適用
連結	不適用
讀取	不適用
重新命名	不適用
重新命名目錄	不適用
設定	不適用
寫入	不適用

ONTAP FPolicy 為 **NFSv4** 監控的支援的檔案操作和過濾器組合

設定FPolicy事件時、您必須注意、監控NFSv4檔案存取作業時、僅支援特定的檔案作業和篩選器組合。

從 ONTAP 9.15.1 開始、 FPolicy 支援 NFSv4.1 傳輸協定。

下表提供 NFSv4 或 NFSv4.1 檔案存取事件的 FPolicy 監控支援檔案作業和篩選器組合清單：

支援的檔案作業	支援的篩選器
關閉	離線位元、排除目錄
建立	離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	離線位元
刪除目錄	目前此檔案作業不支援篩選器。
GetAttr	離線位元、排除目錄
連結	離線位元
查詢	離線位元、排除目錄
開啟	離線位元、排除目錄
讀取	離線位元、第一讀取
寫入	離線位元、第一寫入、大小變更寫入
重新命名	離線位元
重新命名目錄	目前此檔案作業不支援篩選器。
設定	離線位元、設定attr_with _Owner_change、設定attr_with _group變更、設定ATr_with模式變更、設定ATtr_with _SACL_change、 setattr_with _dacl_change、setattr_with _dmodify_time_change、setattr_with _access_time_change、setattr_with _size_change、exclude目錄
symlink	離線位元

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的拒絕存取檔案作業清單、以及 FPolicy 監控 NFSv4 或 NFSv4.1 檔案存取事件的篩選組合：

支援的存取遭拒檔案作業	支援的篩選器
存取	不適用

建立	不適用
create_dir	不適用
刪除	不適用
刪除目錄	不適用
連結	不適用
開啟	不適用
讀取	不適用
重新命名	不適用
重新命名目錄	不適用
設定	不適用
寫入	不適用

完成 **ONTAP FPolicy** 事件設定工作表

您可以使用這份工作表單來記錄FPolicy事件組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的值、再設定FPolicy事件。

您應該記錄是否要在FPolicy事件組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
事件名稱	是的	是的	
傳輸協定	否		
檔案作業	否		
篩選器	否		
Volume作業	否		

存取遭拒事件 （從 ONTAP 9.13 開始支援）	否		

規劃FPolicy原則組態

了解 ONTAP FPolicy 策略配置

在設定FPolicy原則之前、您必須先瞭解建立原則時需要哪些參數、以及設定某些選用參數的原因。此資訊可協助您判斷要為每個參數設定哪些值。

建立FPolicy原則時、您會將原則與下列項目建立關聯：

- 儲存虛擬機器（SVM）
- 一或多個FPolicy事件
- FPolicy外部引擎

您也可以設定多個選用的原則設定。

FPolicy原則組態包含的內容

您可以使用下列可用的必要FPolicy原則清單和選用參數來協助規劃組態：

資訊類型	選項	必要	預設
*SVM*名稱 指定您要在其中建立FPolicy原則的SVM名稱。	`-vserver vserver_name`	是的	無

原則名稱 指定FPolicy原則的名稱。 名稱最長可達256個字元。 如果在MetroCluster 還原或SVM災難恢復組態中設定原則、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • a 透過 z • A 透過 Z • 0 透過 9 • “_” 、 “-”, and “.”	`-policy-name policy_name`	是的	無
事件名稱_ 指定要與FPolicy原則相關聯的以逗號分隔的事件清單。 • 您可以將多個事件與原則建立關聯。 • 事件是特定於傳輸協定的事件。 • 您可以使用單一原則來監控多個傳輸協定的檔案存取事件、方法是針對您要原則監控的每個傳輸協定建立事件、然後將事件與原則建立關聯。 • 事件必須已經存在。	`-events event_name、 ...`	是的	無
Persistent stority 從 ONTAP 9.14.1 開始、此參數會指定持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。	`-persistent -store persistent_store_name`	否	無

外部引擎名稱_ 指定要與FPolicy原則關聯的外部引擎名稱。 • 外部引擎包含節點傳送通知至FPolicy伺服器所需的資訊。 • 您可以將FPolicy設定為使用ONTAP 靜態原生外部引擎來進行簡單的檔案封鎖、或是使用外部引擎來設定使用外部FPolicy伺服器（FPolicy伺服器）來進行更精密的檔案封鎖和檔案管理。 • 如果您想要使用原生外部引擎、則無法指定此參數的值、也可以指定 `native` 做為價值。 • 如果您要使用FPolicy伺服器、則外部引擎的組態必須已經存在。	`-engine engine_name`	是（除非原則使用內部ONTAP 的非原生引擎）	`native`
是必填篩選 指定是否需要強制檔案存取篩選。 • 強制篩選設定可決定當所有主要和次要伺服器都當機、或在指定的逾時期間內未收到FPolicy伺服器的回應時、檔案存取事件會採取什麼行動。 • 設定為時 `true`、檔案存取事件遭拒。 • 設定為時 `false`，允許檔案存取事件。	`-is-mandatory {true`	`false}`	否

true	允許權限存取_ 指定您是否要FPolicy伺服器使用權限資料連線、以具有存取受監控檔案和資料夾的權限。 如果設定、FPolicy伺服器可以使用權限資料連線、從SVM的根目錄存取包含受監控資料的檔案。 若要進行特殊權限的資料存取、必須在叢集上授權 SMB 、且必須將用於連線至 FPolicy 伺服器的所有資料生命體設定為具有 `cifs` 作為其中一種允許的通訊協定。 如果您想要設定原則以允許權限存取、也必須為您想要FPolicy伺服器用於權限存取的帳戶指定使用者名稱。	`-allow -privileged -access {yes`	`no}`
否（除非啟用Passthrough-read）	`no`	特殊權限使用者名稱 指定FPolicy伺服器用來存取特殊權限資料的帳戶使用者名稱。 • 此參數的值應使用「'domain\username'」格式。 • 如果 `-allow -privileged -access` 設為 `no`，將忽略爲此參數設置的任何值。	`-privileged -user-name user_name`

否（除非已啟用權限存取）	無	允許Passthrough-read_ 指定FPolicy伺服器是否能為FPolicy伺服器歸檔至次要儲存設備（離線檔案）的檔案提供Passter-Read服務： • Passthsther-read是一種讀取離線檔案資料的方法、無需將資料還原至主要儲存設備。 Passthroh-read可減少回應延遲、因為在回應讀取要求之前、不需要將檔案重新叫用回主要儲存設備。此外、Passthrough-read可免除使用僅為了滿足讀取要求而回收的檔案來耗用主要儲存空間的需求、藉此優化儲存效率。 • 啟用時、FPolicy伺服器會透過專為Passthrough-Reads所開啟的個別特殊權限資料通道、提供檔案的資料。 • 如果您想要設定Passthrough-read、也必須將原則設定為允許權限存取。	`-is-passthrough-read-enabled {true`

如果 **FPolicy** 政策使用本機引擎，則需要 **ONTAP FPolicy** 範圍配置

如果您將FPolicy原則設定為使用原生引擎、則需要針對原則設定的FPolicy範圍進行定義。

FPolicy範圍會定義套用FPolicy原則的界限、例如FPolicy是否套用至指定的磁碟區或共用區。有許多參數會進一步限制FPolicy原則套用的範圍。其中一個參數、 `-is-file-extension-check-on-directories`

`-enabled`，指定是否檢查目錄上的副檔名。預設值為 `false`，這表示不會檢查目錄上的副檔名。

當使用原生引擎的 FPolicy 原則在共用區或磁碟區和上啟用時 `-is-file-extension-check-on-directories-enabled` 參數設定為 `false` 對於原則的範圍、目錄存取會被拒絕。使用此組態時、因為不會檢查目錄的副檔名、所以如果目錄作業屬於原則範圍、則會拒絕任何目錄作業。

若要確保使用原生引擎時目錄存取成功、您必須設定 `-is-file-extension-check-on-directories-enabled parameter` 至 `true` 建立範圍時。

將此參數設為 `true`、會針對目錄作業進行延伸檢查、並根據 FPolicy 範圍組態中所包含或排除的延伸來決定是否允許或拒絕存取。

完成 **ONTAP FPolicy** 策略工作表

您可以使用這份工作表單來記錄FPolicy原則組態程序期間所需的值。您應該記錄是否要在FPolicy原則組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	
原則名稱	是的	
事件名稱	是的	
持續儲存區		
外部引擎名稱		
是否需要強制篩選？		
允許特殊權限存取		
權限使用者名稱		
是否已啟用Passthrough-read？		

規劃**FPolicy**範圍組態

了解 **ONTAP FPolicy** 範圍配置

在設定FPolicy範圍之前、您必須先瞭解建立範圍的意義。您必須瞭解範圍組態包含哪些內容。您也需要瞭解優先順序的範圍規則。此資訊可協助您規劃要設定的值。

建立**FPolicy**範圍的意義

建立FPolicy範圍是指定義套用FPolicy原則的界限。儲存虛擬機器（SVM）是基本邊界。當您建立FPolicy原則的

範圍時、必須定義要套用該原則的FPolicy原則、而且必須指定要套用範圍的SVM。

有許多參數會進一步限制指定SVM內的範圍。您可以指定要納入範圍的內容、或指定要從範圍中排除的項目、來限制範圍。將範圍套用至已啟用的原則之後、原則事件檢查就會套用至此命令所定義的範圍。

系統會針對檔案存取事件產生通知、其中「include'」選項中有相符項目。不會針對檔案存取事件產生通知、其中「exclude」選項中有相符項目。

FPolicy範圍組態定義下列組態資訊：

- SVM名稱
- 原則名稱
- 要納入或排除的共享區
- 匯出原則、以納入或排除受監控的內容
- 要納入或排除的磁碟區
- 要納入或排除的檔案副檔名
- 是否對目錄物件進行檔案副檔名檢查

> 叢集FPolicy原則的範圍有特殊考量。叢集FPolicy原則是叢集管理員為管理SVM所建立的原則。如果叢集管理員也為該叢集FPolicy原則建立範圍、則SVM管理員無法為該相同原則建立範圍。但是、如果叢集管理員未建立叢集FPolicy原則的範圍、則任何SVM管理員都可以建立該叢集原則的範圍。如果SVM管理員為該叢集FPolicy原則建立範圍、叢集管理員便無法隨後為該相同的叢集原則建立叢集範圍。這是因為叢集管理員無法覆寫同一個叢集原則的範圍。

優先順序的範圍規則為何

下列優先規則適用於範圍組態：

- 當共享區包含在中時 `-shares-to-include` 共享區的參數和父Volume會包含在中 `-volumes-to-exclude` 參數、 `-volumes-to-exclude` 優先於 `-shares-to-include`。
- 當中包含匯出原則時 `-export-policies-to-include` 匯出原則的參數和父Volume會包含在中 `-volumes-to-exclude` 參數、 `-volumes-to-exclude` 優先於 `-export-policies-to-include`。
- 系統管理員可以同時指定兩者 `-file-extensions-to-include` 和 `-file-extensions-to-exclude` 清單。

  。 `-file-extensions-to-exclude` 參數會在之前檢查 `-file-extensions-to-include` 參數已核取。

FPolicy範圍組態包含的內容

您可以使用下列可用的FPolicy範圍組態參數清單來協助規劃組態：

> 當設定要納入或排除範圍的共用、匯出原則、磁碟區及副檔名時、包含和排除參數可以包含像是「」之類的元元符號?" and "*。 不支援使用規則運算式。

資訊類型	選項

SVM 指定您要在其中建立FPolicy範圍的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`
原則名稱 指定要附加範圍的FPolicy原則名稱。FPolicy原則必須已經存在。	`-policy-name policy_name`
要納入的共享_ 指定以逗號分隔的共用清單、以監控套用範圍的FPolicy原則。	`-shares-to-include share_name、...`
要排除的共享_ 指定要從套用範圍之FPolicy原則的監控中排除的以逗號分隔的共用清單。	`-shares-to-exclude share_name、...`
_要包含的磁碟區_指定以逗號分隔的磁碟區清單、以監控套用範圍的FPolicy原則。	`-volumes-to-include volume_name、...`
要排除的磁碟區_ 指定要從套用範圍之FPolicy原則的監控中排除的以逗號分隔的磁碟區清單。	`-volumes-to-exclude volume_name、...`
匯出要納入的原則_ 指定以逗號分隔的匯出原則清單、以監控套用範圍的FPolicy原則。	`-export-policies-to -include export_policy_name、...`
匯出要排除的原則_ 指定要從套用範圍之FPolicy原則的監控中排除的匯出原則清單（以英文分隔）。	`-export-policies-to -exclude export_policy_name、...`
要包括的副檔名 指定要監控套用範圍之FPolicy原則的檔案副檔名以逗號分隔的清單。	`-file-extensions-to -include file_extensions、...`
要排除的檔案副檔名_ 指定要從套用範圍之FPolicy原則的監控中排除的檔案副檔名以逗號分隔的清單。	`-file-extensions-to -exclude file_extensions、...`

檔案副檔名檢查是否已啟用目錄？ 指定副檔名檢查是否也適用於目錄物件。如果此參數設為 `true`，目錄物件會受到與一般檔案相同的副檔名檢查。如果此參數設為 `false`，目錄名稱不符合副檔名，即使目錄的副檔名不符，也會傳送通知給目錄。 如果將範圍指派給的 FPolicy 原則設定為使用原生引擎、則必須將此參數設定為 `true`。	`-is-file-extension -check-on-directories -enabled {true`
`false`	}

完成 **ONTAP FPolicy** 範圍工作表

您可以使用這份工作表單來記錄FPolicy範圍組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的使用值、然後再設定FPolicy範圍。

您應該記錄是否要在FPolicy範圍組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
原則名稱	是的	是的	
要納入的共享區	否		
要排除的共享區	否		
要包含的磁碟區	否		
要排除的磁碟區	否		
匯出要納入的原則	否		
匯出要排除的原則	否		
要包含的副檔名	否		
要排除的副檔名	否		
是否已啟用目錄的副檔名檢查？	否		

建立**FPolicy**組態

創建 ONTAP FPolicy 外部引擎

您必須建立外部引擎、才能開始建立FPolicy組態。外部引擎定義FPolicy如何建立及管理外部FPolicy伺服器的連線。如果您的組態使用內部ONTAP 的靜態引擎（原生外部引擎）來進行簡單的檔案封鎖、則不需要設定個別的FPolicy外部引擎、也不需要執行此步驟。

開始之前

。 "外部引擎" 工作表應填寫完畢。

關於這項工作

如果外部引擎用於MetroCluster 整個功能表組態、您應該將來源站台的FPolicy伺服器IP位址指定為主要伺服器。目的地站台FPolicy伺服器的IP位址應指定為次要伺服器。

步驟

1. 使用建立 FPolicy 外部引擎 `vserver fpolicy policy external-engine create` 命令。

   下列命令會在儲存虛擬機器（SVM）vs1.example.com上建立外部引擎。與FPolicy伺服器的外部通訊不需要驗證。

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. 使用驗證 FPolicy 外部引擎組態 `vserver fpolicy policy external-engine show` 命令。

   下列命令會顯示有關SVM vs1.example.com上設定的所有外部引擎資訊：

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                Primary         Secondary
   External
   Vserver             Engine   Servers         Servers        Port Engine
   Type
   ---------------     ---------- -------------- ----------- ------
   -----------
   vs1.example.com     engine1    10.1.1.2,       -             6789
   synchronous
                                  10.1.1.3
   ```

   下列命令會在SVM vs1.example.com上顯示名為「engin1」的外部引擎詳細資訊：

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

```
                            Vserver: vs1.example.com
                             Engine: engine1
              Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
       Port Number of FPolicy Service: 6789
            Secondary FPolicy Servers: -
                 External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
               Certificate Authority: -
```

建立 ONTAP FPolicy 事件

在建立FPolicy原則組態時、您需要建立FPolicy事件。您可以在建立事件時、將其與FPolicy原則建立關聯。事件會定義要監控的傳輸協定、以及要監控和篩選的檔案存取事件。

開始之前

您應該完成 FPolicy 事件"工作表"。

建立FPolicy事件

1. 使用建立 FPolicy 事件 `vserver fpolicy policy event create` 命令。

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. 使用驗證 FPolicy 事件組態 `vserver fpolicy policy event show` 命令。

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                     Event                File                      Is Volume
   Vserver           Name      Protocols  Operations    Filters     Operation
   ---------------   --------- ---------  ------------- ---------
   ------------
   vs1.example.com   event1    cifs       open, close,  -           false
                                          read, write
   ```

建立 FPolicy 存取遭拒事件

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。這些通知對於安全性、勒索軟體保護和治理來說非常重要。

1. 使用建立 FPolicy 事件 `vserver fpolicy policy event create` 命令。

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

建立 ONTAP FPolicy 持久性存儲

持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。從 ONTAP 9.14.1 開始、 FPolicy 可讓您進行設定 "持續儲存區" 擷取 SVM 中非強制性非非同步原則的檔案存取事件。不支援同步（強制或非強制）和非同步強制組態。

從 ONTAP 9.15.1 開始、 FPolicy 永續性儲存區組態已簡化。。 `persistent-store create` 命令可自動建立 SVM 的 Volume 、並設定持續儲存區的 Volume 。

根據 ONTAP 版本的不同、有兩種方法可以建立持續儲存區：

- ONTAP 9.15.1 或更新版本：當您建立持續儲存區時、 ONTAP 會自動同時建立及設定其 Volume 。如此可簡化 FPolicy 持續儲存區組態、並實作所有最佳實務做法。
- ONTAP 9.14.1 ：手動建立和設定磁碟區、然後為新建立的磁碟區建立持續儲存區。

每個 SVM 只能設定一個持續儲存區。此單一持續儲存區必須用於該 SVM 上的所有 FPolicy 組態、即使這些原則來自不同的合作夥伴。

建立持續儲存區（ ONTAP 9.15.1 或更新版本）

從 ONTAP 9.15.1 開始、請使用 `fpolicy persistent-store create` 命令來建立具有內嵌磁碟區建立和組態的 FPolicy 持續儲存區。ONTAP 會自動封鎖磁碟區、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。

開始之前

- 您要建立持續儲存區的 SVM 必須至少有一個集合體。
- 您應該可以存取 SVM 可用的集合體、並擁有足夠的權限來建立 Volume 。

步驟

1. 建立持續儲存區、以自動建立和設定磁碟區：

   ```
   vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
   <name> -volume <volume_name> -size <size> -autosize-mode
   <off|grow|grow_shrink>
   ```

   - 。 `vserver` 參數是 SVM 的名稱。
   - 。 `persistent-store` 參數是持續儲存區的名稱。
   - 。 `volume` 參數是持續儲存區磁碟區的名稱。

     > ⓘ 如果您想要使用現有的空白磁碟區、請使用 `volume show` 命令來尋找它、並在 Volume 參數中指定它。

   - 。 `size` 參數是根據您想要保留未傳送至外部伺服器（合作夥伴應用程式）的事件的持續時間。

     例如、如果您想要在每秒有 30K 通知的叢集中保留 30 分鐘的事件容量：

所需 Volume 大小 = 30000 x 30 x 60 x 0.6KB （平均通知記錄大小） = 32400000 KB = ~32 GB

要查找大致的通知率，您可以聯繫您的 FPolicy 合作伙伴應用程序或使用 FPolicy 計數器 `requests_dispatched_rate`。

如果您使用現有的 Volume 、則 Size 參數為選用項目。如果您確實為 size 參數提供值、它會以您指定的大小修改 Volume 。

- 。 `autosize-mode` 參數指定 Volume 的自動調整模式。支援的自動調整大小模式包括：
  - Off （關） - 磁碟區不會因應使用空間量而增加或縮小大小。
  - 擴充 - 當磁碟區中的使用空間超過擴充臨界值時、磁碟區會自動增加。
  - GROW _ 收縮：磁碟區會隨著使用空間的數量而增加或縮小大小。

2. 建立 FPolicy 原則、並將持續儲存區名稱新增至該原則。如需詳細資訊、請參閱 "建立FPolicy原則"。

建立持續儲存區（ **ONTAP 9.14.1** ）

您可以建立磁碟區、然後建立持續儲存區以使用該磁碟區。接著、您可以封鎖新建立的 Volume 、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。

步驟

1. 在 SVM 上建立一個空的磁碟區、以便為持續儲存區進行資源配置：

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
-snapshot-policy <none>
```

系統管理員使用者若擁有足夠的 RBAC 權限（以建立 Volume ）、就會建立所需大小的 Volume （使用 Volume CLI 命令或 REST API ）、並提供該 Volume 的名稱做為 `-volume` 在持續儲存區中、建立 CLI 命令或 REST API 。

- 。 `vserver` 參數是 SVM 的名稱。
- 。 `volume` 參數是持續儲存區磁碟區的名稱。
- 。 `state` 參數應設為線上、以便使用 Volume 。
- 。 `policy` 如果您已設定 FPolicy 服務原則、則參數會設為 FPolicy 服務原則。如果沒有、您可以使用 `volume modify` 命令稍後新增原則。
- 。 `unix-permissions` 參數為選用項目。
- 。 `size` 參數是根據您想要保留未傳送至外部伺服器（合作夥伴應用程式）的事件的持續時間。

  例如、如果您想要在每秒有 30K 通知的叢集中保留 30 分鐘的事件容量：

  所需 Volume 大小 = 30000 x 30 x 60 x 0.6KB （平均通知記錄大小） = 32400000 KB = ~32 GB

要查找大致的通知率，您可以聯繫您的 FPolicy 合作伙伴應用程序或使用 FPolicy 計數器 `requests_dispatched_rate`。

- FlexVol Volume 需要 Aggregate 參數、否則不需要。

- 。 `snapshot-policy` 參數必須設定為無。如此可確保不會意外還原快照、導致目前事件遺失、並防止可能的重複事件處理。

  如果您想要使用現有的空白磁碟區、請使用 `volume show` 命令來尋找它和 `volume modify` 命令進行任何必要的變更。確保原則、大小和 `snapshot-policy` 持續儲存區的參數已正確設定。

2. 建立持續儲存區：

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store
<PS_name> -volume <volume>
```

   - 。 `vserver` 參數是 SVM 的名稱。
   - 。 `persistent-store` 參數是持續儲存區的名稱。
   - 。 `volume` 參數是持續儲存區磁碟區的名稱。

3. 建立 FPolicy 原則、並將持續儲存區名稱新增至該原則。如需詳細資訊、請參閱 "建立FPolicy原則"。

建立 **ONTAP FPolicy** 策略

當您建立FPolicy原則時、會將外部引擎和一或多個事件與原則建立關聯。此原則也會指定是否需要強制篩選、FPolicy伺服器是否具有存取儲存虛擬機器（SVM）上資料的權限、以及是否啟用離線檔案的傳遞讀取。

開始之前

- FPolicy原則工作表應完成。
- 如果您打算設定原則使用FPolicy伺服器、則外部引擎必須存在。
- 您計畫與FPolicy原則建立關聯的FPolicy事件必須至少存在一個。
- 如果您要設定特殊權限資料存取、SVM上必須有SMB伺服器。
- 若要設定原則的持續儲存區、引擎類型必須為 * 非同步 * 、原則必須為 * 非強制 * 。

  如需詳細資訊、請參閱 "建立持續儲存區"。

步驟

1. 建立FPolicy原則：

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

   - 您可以將一或多個事件新增至FPolicy原則。
   - 預設會啟用強制篩選。
   - 如果您想要透過設定來允許特殊權限存取 `-allow-privileged-access` 參數至 `yes`、您也必須設定權限使用者名稱以進行權限存取。
   - 如果您想要設定 Passthrough-read 、請設定 `-is-passthrough-read-enabled` 參數至 `true`、您也

必須設定特殊權限資料存取。

下列命令會建立名為「policy1'」的原則、其事件名稱為「EVENT1」、外部引擎名稱為「engine 1'」。此原則會在原則組態中使用預設值：

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1
-events event1 -engine engine1
```

下列命令會建立名為「policy2」的原則、其事件名稱為「'Event2」、外部引擎名稱為「engine 2」。此原則設定為使用指定的使用者名稱來使用權限存取。Passthsthread-read已啟用：

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-
user-name example\archive_acct -is-passthrough-read-enabled true
```

下列命令會建立名為「native1」的原則、並將事件命名為「事件3」。此原則使用原生引擎、並在原則組態中使用預設值：

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. 使用驗證 FPolicy 原則組態 `vserver fpolicy policy show` 命令。

   下列命令會顯示有關三個已設定的FPolicy原則的資訊、包括下列資訊：

   - 與原則相關聯的SVM
   - 與原則相關聯的外部引擎
   - 與原則相關的事件
   - 是否需要強制篩選
   - 是否需要權限存取

   ```
   vserver fpolicy policy show
   ```

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                       Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

建立 **ONTAP FPolicy** 範圍

建立FPolicy原則之後、您需要建立FPolicy範圍。建立範圍時、您會將範圍與FPolicy原則建立關聯。範圍會定義套用FPolicy原則的界限。範圍可以根據共用、匯出原則、磁碟區和副檔名來包含或排除檔案。

開始之前

必須填寫FPolicy範圍工作表。FPolicy原則必須與關聯的外部引擎一起存在（如果原則設定為使用外部FPolicy伺

服器）、且必須至少有一個關聯的FPolicy事件。

步驟

1. 使用建立 FPolicy 範圍 `vserver fpolicy policy scope create` 命令。

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
policy1 -volumes-to-include datavol1,datavol2
```

2. 使用驗證 FPolicy 範圍組態 `vserver fpolicy policy scope show` 命令。

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
 Export Policies to Include: -
 Export Policies to Exclude: -
 File Extensions to Include: -
 File Extensions to Exclude: -
```

啟用 **ONTAP FPolicy** 策略

完成FPolicy原則組態設定之後、您就可以啟用FPolicy原則。啟用原則會設定其優先順序、並開始監控原則的檔案存取。

開始之前

FPolicy原則必須與關聯的外部引擎一起存在（如果原則設定為使用外部FPolicy伺服器）、且必須至少有一個關聯的FPolicy事件。FPolicy原則範圍必須存在、而且必須指派給FPolicy原則。

關於這項工作

當在儲存虛擬機器（SVM）上啟用多個原則、且有多個原則已訂閱相同的檔案存取事件時、就會使用優先順序。使用原生引擎組態的原則優先順序高於任何其他引擎的原則、無論啟用原則時指派給它們的順序編號為何。

無法在管理SVM上啟用原則。

步驟

1. 使用啟用 FPolicy 原則 `vserver fpolicy enable` 命令。

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
-sequence-number 1
```

2. 使用確認 FPolicy 原則已啟用 `vserver fpolicy show` 命令。

```
vserver fpolicy show -vserver vs1.example.com
```

```
                                    Sequence
Vserver          Policy Name          Number  Status   Engine
---------------  ----------------- --------  -------- ---------
vs1.example.com  policy1                   1  on       engine1
```

管理 FPolicy 組態

修改FPolicy組態

在 ONTAP 中修改 FPolicy 配置的命令

您可以修改組成組態的元素、以修改FPolicy組態。您可以修改外部引擎、 FPolicy 事件、 FPolicy 範圍、 FPolicy 持續儲存區和 FPolicy 原則。您也可以啟用或停用FPolicy原則。當您停用FPolicy原則時、該原則的檔案監控將會中斷。

您應該先停用 FPolicy 原則、再修改其組態。

如果您要修改...	使用此命令...
外部引擎	`vserver fpolicy policy external-engine modify`
活動	`vserver fpolicy policy event modify`
範圍	`vserver fpolicy policy scope modify`
持續儲存區	`vserver fpolicy persistent-store modify`
原則	`vserver fpolicy policy modify`

如"指令參考資料ONTAP"需詳細 `vserver fpolicy policy`資訊，請參閱。

啟用或停用 ONTAP FPolicy 策略

您可以在組態完成後啟用FPolicy原則。啟用原則會設定其優先順序、並開始監控原則的檔案存取。若要停止原則的檔案存取監控、您可以停用FPolicy原則。

開始之前

在啟用FPolicy原則之前、必須先完成FPolicy組態。

關於這項工作

- 當在儲存虛擬機器（SVM）上啟用多個原則、且有多個原則已訂閱相同的檔案存取事件時、就會使用優先順序。
- 使用原生引擎組態的原則優先順序高於任何其他引擎的原則、無論啟用原則時指派給它們的順序編號為何。
- 若要變更FPolicy原則的優先順序、您必須停用該原則、然後使用新的順序編號重新啟用。

步驟

1. 執行適當的行動：

如果您想要...	輸入下列命令...
啟用FPolicy原則	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
停用FPolicy原則	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

顯示FPolicy組態的相關資訊

了解 ONTAP FPolicy 顯示命令

在顯示有關 FPolicy 組態的資訊以瞭解的方式時、這很有幫助 `show` 命令運作正常。

答 `show` 不含其他參數的命令會以摘要形式顯示資訊。此外、每個 `show` Command 具有相同的兩個互斥選擇性參數、 `-instance` 和 `-fields`。

當您使用時 `-instance` 參數與 `show` 命令時、命令輸出會以清單格式顯示詳細資訊。在某些情況下、詳細輸出可能會很長、而且包含的資訊比您需要的還多。您可以使用 `-fields fieldname[,fieldname…]` 此參數可自訂輸出、使其僅顯示指定欄位的資訊。您可以輸入來識別您可以指定的欄位 `?` 之後 `-fields` 參數。

的輸出 `show` 命令 `-fields` 參數可能會顯示與所要求欄位相關的其他相關和必要欄位。

每個 `show` 命令具有一個或多個可選參數，用於篩選輸出結果，並使您能夠縮小命令輸出中顯示的信息範圍。您可以輸入、識別命令可使用的選用參數 `?` 之後 `show` 命令。

。 `show` 命令支援 UNIX 樣式的模式和萬用字元、可讓您在命令參數引數中比對多個值。例如、您可以使用萬用字元運算子（*）、非運算子（！）、OR運算子（|）、範圍運算子（integer…integer）、小於運算子（<）、大於運算子（>）、小於或等於運算子（<=）、以及大於或等於運算子（>=）來指定值。

如需使用UNIX樣式模式和萬用字元的詳細資訊、請參閱 使用ONTAP 指令行介面。

用於在 ONTAP 中顯示 FPolicy 組態資訊的命令

您可以使用 `fpolicy show` 顯示 FPolicy 組態相關資訊的命令、包括有關 FPolicy 外部引擎、事件、範圍和原則的資訊。

如果您要顯示FPolicy的相關資訊...	使用此命令...
外部引擎	`vserver fpolicy policy external-engine show`
活動	`vserver fpolicy policy event show`
範圍	`vserver fpolicy policy scope show`

原則	`vserver fpolicy policy show`

如"指令參考資料ONTAP"需詳細 `vserver fpolicy policy`資訊，請參閱。

顯示有關 **ONTAP FPolicy** 策略狀態的信息

您可以顯示FPolicy原則狀態的相關資訊、以判斷原則是否已啟用、原則要使用的外部引擎、原則的順序編號、以及FPolicy原則與哪個儲存虛擬機器（SVM）相關聯。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 原則名稱
- 原則順序編號
- 原則狀態

除了顯示叢集或特定SVM上所設定之FPolicy原則的原則狀態資訊、您也可以使用命令參數、依其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 參數、僅顯示命令輸出或中指定的欄位 `-fields ?` 決定您可以使用哪些欄位。

步驟

1. 使用適當的命令顯示FPolicy原則狀態的篩選資訊：

如果您要顯示原則的狀態資訊…	輸入命令…
在叢集上	`vserver fpolicy show`
具有指定狀態的	`vserver fpolicy show -status {on
off}`	在指定的SVM上
`vserver fpolicy show -vserver vserver_name`	使用指定的原則名稱
`vserver fpolicy show -policy-name policy_name`	使用指定的外部引擎

範例

下列範例顯示叢集上FPolicy原則的相關資訊：

```
cluster1::> vserver fpolicy show
                                        Sequence
Vserver              Policy Name          Number  Status      Engine
-------------------- -------------------- --------  ---------   ---------
FPolicy              cserver_policy       -         off         eng1
vs1.example.com      v1p1                 -         off         eng2
vs1.example.com      v1p2                 -         off         native
vs1.example.com      v1p3                 -         off         native
vs1.example.com      cserver_policy       -         off         eng1
vs2.example.com      v1p1                 3         on          native
vs2.example.com      v1p2                 1         on          eng3
vs2.example.com      cserver_policy       2         on          eng1
```

顯示有關已啟用的 **ONTAP FPolicy** 策略的信息

您可以顯示已啟用FPolicy原則的相關資訊、以判斷其設定使用的FPolicy外部引擎、原則的優先順序、以及FPolicy原則關聯的儲存虛擬機器（SVM）。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 原則名稱
- 原則優先順序

您可以使用命令參數、根據指定的條件篩選命令的輸出。

步驟

1. 使用適當的命令顯示已啟用的FPolicy原則相關資訊：

如果您要顯示已啟用原則的相關資訊…	輸入命令…
在叢集上	`vserver fpolicy show-enabled`
在指定的SVM上	`vserver fpolicy show-enabled -vserver vserver_name`
使用指定的原則名稱	`vserver fpolicy show-enabled -policy-name policy_name`
使用指定的序號	`vserver fpolicy show-enabled -priority integer`

範例

下列範例顯示叢集上已啟用FPolicy原則的相關資訊：

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

管理FPolicy伺服器連線

連線至 ONTAP 中的外部 FPolicy 伺服器

若要啟用檔案處理、您可能需要手動連線至外部FPolicy伺服器（如果先前已終止連線）。連線會在伺服器逾時後終止、或因為發生錯誤而終止。或者、系統管理員也可以手動終止連線。

關於這項工作

如果發生嚴重錯誤、則可終止與FPolicy伺服器的連線。解決造成嚴重錯誤的問題之後、您必須手動重新連線至FPolicy伺服器。

步驟

1. 使用連線至外部 FPolicy 伺服器 `vserver fpolicy engine-connect` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver fpolicy engine-connect`資訊，請參閱。

2. 使用確認外部 FPolicy 伺服器已連線 `vserver fpolicy show-engine` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver fpolicy show-engine`資訊，請參閱。

中斷與 ONTAP 中外部 FPolicy 伺服器的連線

您可能需要手動中斷與外部FPolicy伺服器的連線。如果FPolicy伺服器在處理通知要求時發生問題、或是您需要在FPolicy伺服器上執行維護、則可能需要這樣做。

步驟

1. 使用中斷與外部 FPolicy 伺服器的連線 `vserver fpolicy engine-disconnect` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver fpolicy engine-disconnect`資訊，請參閱。

2. 使用確認外部 FPolicy 伺服器已中斷連線 `vserver fpolicy show-engine` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver fpolicy show-engine`資訊，請參閱。

您可以顯示叢集或特定儲存虛擬機器（SVM）與外部FPolicy伺服器（FPolicy伺服器）連線的狀態資訊。此資訊可協助您判斷哪些FPolicy伺服器已連線。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 節點名稱
- FPolicy原則名稱
- FPolicy伺服器IP位址
- FPolicy伺服器狀態
- FPolicy伺服器類型

除了顯示叢集或特定SVM上FPolicy連線的相關資訊、您也可以使用命令參數、根據其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 此參數僅顯示命令輸出中指定的欄位。您可以輸入 `?` 之後 `-fields` 參數來找出您可以使用的欄位。

步驟

1. 使用適當的命令、顯示節點與FPolicy伺服器之間連線狀態的篩選資訊：

如果您要顯示FPolicy伺服器的連線狀態資訊…	輸入…
您指定的	`vserver fpolicy show-engine -server IP_address`
適用於指定的SVM	`vserver fpolicy show-engine -vserver vserver_name`
隨附於指定原則的	`vserver fpolicy show-engine -policy-name policy_name`
使用您指定的伺服器狀態	`vserver fpolicy show-engine -server-status status` 伺服器狀態可以是下列其中一項： • `connected` • `disconnected` • `connecting` • `disconnecting`

使用指定類型	`vserver fpolicy show-engine -server-type type` FPolicy伺服器類型可以是下列其中一種： • `primary` • `secondary`
已中斷連線的原因	`vserver fpolicy show-engine -disconnect-reason text` 中斷連線可能有多種原因。以下是中斷連線的常見原因： • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

範例

此範例顯示SVM vs1.example.com上的FPolicy伺服器外部引擎連線相關資訊：

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

此範例僅顯示連線的FPolicy伺服器相關資訊：

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver          policy-name server
---------- ---------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

顯示有關 **ONTAP FPolicy** 直通讀取連線狀態的信息

您可以針對叢集或特定儲存虛擬機器（SVM）、顯示與外部FPolicy伺服器（FPolicy伺服器）的FPolicy Passthrough-read連線狀態相關資訊。此資訊可協助您判斷哪些FPolicy伺服器具有直通讀取資料連線、以及哪些FPolicy伺服器的直通讀取連線中斷。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- FPolicy原則名稱
- 節點名稱
- FPolicy伺服器IP位址
- FPolicy Passthrough-read連線狀態

除了顯示叢集或特定SVM上FPolicy連線的相關資訊、您也可以使用命令參數、根據其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 此參數僅顯示命令輸出中指定的欄位。您可以輸入 `?` 之後 `-fields` 參數來找出您可以使用的欄位。

步驟

1. 使用適當的命令、顯示節點與FPolicy伺服器之間連線狀態的篩選資訊：

如果您要顯示有關…的連線狀態資訊	輸入命令…
叢集的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection`
指定SVM的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
指定原則的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
指定原則的詳細FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`

您指定狀態的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` 伺服器狀態可以是下列其中一項： • `connected` • `disconnected`

範例

下列命令會顯示叢集上所有FPolicy伺服器的Passthrough-read連線相關資訊：

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------ ----------- -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01  2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01  1.1.1.1           connected
```

下列命令會顯示「'pol_CIFS _1'」原則中所設定之FPolicy伺服器的Passthrough-read連線詳細資訊：

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                       Node: FPolicy-01
                                    Vserver: vs1.example.com
                                     Policy: pol_cifs_1
                                     Server: 1.1.1.1
               Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

使用安全性追蹤來驗證存取

了解 **ONTAP** 安全追蹤

您可以新增權限追蹤篩選器、以指示ONTAP Sfin記錄儲存虛擬機器（SVM）上SMB和NFS伺服器為何允許或拒絕用戶端或使用者執行作業的要求。當您想要驗證檔案存取安全性配置是否適當、或是想要疑難排解檔案存取問題時、這項功能就很實用。

安全追蹤可讓您設定篩選器、偵測SVM上SMB和NFS上的用戶端作業、並追蹤符合該篩選器的所有存取檢查。然後您可以檢視追蹤結果、以方便的方式摘要說明允許或拒絕存取的原因。

當您想要驗證SVM上檔案和資料夾的SMB或NFS存取安全性設定、或是遇到存取問題時、可以快速新增篩選器來開啟權限追蹤。

下列清單概述安全追蹤運作方式的重要事實：

- 在SVM層級套用安全追蹤。ONTAP
- 每個傳入要求都會經過篩選、以查看是否符合任何已啟用安全追蹤的篩選條件。
- 檔案和資料夾存取要求都會執行追蹤。
- 追蹤可以根據下列準則進行篩選：
  - 用戶端 IP
  - SMB或NFS路徑
  - Windows名稱
  - UNIX 名稱
- 系統會針對「允許_」和「拒絕_」存取回應結果進行篩選。
- 每個符合已啟用追蹤篩選條件的要求、都會記錄在追蹤結果記錄中。
- 儲存管理員可在篩選器上設定逾時、以自動停用篩選器。
- 如果某個要求符合多個篩選器、則會記錄索引編號最高的篩選器結果。
- 儲存管理員可從追蹤結果記錄列印結果、以判斷允許或拒絕存取要求的原因。

ONTAP SVM 上的存取檢查安全追蹤監視器的類型

檔案或資料夾的存取檢查是根據多個準則進行。安全追蹤會監控所有這些準則的作業。

安全追蹤監控的存取檢查類型包括：

- Volume與qtree安全樣式
- 檔案系統的有效安全性、其中包含要求執行作業的檔案和資料夾
- 使用者對應
- 共用層級權限
- 匯出層級權限
- 檔案層級權限
- 儲存層級的存取保護安全性

在 ONTAP SVM 上建立安全追蹤時的注意事項

在儲存虛擬機器（SVM）上建立安全追蹤時、請謹記幾個考量事項。例如、您需要知道可以建立追蹤的通訊協定、支援哪些安全性樣式、以及最大作用中追蹤數量。

- 您只能在SVM上建立安全追蹤。

- 每個安全性追蹤篩選器項目都是SVM專屬項目。

  您必須指定要在其中執行追蹤的SVM。

- 您可以新增SMB和NFS要求的權限追蹤篩選器。
- 您必須在要建立追蹤篩選器的SVM上設定SMB或NFS伺服器。
- 您可以為位於NTFS、UNIX及混合式安全型磁碟區和qtree上的檔案和資料夾建立安全追蹤。
- 每個SVM最多可新增10個權限追蹤篩選器。
- 建立或修改篩選時、必須指定篩選索引編號。

  篩選條件會依索引編號的順序進行考量。索引編號較高的篩選條件、會在索引編號較低的條件之前考量。如果要追蹤的要求符合多個已啟用篩選器中的條件、則只會觸發索引編號最高的篩選器。

- 建立並啟用安全性追蹤篩選器之後、您必須在用戶端系統上執行部分檔案或資料夾要求、以產生追蹤篩選器可擷取並登入追蹤結果記錄的活動。
- 您應該新增權限追蹤篩選器、僅供檔案存取驗證或疑難排解之用。

  新增權限追蹤篩選器對控制器效能的影響不大。

  完成驗證或疑難排解活動後、您應該停用或移除所有權限追蹤篩選器。此外、您選取的篩選條件應盡可能明確、ONTAP 以便不將大量的追蹤結果傳送到記錄檔。

執行安全追蹤

學習執行 **ONTAP** 安全追蹤

執行安全性追蹤包括建立安全性追蹤篩選器、驗證篩選條件、在符合篩選條件的SMB或NFS用戶端上產生存取要求、以及檢視結果。

完成使用安全篩選器擷取追蹤資訊之後、您可以修改篩選器並重複使用、或是在不再需要時停用篩選器。檢視及分析篩選追蹤結果之後、您可以在不再需要時將其刪除。

在 **ONTAP SVM** 中建立安全追蹤過濾器

您可以建立安全追蹤篩選器、以偵測儲存虛擬機器（SVM）上的SMB和NFS用戶端作業、並追蹤符合篩選器的所有存取檢查。您可以使用安全追蹤的結果來驗證組態或疑難排解存取問題。

關於這項工作

Vserver安全追蹤篩選器create命令需要兩個參數：

必要參數	說明
`-vserver vserver_name`	*SVM*名稱 包含您要套用安全性追蹤篩選器之檔案或資料夾的SVM名稱。

`-index index_number`	篩選索引編號_ 要套用至篩選的索引編號。每個SVM最多可有10個追蹤篩選器。此參數允許的值為1到10。

許多選用的篩選參數可讓您自訂安全性追蹤篩選器、以便縮小安全性追蹤所產生的結果：

篩選參數	說明
`-client-ip IP_Address`	此篩選器會指定使用者存取SVM的IP位址。
`-path path`	此篩選器會指定要套用權限追蹤篩選器的路徑。的價值 `-path` 可以使用下列其中一種格式： • 完整路徑、從共用區根目錄或匯出開始 • 部分路徑、相對於共用的根目錄 您必須在路徑值中使用NFS樣式目錄UNIX型目錄分隔符號。
`-windows-name win_user_name` 或 `-unix -name``unix_user_name`	您可以指定要追蹤其存取要求的Windows使用者名稱或UNIX使用者名稱。使用者名稱變數不區分大小寫。您無法在同一個篩選器中同時指定Windows使用者名稱和UNIX使用者名稱。 即使您可以追蹤SMB和NFS存取事件、對應的UNIX使用者和對應的UNIX使用者群組也可以在混合或UNIX安全型資料上執行存取檢查。
`-trace-allow {yes`	`no}`
安全性追蹤篩選器一律會啟用拒絕事件追蹤。您可以選擇追蹤允許事件。若要追蹤允許事件、請將此參數設為 `yes`。	`-enabled {enabled`
`disabled}`	您可以啟用或停用安全性追蹤篩選器。依預設、安全性追蹤篩選器為啟用狀態。
`-time-enabled integer`	您可以指定篩選器的逾時時間、之後篩選器就會停用。

步驟

1. 建立安全追蹤篩選器：

   ```
   vserver security trace filter create -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   `filter_parameters` 為選用篩選參數清單。

如"指令參考資料ONTAP"需詳細 `vserver security trace filter create`資訊，請參閱。

2. 驗證安全性追蹤篩選器項目：

```
vserver security trace filter show -vserver vserver_name -index index_number
```

範例

下列命令會為任何使用者建立安全性追蹤篩選器、以存取具有共用路徑的檔案 `\\server\share1\dir1\dir2\file.txt` 從 IP 位址 10.10.10.7 。篩選器使用的完整路徑 `-path` 選項。用於存取資料的用戶端IP位址為10.10.10.7.篩選器在30分鐘後逾時：

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

下列命令會使用的相對路徑來建立安全性追蹤篩選器 `-path` 選項。篩選器會追蹤名為「'joe'」之Windows使用者的存取權。Joe 正在存取具有共用路徑的檔案 `\\server\share1\dir1\dir2\file.txt`。篩選器追蹤會允許及拒絕事件：

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                              Vserver: vs1
                         Filter Index: 2
            Client IP Address to Match: -
                                  Path: /dir1/dir2/file.txt
                  Windows User Name: mydomain\joe
                     UNIX User Name: -
                  Trace Allow Events: yes
                      Filter Enabled: enabled
             Minutes Filter is Enabled: 60
```

顯示有關 **ONTAP SVM** 中的安全追蹤過濾器的信息

檢視儲存虛擬機器（SVM）上的安全追蹤篩選器詳細資料，以識別每個篩選器追蹤的存取事件。

系統管理員

從 ONTAP 9.6 開始，您可以使用 System Manager 追蹤 SVM 上的檔案存取。

步驟

1. 開啟 System Manager 儀表板。
2. 在 **Cluster** 下，選擇 **Storage VMs** 。
3. 選擇適用的 SVM 的 ⋮。
4. 選擇 **Trace file access** 。
5. 將檔案存取通訊協定類型設定為 **SMB/CIFS** 或 **NFS**。
6. 輸入 **User name**。
7. 輸入 **Client IP address**。
8. （選用）選取下列一項或多項：
   a. 選擇 **Trace particular path** 以指定要追蹤的檔案或檔案路徑。
   b. 選擇 **Show only access denied entries** 可將追蹤範圍限制為存取被拒絕的事件。
9. 選擇 **Start tracing** 。

CLI

使用 CLI 追蹤 SVM 上的檔案存取。

步驟

1. 使用顯示安全性追蹤篩選項目的相關資訊 `vserver security trace filter show` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver security trace filter show`資訊，請參閱。

範例

下列命令會顯示SVM VS1上所有安全追蹤篩選器的相關資訊：

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

在 **ONTAP SVM** 中顯示安全性追蹤結果

您可以顯示針對符合安全性追蹤篩選器的檔案作業所產生的安全性追蹤結果。您可以使用結果來驗證檔案存取安全性組態、或疑難排解SMB和NFS檔案存取問題。

開始之前

啟用的安全性追蹤篩選器必須存在、而且必須從SMB或NFS用戶端執行作業、且該用戶端必須符合安全性追蹤篩選器、才能產生安全性追蹤結果。

關於這項工作

您可以顯示所有安全性追蹤結果的摘要、也可以指定選用參數來自訂輸出中顯示的資訊。當安全性追蹤結果包含大量記錄時、這一點很有幫助。

如果您未指定任何選用參數、則會顯示下列項目：

- 儲存虛擬機器（SVM）名稱
- 節點名稱
- 安全性追蹤索引編號
- 安全風格
- 路徑
- 理由
- 使用者名稱

  使用者名稱會根據追蹤篩選器的設定方式顯示：

如果篩選器已設定…	然後…
使用UNIX使用者名稱	安全性追蹤結果會顯示UNIX使用者名稱。
使用Windows使用者名稱	安全性追蹤結果會顯示Windows使用者名稱。
沒有使用者名稱	安全性追蹤結果會顯示Windows使用者名稱。

您可以使用選用參數來自訂輸出。您可以使用某些選用參數來縮小命令輸出中傳回的結果範圍、其中包括：

選用參數	說明
`-fields field_name、 ...`	在您選擇的欄位上顯示輸出。您可以單獨使用此參數、也可以搭配其他選用參數一起使用。
`-instance`	顯示安全性追蹤事件的詳細資訊。此參數可搭配其他選用參數使用、以顯示特定篩選結果的詳細資訊。
`-node node_name`	僅顯示有關指定節點上事件的資訊。
`-vserver vserver_name`	僅顯示指定SVM上事件的相關資訊。
`-index integer`	顯示與指定索引編號對應之篩選器所產生之事件的相關資訊。

`-client-ip IP_address`	顯示從指定用戶端IP位址存取檔案所發生事件的相關資訊。
`-path path`	顯示因檔案存取指定路徑而發生事件的相關資訊。
`-user-name user_name`	顯示指定Windows或UNIX使用者存取檔案時所發生事件的相關資訊。
`-security-style security_style`	顯示在具有指定安全樣式的檔案系統上發生事件的相關資訊。

如需其他選用參數的詳細"指令參考資料ONTAP"資訊，請參閱。

步驟

1. 使用顯示安全性追蹤篩選結果 `vserver security trace trace-result show` 命令。

```
vserver security trace trace-result show -user-name domain\user
```

```
Vserver: vs1

Node      Index   Filter Details          Reason
--------  ------- ----------------------  ------------------------------
node1     3       User:domain\user        Access denied by explicit ACE
                  Security Style:mixed
                  Path:/dir1/dir2/

node1     5       User:domain\user        Access denied by explicit ACE
                  Security Style:unix
                  Path:/dir1/
```

修改 **ONTAP SVM** 上的安全性追蹤過濾器

如果您想要變更選用的篩選參數、以決定追蹤哪些存取事件、您可以修改現有的安全性追蹤篩選器。

關於這項工作

您必須指定要套用篩選器的儲存虛擬機器（SVM）名稱、以及篩選器的索引編號、以識別要修改的安全性追蹤篩選器。您可以修改所有選用的篩選參數。

步驟

1. 修改安全性追蹤篩選器：

```
vserver security trace filter modify -vserver vserver_name -index
index_numberfilter_parameters
```

   ◦ `vserver_name` 是要套用安全性追蹤篩選器的 SVM 名稱。

- `index_number` 是您要套用至篩選的索引編號。此參數允許的值為1到10。
- `filter_parameters` 為選用篩選參數清單。

2. 驗證安全性追蹤篩選器項目：

```
vserver security trace filter show -vserver vserver_name -index index_number
```

範例

下列命令會修改索引編號為1的安全性追蹤篩選器。篩選器會追蹤任何使用者存取具有共用路徑之檔案的事件 `\\server\share1\dir1\dir2\file.txt` 來自任何 IP 位址。篩選器使用的完整路徑 `-path` 選項。篩選器追蹤會允許及拒絕事件：

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                Vserver: vs1
                           Filter Index: 1
             Client IP Address to Match: -
                                   Path: /dir1/dir2/file.txt
                     Windows User Name: -
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
              Minutes Filter is Enabled: 60
```

刪除 **ONTAP SVM** 上的安全性追蹤過濾器

當您不再需要安全性追蹤篩選器項目時、可以將其刪除。由於每個儲存虛擬機器（SVM）最多可有10個安全追蹤篩選器、因此刪除不需要的篩選器後、您就能在達到上限時建立新的篩選器。

關於這項工作

若要唯一識別您要刪除的安全性追蹤篩選器、您必須指定下列項目：

- 套用追蹤篩選器的SVM名稱
- 追蹤篩選器的篩選索引編號

步驟

1. 識別您要刪除之安全性追蹤篩選器項目的篩選器索引編號：

```
vserver security trace filter show -vserver vserver_name

vserver security trace filter show -vserver vs1
```

```
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1     -            /dir1/dir2/file.txt          yes      -
vs1        2     -            /dir3/dir4/                  no
mydomain\joe
```

2. 使用上一個步驟的篩選索引編號資訊、刪除篩選項目：

```
vserver security trace filter delete -vserver vserver_name -index index_number
```

```
vserver security trace filter delete -vserver vs1 -index 1
```

3. 確認安全性追蹤篩選器項目已刪除：

```
vserver security trace filter show -vserver vserver_name
```

```
vserver security trace filter show -vserver vs1
```

```
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        2     -            /dir3/dir4/                  no
mydomain\joe
```

刪除 **ONTAP SVM** 上的安全性追蹤記錄

使用篩選器追蹤記錄來驗證檔案存取安全性或疑難排解SMB或NFS用戶端存取問題之後、您可以從安全性追蹤記錄中刪除安全性追蹤記錄。

關於這項工作

在刪除安全性追蹤記錄之前、您必須知道記錄的序號。

> 每個儲存虛擬機器（SVM）最多可儲存128筆追蹤記錄。如果SVM達到上限、則會在新增追蹤記錄時自動刪除最舊的追蹤記錄。如果您不想手動刪除此SVM上的追蹤記錄、ONTAP 可讓SVM在達到最大值後自動刪除最舊的追蹤結果、以便留出新結果的空間。

步驟

1. 識別您要刪除的記錄序號：

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. 刪除安全性追蹤記錄：

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer

vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

- `-node node_name` 是您要刪除之權限追蹤事件所在的叢集節點名稱。

  這是必要的參數。

- `-vserver vserver_name` 是您要刪除之權限追蹤事件所在的 SVM 名稱。

  這是必要的參數。

- `-seqnum integer` 為您要刪除的記錄事件序號。

  這是必要的參數。

刪除 **ONTAP SVM** 上的所有安全追蹤記錄

如果您不想保留任何現有的安全性追蹤記錄、可以使用單一命令刪除節點上的所有記錄。

步驟

1. 刪除所有安全追蹤記錄：

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name *
```

- `-node node_name` 是您要刪除之權限追蹤事件所在的叢集節點名稱。
- `-vserver vserver_name` 是您要刪除之權限追蹤事件所在的儲存虛擬機器（ SVM ）名稱。

解釋 **ONTAP** 安全追蹤結果

安全性追蹤結果提供允許或拒絕要求的原因。輸出會結合允許或拒絕存取的原因、以及允許或拒絕存取的存取檢查路徑中的位置、來顯示結果。您可以使用結果來隔離及識別為何允許或不允許採取行動。

尋找結果類型清單和篩選詳細資料的相關資訊

您可以在命令的安全性追蹤結果中找到結果類型清單和篩選詳細資料 `vserver security trace trace-result show`。如"指令參考資料ONTAP"需詳細 `vserver security trace trace-result show`資訊，請參閱。

的輸出範例 `Reason` 欄位 `Allow` 結果類型

以下是的輸出範例 `Reason` 出現在追蹤結果中的欄位會登入 `Allow` 結果類型：

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

的輸出範例 `Reason` 欄位 `Allow` 結果類型

以下是的輸出範例 `Reason` 出現在追蹤結果中的欄位會登入 `Deny` 結果類型：

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

的輸出範例 `Filter details` 欄位

以下是的輸出範例 `Filter details` 追蹤結果記錄中的欄位、其中列出檔案系統的有效安全樣式、其中包含符合篩選條件的檔案和資料夾：

```
Security Style: MIXED and ACL
```

在哪裡可以找到有關 **ONTAP SVM** 的更多信息

成功測試 SMB 用戶端存取之後、您可以執行進階 SMB 組態或新增 SAN 存取。成功測試NFS用戶端存取之後、您可以執行進階NFS組態或新增SAN存取。傳輸協定存取完成時、您應該保護SVM的根Volume。

SMB 組態

您可以使用下列項目來進一步設定SMB存取：

- "中小企業管理"

  說明如何使用 SMB 通訊協定來設定及管理檔案存取。

- "NetApp技術報告4191：叢集Data ONTAP 式更新的最佳實務做法指南8.2 Windows檔案服務"

  提供SMB實作與其他Windows檔案服務功能的簡短概述、並提供ONTAP 有關的建議與基本疑難排解資訊。

- "NetApp技術報告3740：SMB 2 Next-Generation CIFS Protocol in Data ONTAP"

  介紹SMB 2的功能、組態詳細資料、以及ONTAP 其在功能方面的實作。

NFS 組態

您可以使用下列項目進一步設定NFS存取：

- "NFS管理"

  說明如何使用NFS傳輸協定來設定及管理檔案存取。

- "NetApp技術報告4067：NFS最佳實務與實作指南"

  可做為NFSv3和NFSv3作業指南、提供ONTAP 關於以NFSv3為焦點的各種作業系統的概述。

- "NetApp技術報告4668：名稱服務最佳實務做法指南"

  提供完整的最佳實務做法、限制、建議及考量清單、以供設定LDAP、NIS、DNS及本機使用者與群組檔案進行驗證。

- "NetApp技術報告4616：ONTAP NFS Kerberos in Some with Microsoft Active Directory"
- "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"
- "NetApp技術報告3580：NFSv4增強功能與最佳實務做法指南Data ONTAP -實作"

  說明在掛接到執行ONTAP 此功能的系統上、在AIX、Linux或Solaris用戶端上實作NFSv4元件時應遵循的最佳實務做法。

根**Volume**保護

在SVM上設定傳輸協定之後、您應確保其根Volume受到保護：

- "資料保護"

  說明如何建立負載共用鏡像來保護SVM根磁碟區、這是NetApp啟用NAS的SVM最佳實務做法。同時也說明如何從負載共用鏡像中提升SVM根磁碟區、以快速從磁碟區故障或損失中恢復。

使用System Manager管理加密

使用基於軟體的加密對**ONTAP**叢集中儲存的資料進行加密

使用Volume加密功能、可確保在基礎裝置被重新調整用途、退回、放錯地方或遭竊時、無法讀取Volume資料。Volume加密不需要特殊磁碟、可搭配所有HDD和SSD使用。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"啟用軟體級加密。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

Volume加密需要金鑰管理程式。您可以使用System Manager來設定Onboard Key Manager。您也可以使用外部金鑰管理程式、但必須先使用ONTAP CLI進行設定。

設定金鑰管理程式之後、新的磁碟區預設會加密。

步驟

1. 按一下*叢集>設定*。
2. 在 * 加密 * 下、按一下 以首次設定 Onboard Key Manager 。
3. 若要加密現有磁碟區、請按一下*儲存>磁碟區*。
4. 在所需的磁碟區上、按一下、然後按一下 * 編輯 * 。

5. 選取*啟用加密*。

使用自加密磁碟機加密ONTAP叢集中儲存的數據

使用磁碟加密可確保當基礎裝置被重新調整用途、退回、放錯位置或遭竊時、無法讀取本機層級中的所有資料。磁碟加密需要特殊的自我加密HDD或SSD。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"啟用硬體級加密。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

磁碟加密需要金鑰管理程式。您可以使用System Manager設定內建金鑰管理程式。 您也可以使用外部金鑰管理程式、但必須先使用ONTAP CLI進行設定。

如果ONTAP 偵測到自我加密磁碟、當您建立本機層時、系統會提示您設定內建金鑰管理程式。

步驟

1. 在 * 加密 * 下、按一下 以設定內建金鑰管理程式。
2. 如果您看到需要重新輸入磁碟的訊息，請按一下，然後按一下 * 重新輸入磁碟 * 。

使用CLI管理加密

了解ONTAP資料加密

NetApp同時提供軟體與硬體加密技術、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。

- 使用NetApp Volume Encryption（NVE）的軟體式加密可一次支援一個磁碟區的資料加密
- 使用NetApp儲存加密（NSE）的硬體式加密可支援寫入資料時的全磁碟加密（FDE）。

配置NetApp捲和聚合加密

了解ONTAP NetApp捲和聚合加密

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、可確保在基礎裝置重新調整用途、退回、放錯位置或遭竊時、無法讀取Volume資料。

瞭解NVE

使用 NVE 時，中繼資料和資料（包括快照）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。外部金鑰管理伺服器或 Onboard Key Manager （ OKM ）可為節點提供金鑰：

- 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）為節點提供金鑰。最佳實務做法是在不同的儲存系統上設定外部金鑰管理伺服器與資料。
- 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、為節點提供金鑰。

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAPVE 授權隨附於"ONTAP One"。設定外部或內建金鑰管理程式時、靜止資料加密的設定方式會改變、以供全新的集合體和全新的磁碟區使用。全新的Aggregate依預設會啟用NetApp Aggregate Encryption（NAE）。非NAE Aggregate一部分的全新磁碟區預設會啟用NetApp Volume Encryption（NVE）。如果資料儲存虛擬機器（SVM）是使用多租戶金鑰管理、以自己的金鑰管理程式進行設定、則為該SVM建立的磁碟區會自動設定NVE。

您可以在新的或現有的磁碟區上啟用加密。NVE支援完整的儲存效率功能、包括重複資料刪除與壓縮。從 ONTAP 9.14.1 開始、您就可以了 在現有 SVM 根磁碟區上啟用 NVE。

如果您使用SnapLock 的是功能區、則只能在新的空白SnapLock 版的功能區上啟用加密功能。您無法在現有SnapLock 的流通量上啟用加密功能。

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搭配硬體加密、在自我加密磁碟機上使用「雙重加密」資料。

啟用 NVE 時、核心傾印也會加密。

Aggregate層級加密

通常、每個加密磁碟區都會指派一個唯一的金鑰。刪除磁碟區時、金鑰會隨之刪除。

從ONTAP SURF9.6開始、您可以使用_NetApp Aggregate Encryption（NAE）_將金鑰指派給內含的Aggregate、以便加密磁碟區。刪除加密磁碟區時、會保留該集合體的金鑰。如果刪除整個Aggregate、則會刪除金鑰。

如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。NVE不支援Aggregate層級的重複資料刪除。

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAP

NVE與NAE磁碟區可共存於同一個Aggregate上。根據預設、在Aggregate層級加密下加密的磁碟區為NAE磁碟區。加密磁碟區時、您可以覆寫預設值。

您可以使用 `volume move` 將 NVE Volume 轉換為 NAE Volume 的命令、反之亦然。您可以將NAE磁碟區複寫至NVE磁碟區。

您無法使用 `secure purge` NAE 磁碟區上的命令。

何時使用外部金鑰管理伺服器

雖然使用內建金鑰管理程式的成本較低、而且通常更方便、但如果下列任一項屬實、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。
- 您需要一套多叢集解決方案、集中管理加密金鑰。
- 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。

外部金鑰管理範圍

外部金鑰管理的範圍決定了金鑰管理伺服器是保護叢集中的所有SVM、還是僅保護選取的SVM：

- 您可以使用_叢集範圍_來設定叢集中所有SVM的外部金鑰管理。叢集管理員可以存取儲存在伺服器上的每個金鑰。
- 從ONTAP S9.6開始、您可以使用_SVM範圍_來設定叢集中命名SVM的外部金鑰管理。這最適合多租戶環境、每個租戶使用不同的SVM（或一組SVM）來提供資料。只有特定租戶的SVM管理員可以存取該租戶的金鑰。
  - 從ONTAP 9.17.1 開始，您可以使用巴比肯 KMS僅保護資料 SVM 的 NVE 金鑰。
  - 從功能升級到功能升級到ONTAP 功能升級、您可以使用 Azure Key Vault與Google Cloud KMS 僅保護資料 SVM 的 NVE 金鑰。從 9.12.0 開始、 AWS 的 KMS 都可以使用這項功能。

您可以在同一個叢集中使用這兩個範圍。如果SVM已設定金鑰管理伺服器、ONTAP 則僅使用這些伺服器來保護金鑰。否則ONTAP 、利用為叢集設定的金鑰管理伺服器來保護金鑰。

中提供已驗證的外部金鑰管理程式清單 "NetApp互通性對照表工具IMT （不含）"。您可以在 IMT 的搜尋功能中輸入「關鍵經理」一詞來找到此清單。

Azure Key Vault 和 AWS KMS 等雲端 KMS 供應商不支援 KMIP 。因此，這些項目並未列在 IMT 上。

支援詳細資料

下表顯示NVE支援詳細資料：

資源或功能	支援詳細資料
平台	需要AES-NI卸載功能。請參閱Hardware Universe 《銷售支援》（HWU）、確認您的平台是否支援NVE和NAE。

加密	從推出更新版本時開始ONTAP 、新建立的Aggregate和Volume會在您新增Volume加密（VE）授權、並設定內建或外部金鑰管理程式時、依預設進行加密。如果您需要建立未加密的Aggregate、請使用下列命令：
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	如果您需要建立純文字Volume、請使用下列命令：
	
	`volume create -encrypt false`
	
	在下列情況下、預設不會啟用加密：
	
	• 未安裝ve授權。
	• 未設定金鑰管理程式。
	• 平台或軟體不支援加密。
	• 硬體加密已啟用。

ONTAP	所有ONTAP實施。 ONTAP9.5 及更高版本支援Cloud Volumes ONTAP 。
裝置	HDD、SSD、混合式陣列LUN。
RAID	RAID0、RAID4、RAID-DP、RAID-TEC
磁碟區	資料磁碟區和現有 SVM 根磁碟區。您無法加密 MetroCluster 中繼資料磁碟區上的資料。在早於 9.14.1 的 ONTAP 版本中、您無法使用 NVE 加密 SVM 根 Volume 上的資料。從 ONTAP 9.14.1 開始、 ONTAP 支援 SVM 根磁碟區上的 NVE。
Aggregate層級加密	從推出支援Aggregate層級加密（NAE）的ONTAP NVE開始： • 如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。 • 您無法重新輸入Aggregate層級加密Volume的金鑰。 • Aggregate層級加密磁碟區不支援安全清除。 • 除了資料磁碟區之外、NAE也支援加密SVM根磁碟區和MetroCluster 元資料Volume。Nae不支援加密根磁碟區。
SVM範圍	從ONTAP 9.8 開始支援MetroCluster 。 從ONTAP 9.6 開始，NVE 僅支援 SVM 範圍的外部金鑰管理，而不支援板載金鑰管理員。
儲存效率	重複資料刪除、壓縮、壓縮、FlexClone。 即使將實體複本從父複本分割出去、複本仍會使用與父複本相同的金鑰。您應該執行 `volume move` 在分割複本上、分割複本之後會有不同的金鑰。
複寫	• 對於 Volume 複寫、來源和目的地磁碟區可以有不同的加密設定。可針對來源設定加密、也可針對目的地設定未設定加密、反之亦然。來源上設定的加密不會複寫到目的地。加密必須在來源和目的地上手動設定。請參閱設定 NVE和使用NVE加密Volume資料。 • 對於SVM複寫、目的地磁碟區會自動加密、除非目的地不包含支援Volume加密的節點、在這種情況下、複寫會成功、但目的地磁碟區不會加密。 • 針對部分組態、每個叢集都會從其設定的金鑰伺服器擷取外部金鑰管理金鑰。MetroCluster組態複寫服務會將OKM金鑰複寫至合作夥伴站台。
法規遵循	合規模式和企業模式均支援SnapLock ，但僅適用於新卷。您無法在現有SnapLock的流通量上啟用加密功能。
資料量FlexGroup	支援FlexGroup磁碟區。目的地Aggregate必須與來源Aggregate的類型相同、無論是Volume層級或Aggregate層級。從功能更新版開始、支援就地重新更新功能、以取代功能。ONTAP FlexGroup

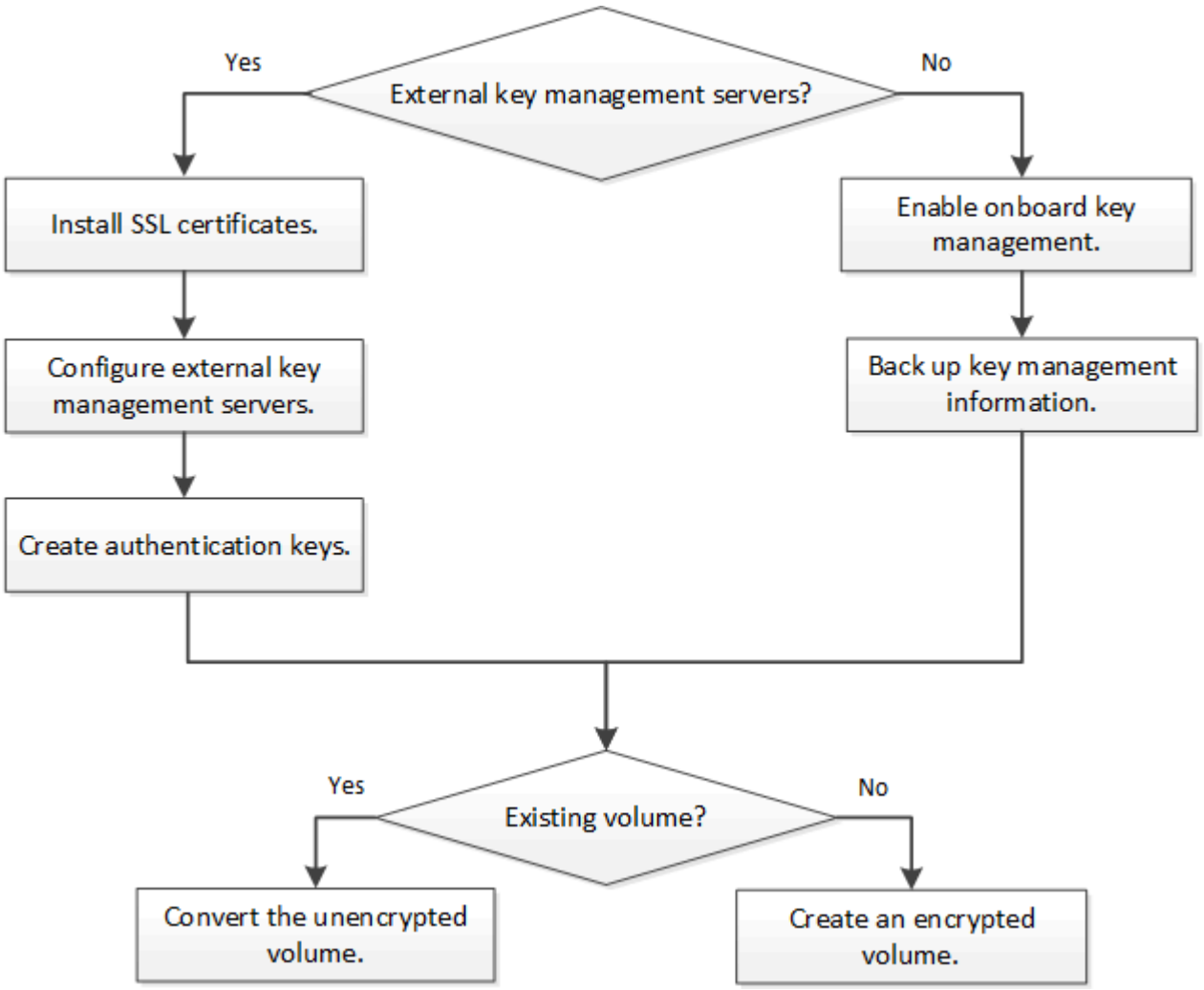
7-Mode轉換	從7-Mode Transition Tool 3.3開始、您可以使用7-Mode Transition Tool CLI、在叢集式系統上執行以複製為基礎的移轉、移轉至啟用NVE的目的地磁碟區。

相關資訊

- "常見問題集- NetApp Volume Encryption與NetApp Aggregate Encryption"
- "儲存聚合創建"

ONTAP NetApp磁碟區加密工作流程

您必須先設定金鑰管理服務、才能啟用磁碟區加密。您可以在新磁碟區或現有磁碟區上啟用加密。



"您必須安裝 VE 授權"並在使用 NVE 加密資料之前、先設定金鑰管理服務。在安裝授權之前"判斷ONTAP 您的版本是否支援NVE"，您應該：

設定 **NVE**

確定您的**ONTAP**叢集版本是否支援 **NVE**

安裝授權之前、您應該先判斷叢集版本是否支援NVE。您可以使用 `version` 判斷叢集版本的命令。

關於這項工作

叢集版本是ONTAP 叢集內任何節點上執行的最低版本的功能。

步驟

1. 判斷叢集版本是否支援NVE：

   `version -v`

   如果命令輸出顯示文字（針對「無靜態資料加密」），或您使用的平台未列於"支援詳細資料"，則不支援 NVE `1Ono-DARE` 。

在**ONTAP**叢集上安裝磁碟區加密許可證

VE授權可讓您在叢集中的所有節點上使用此功能。使用 NVE 加密資料之前、必須先取得此授權。隨附於"ONTAP One"。

在 ONTAP One 之前、 VE 授權已包含在加密套件中。加密套件已不再提供、但仍然有效。雖然目前並不需要"升級至 ONTAP One"、但現有客戶仍可選擇。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您必須已從銷售代表處收到 VE 授權金鑰、或已安裝 ONTAP 。

步驟

1. "確認已安裝 VE 授權"。

   VE 授權套件名稱為 `VE`。

2. 如果未安裝授權、"使用系統管理器或 ONTAP CLI 進行安裝"。

設定外部金鑰管理

了解如何使用**ONTAP NetApp**磁碟區加密設定外部金鑰管理

您可以使用一個或多個外部金鑰管理伺服器來保護叢集用於存取加密資料的金鑰。外部金鑰管理伺服器是儲存環境中的第三方系統，它使用金鑰管理互通性協定 (KMIP) 向節點提供金鑰。除了板載金鑰管理器之外， ONTAP還支援多個外部金鑰管理伺服器。

從ONTAP 9.10.1 開始，您可以使用 Azure Key Vault 或 Google Cloud Key Manager 服務 保護您的資料 SVM 的 NVE 金鑰。從ONTAP 9.11.1 開始，您可以在叢集中設定多個外部金鑰管理員。看配置叢集金鑰伺服器。從ONTAP 9.12.0 開始，您可以使用 "AWS 的 KMS" 保護您的資料 SVM 的 NVE 金鑰。從ONTAP 9.17.1 開始，您可以使用 OpenStack 的 巴比肯 KMS 保護您的資料 SVM 的 NVE 金鑰。

從 ONTAP 9.7 開始、您可以使用內建金鑰管理程式來儲存及管理驗證與加密金鑰。從 ONTAP 9.13.1 開始、您也可以使用外部金鑰管理員來儲存及管理這些金鑰。

Onboard Key Manager 會將金鑰儲存並管理在叢集內部的安全資料庫中。其範圍是叢集。外部金鑰管理程式會儲存和管理叢集外部的金鑰。其範圍可以是叢集或儲存 VM 。可以使用一或多個外部金鑰管理員。適用下列條件：

- 如果已啟用 Onboard Key Manager 、則無法在叢集層級啟用外部金鑰管理程式、但可以在儲存 VM 層級啟用外部金鑰管理程式。
- 如果在叢集層級啟用外部金鑰管理程式、則無法啟用 Onboard Key Manager 。

使用外部金鑰管理程式時、每個儲存 VM 和叢集最多可註冊四個主要金鑰伺服器。每個主要金鑰伺服器最多可叢集三個次要金鑰伺服器。

設定外部金鑰管理程式

若要新增儲存 VM 的外部金鑰管理程式、您應該在設定儲存 VM 的網路介面時新增選用閘道。如果儲存 VM 是在沒有網路路由的情況下建立的、您必須為外部金鑰管理程式明確建立路由。請參閱 "建立 LIF （網路介面）"。

步驟

您可以從 System Manager 的不同位置設定外部金鑰管理程式。

1. 若要設定外部金鑰管理程式、請執行下列其中一個啟動步驟。

工作流程	導覽	開始步驟
設定金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下，選擇 ⚙。選取 * 外部金鑰管理員 * 。
新增本機層	• 儲存 * > * Tiers*	選取 *+ 新增本機層 * 。核取標有「 Configure Key Manager 」的核取方塊。選取 * 外部金鑰管理員 * 。
準備儲存設備	• 儀表板 *	在 * 容量 * 區段中、選取 * 準備儲存 * 。 然後選取「設定金鑰管理程式」。選取 * 外部金鑰管理員 * 。
設定加密（僅限儲存 VM 範圍的金鑰管理程式）	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全 * 下的 * 加密 * 區段中，選擇 ⚙。

2. 要添加主密鑰服務器，請選擇 + Add ，然後填寫 **IP** 地址或主機名 * 和 ***Port** 字段。
3. 現有安裝的憑證會列在 * KMIP 伺服器 CA 憑證 * 和 * KMIP 用戶端憑證 * 欄位中。 您可以執行下列任一動作：
   - 選取 ⌄ 以選取您要對應至金鑰管理程式的已安裝憑證。（可以選取多個服務 CA 憑證、但只能選取一個用戶端憑證。）
   - 選取 * 新增憑證 * 以新增尚未安裝的憑證、並將其對應至外部金鑰管理員。
   - 選取 × 憑證名稱旁的、以刪除您不想對應至外部金鑰管理程式的已安裝憑證。

4. 若要新增次要金鑰伺服器、請在 * 次要金鑰伺服器 * 欄中選取 * 新增 * 、並提供詳細資料。
5. 選取 * 儲存 * 以完成組態。

編輯現有的外部金鑰管理程式

如果您已設定外部金鑰管理員、則可以修改其設定。

步驟

1. 若要編輯外部金鑰管理程式的組態、請執行下列其中一個開始步驟。

範圍	導覽	開始步驟
叢集範圍外部金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下，選擇 ⋮ ，然後選擇 * 編輯外部金鑰管理程式 * 。
儲存 VM 範圍外部金鑰管理程式	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全性 * 下的 * 加密 * 區段中、選取 ⋮ 、然後選取 * 編輯外部金鑰管理員 * 。

2. 現有的主要伺服器會列在 * 金鑰伺服器 * 表中。您可以執行下列作業：
   - 選取以新增金鑰伺服器 + Add 。
   - 選取包含金鑰伺服器名稱的表格儲存格結尾處、以刪除金鑰伺 ⋮ 服器。與該主要金鑰伺服器相關的次要金鑰伺服器也會從組態中移除。

刪除外部金鑰管理程式

如果磁碟區未加密、則可以刪除外部金鑰管理程式。

步驟

1. 若要刪除外部金鑰管理程式、請執行下列其中一個步驟。

範圍	導覽	開始步驟
叢集範圍外部金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下、選取 ⋮ 、然後選取 * 刪除外部金鑰管理員 * 。
儲存 VM 範圍外部金鑰管理程式	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全性 * 下的 * 加密 * 區段中、選取 ⋮ 、然後選取 * 刪除外部金鑰管理員 * 。

在關鍵經理之間移轉金鑰

當叢集上啟用多個金鑰管理程式時、金鑰必須從一個金鑰管理程式移轉至另一個金鑰管理程式。系統管理員會自動完成此程序。

- 如果已在叢集層級啟用 Onboard Key Manager 或外部金鑰管理程式、且某些磁碟區已加密、 然後、當您在儲存 VM 層級設定外部金鑰管理程式時、金鑰必須從叢集層級的 Onboard Key Manager 或外部金鑰管理程

式移轉至儲存 VM 層級的外部金鑰管理程式。系統管理員會自動完成此程序。

- 如果在儲存 VM 上建立的磁碟區沒有加密、則不需要移轉金鑰。

在**ONTAP**叢集上安裝 **SSL** 憑證

叢集與KMIP伺服器使用KMIP SSL憑證來驗證彼此的身分、並建立SSL連線。在使用KMIP伺服器設定SSL連線之前、您必須先安裝叢集的KMIP用戶端SSL憑證、以及KMIP伺服器根憑證授權單位（CA）的SSL公開憑證。

關於這項工作

在HA配對中、兩個節點必須使用相同的公有和私有KMIP SSL憑證。如果您將多個HA配對連線至相同的KMIP伺服器、HA配對中的所有節點都必須使用相同的公有和私有KMIP SSL憑證。

開始之前

- 建立憑證、KMIP伺服器和叢集的伺服器上、必須同步時間。
- 您必須已取得叢集的公用SSL KMIP用戶端憑證。
- 您必須取得與叢集SSL KMIP用戶端憑證相關的私密金鑰。
- SSL KMIP用戶端憑證不得受密碼保護。
- 您必須已取得KMIP伺服器根憑證授權單位（CA）的SSL公開憑證。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

您可以在叢集上安裝憑證之前或之後、在KMIP伺服器上安裝用戶端和伺服器憑證。

步驟

1. 安裝叢集的SSL KMIP用戶端憑證：

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   系統會提示您輸入SSL KMIP公開和私有憑證。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. 安裝KMIP伺服器根憑證授權單位（CA）的SSL公開憑證：

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

相關資訊

- "安全性憑證安裝"

在**ONTAP 9.6** 及更高版本中為 **NVE** 啟用外部金鑰管理

使用 KMIP 伺服器來保護叢集用於存取加密資料的金鑰。從ONTAP 9.6 開始，您可以選擇配置單獨的外部金鑰管理器來保護資料 SVM 用於存取加密資料的金鑰。

從 ONTAP 9.11.1 開始、每個主要金鑰伺服器最多可新增 3 個次要金鑰伺服器、以建立叢集金鑰伺服器。如需詳細資訊、請參閱 設定叢集式外部金鑰伺服器。

關於這項工作

您最多可以將四個 KMIP 伺服器連接到叢集或 SVM。使用至少兩台伺服器以實現冗餘和災難復原。

外部金鑰管理的範圍決定了金鑰管理伺服器是保護叢集中的所有SVM、還是僅保護選取的SVM：

- 您可以使用_叢集範圍_來設定叢集中所有SVM的外部金鑰管理。叢集管理員可以存取儲存在伺服器上的每個金鑰。
- 從ONTAP 功能表9.6開始、您可以使用_SVM範圍來設定叢集中資料SVM的外部金鑰管理。這最適合多租戶環境、每個租戶使用不同的SVM（或一組SVM）來提供資料。只有特定租戶的SVM管理員可以存取該租戶的金鑰。
- 對於多租戶環境、請使用下列命令安裝_MT_EK-Mgmt_的授權：

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  如"指令參考資料ONTAP"需詳細 `system license add`資訊，請參閱。

您可以在同一個叢集中使用這兩個範圍。如果SVM已設定金鑰管理伺服器、ONTAP 則僅使用這些伺服器來保護金鑰。否則ONTAP 、利用為叢集設定的金鑰管理伺服器來保護金鑰。

您可以在叢集範圍設定內建金鑰管理、並在SVM範圍設定外部金鑰管理。您可以使用 `security key-manager key migrate` 命令將金鑰從叢集範圍內的機載金鑰管理移轉至 SVM 範圍內的外部金鑰管理程式。

如"指令參考資料ONTAP"需詳細 `security key-manager key migrate`資訊，請參閱。

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- KMIP 伺服器必須能夠從每個節點的節點管理 LIF 存取。
- 您必須是叢集或SVM管理員、才能執行此工作。
- 在MetroCluster環境中：
  - 在啟用外部金鑰管理之前，必須完全配置MetroCluster 。
  - 您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。
  - 必須在兩個叢集上配置外部密鑰管理器。

步驟

1. 設定叢集的金鑰管理程式連線：

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   這 `security key-manager external enable`命令替換 `security key-manager setup`命令。如果在叢集登入提示字元下執行該命令， `*admin_SVM*`預設為目前叢集的管理 SVM。您可以運行 `security key-manager external modify`命令來更改外部密鑰管理配置。

下列命令可啟用的外部金鑰管理 `cluster1` 使用三個外部金鑰伺服器。第一個金鑰伺服器是使用其主機名稱和連接埠來指定、第二個金鑰伺服器是使用IP位址和預設連接埠來指定、第三個金鑰伺服器則是使用IPv6位址和連接埠來指定：

```
clusterl::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 設定SVM的金鑰管理程式：

```
security key-manager external enable -vserver SVM -key-servers
host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

- 如果在 SVM 登入提示字元下執行該命令， `SVM`預設為當前 SVM。您可以運行 `security key-manager external modify`命令來更改外部密鑰管理配置。
- 在支援資料SVM的環境中、如果您要設定外部金鑰管理、就不需要重複執行MetroCluster `security key-manager external enable` 合作夥伴叢集上的命令。

下列命令可啟用的外部金鑰管理 `svm1` 使用單一金鑰伺服器聆聽預設連接埠 5696 ：

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. 針對任何其他SVM重複最後一個步驟。

您也可以使用 `security key-manager external add-servers`命令來設定其他 SVM 。命令會 `security key-manager external add-servers`取代 `security key-manager add`命令。如"指令參考資料ONTAP"需詳細 `security key-manager external add-servers`資訊，請參閱。

4. 確認所有已設定的KMIP伺服器均已連線：

```
security key-manager external show-status -node node_name
```

命令會 `security key-manager external show-status`取代 `security key-manager show -status`命令。如"指令參考資料ONTAP"需詳細 `security key-manager external show-status`資訊，請參閱。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  -----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. 也可以將純文字磁碟區轉換為加密磁碟區。

   `volume encryption conversion start`

   在轉換磁碟區之前，必須完全設定外部金鑰管理員。

相關資訊

- 設定叢集式外部金鑰伺服器
- "系統許可證添加"
- "安全金鑰管理員金鑰遷移"
- "安全金鑰管理員外部新增伺服器"
- "安全金鑰管理員外部顯示狀態"

在ONTAP 9.5 及更早版本中為 NVE 啟用外部金鑰管理

您可以使用一或多個KMIP伺服器來保護叢集用來存取加密資料的金鑰。您最多可將四個KMIP伺服器連線至一個節點。建議至少使用兩部伺服器來進行備援和災難恢復。

關於這項工作

可為叢集中的所有節點設定KMIP伺服器連線。ONTAP

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- 您必須是叢集管理員才能執行此工作。
- 在設定外部金鑰管理程式之前、您必須先設定MetroCluster 此解決方案。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

步驟

1. 設定叢集節點的金鑰管理程式連線：

   `security key-manager setup`

   金鑰管理程式設定隨即開始。

   在MetroCluster環境中，您必須在兩個叢集上執行此命令。詳細了解 `security key-manager setup`在"指令參考資料ONTAP"。

2. 在每個提示字元輸入適當的回應。
3. 新增KMIP伺服器：

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

4. 新增額外的KMIP伺服器以提供備援：

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

5. 確認所有已設定的KMIP伺服器均已連線：

   `security key-manager show -status`

   詳細了解此過程中所述的命令"指令參考資料ONTAP"。

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. 也可以將純文字磁碟區轉換為加密磁碟區。

   `volume encryption conversion start`

   在轉換磁碟區之前、必須先完整設定外部金鑰管理程式。在 MetroCluster 環境中、必須在兩個站台上設定外部金鑰管理員。

透過雲端供應商管理**ONTAP**資料 **SVM** 的 **NVE** 金鑰

從 ONTAP 9.10.1 開始，您可以在雲端代管應用程式中使用"Azure Key Vault（AKV）"和"Google Cloud Platform的金鑰管理服務（雲端KMS）"保護 ONTAP 加密金鑰。從 ONTAP 9.12.0 開始，您也可以使用來保護 NVE 金鑰"AWS 的 KMS"。

AWS KMS 、 AKV 和 Cloud KMS 可用於保護 "NetApp Volume Encryption（NVE）金鑰" 僅適用於資料SVM。

關於這項工作

您可以使用 CLI 或 ONTAP REST API 來啟用雲端供應商的金鑰管理。

使用雲端供應商保護金鑰時、請注意、根據預設、資料 SVM LIF 會用於與雲端金鑰管理端點通訊。節點管理網路用於與雲端供應商的驗證服務（login.microsoftonline.com for Azure；oauth2.googleapis.com for Cloud KMS ）進行通訊。如果叢集網路未正確設定，叢集將無法正確使用金鑰管理服務。

使用雲端供應商金鑰管理服務時、您應注意下列限制：

- 雲端供應商金鑰管理不適用於 NetApp 儲存加密（ NSE ）和 NetApp Aggregate Encryption （ NAE ）。"外部KMIP" 可以改用。
- 雲端供應商金鑰管理不適用於 MetroCluster 組態。
- 雲端供應商金鑰管理只能在資料 SVM 上設定。

開始之前

- 您必須在適當的雲端供應商上設定 KMS 。
- ONTAP 叢集的節點必須支援 NVE 。
- "您必須已安裝 Volume Encryption （ VE ）和多租戶加密金鑰管理（ MTEKM ）授權"。這些授權隨附於"ONTAP One"。
- 您必須是叢集或 SVM 管理員。
- 資料 SVM 不得包含任何加密的磁碟區、也不得採用金鑰管理程式。如果資料 SVM 包含加密的磁碟區、您

必須先移轉這些磁碟區、才能設定 KMS 。

啟用外部金鑰管理

啟用外部金鑰管理取決於您使用的特定金鑰管理程式。選擇適當的金鑰管理程式和環境標籤。

AWS

開始之前

- 您必須為 AWS KMS 金鑰建立授權、以便由管理加密的 IAM 角色使用。IAM 角色必須包含允許下列作業的原則：
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

    如需詳細資訊、請參閱 AWS 文件 "補助"。

在 **ONTAP SVM** 上啟用 **AWS KMV**

1. 開始之前、請先從 AWS KMS 取得存取金鑰 ID 和秘密金鑰。
2. 將權限層級設為進階：
   `set -priv advanced`
3. 啟用 AWS KMS ：
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. 出現提示時、請輸入秘密金鑰。
5. 確認 AWS KMS 已正確設定：
   `security key-manager external aws show -vserver` *`svm_name`*

   如"指令參考資料ONTAP"需詳細 `security key-manager external aws`資訊，請參閱。

Azure

在 **ONTAP SVM** 上啟用 **Azure Key Vault**

1. 開始之前、您必須先從Azure帳戶取得適當的驗證認證資料、包括用戶端機密或憑證。您也必須確保叢集中的所有節點都正常運作。您可以使用命令來檢查 `cluster show`。如"指令參考資料ONTAP"需詳細 `cluster show`資訊，請參閱。
2. 將權限層級設為進階
   `set -priv advanced`
3. 在 SVM 上啟用 AKV
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`
   出現提示時、請輸入 Azure 帳戶的用戶端憑證或用戶端機密。
4. 確認 AKV 已正確啟用：
   `security key-manager external azure show vserver` *`svm_name`*
   如果服務連線能力不正常、請透過資料 SVM LIF 建立與 AKV 金鑰管理服務的連線。

   如"指令參考資料ONTAP"需詳細 `security key-manager external azure`資訊，請參閱。

Google Cloud

在 **ONTAP SVM** 上啟用雲端 **KMS**

1. 開始之前、請先以 JSON 格式取得 Google Cloud KMS 帳戶金鑰檔案的私密金鑰。您可以在GCP帳戶中找到這項資訊。您也必須確保叢集中的所有節點都正常運作。您可以使用命令來檢查 `cluster show`。如"指令參考資料ONTAP"需詳細 `cluster show`資訊，請參閱。
2. 將權限等級設為進階：
   `set -priv advanced`
3. 在 SVM 上啟用 Cloud KMS
   `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
   出現提示時、請使用服務帳戶私密金鑰輸入 JSON 檔案的內容
4. 驗證 Cloud KMS 是否配置了正確的參數：
   `security key-manager external gcp show vserver svm_name`現狀 `kms_wrapped_key_status`將`"UNKNOWN"`如果沒有建立加密磁碟區。如果服務可達性不正常，則透過資料 SVM LIF 建立與 GCP 金鑰管理服務的連線。

   如"指令參考資料ONTAP"需詳細 `security key-manager external gcp`資訊，請參閱。

如果已為資料SVM設定一或多個加密磁碟區、且對應的NVE金鑰由管理SVM內建金鑰管理程式管理、則這些金鑰應移轉至外部金鑰管理服務。若要使用 CLI 執行此作業、請執行命令：
`security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM`
在成功移轉資料 SVM 的所有 NVE 金鑰之前、無法為租戶的資料 SVM 建立新的加密磁碟區。

相關資訊

- "使用適用於 Cloud Volumes ONTAP 的 NetApp 加密解決方案來加密磁碟區"
- "安全金鑰管理員外部"

使用 **Barbican KMS** 管理**ONTAP**金鑰

從ONTAP 9.17.1 開始，您可以使用 OpenStack 的"巴比肯 KMS"保護ONTAP加密金鑰。BarbicanKMS 是一項安全儲存和存取金鑰的服務。 BarbicanKMS 可用於保護資料 SVM 的NetApp磁碟區加密 (NVE) 金鑰。 Barbican依賴"OpenStack Keystone" ，OpenStack 的身份服務，用於身份驗證。

關於這項工作

您可以使用 CLI 或ONTAP REST API 使用 Barbican KMS 設定金鑰管理。在 9.17.1 版本中，Barbican KMS 支援有以下限制：

- Barbican KMS 不支援NetApp儲存加密 (NSE) 和NetApp聚合加密 (NAE)。或者，您可以使用"外部 KMIP"或"板載密鑰管理器 (OKM)"用於 NSE 和 NVE 金鑰。
- MetroCluster配置不支援 Barbican KMS。
- Barbican KMS 只能為資料 SVM 配置，不適用於管理 SVM。

除非另有說明，管理員 `admin`特權等級可以執行下列操作程序。

開始之前

- 必須配置 Barbican KMS 和 OpenStack Keystone 。您用於 Barbican 的 SVM 必須能夠透過網路存取

Barbican 和 OpenStack Keystone伺服器。

- 如果您正在為 Barbican 和 OpenStack Keystone伺服器使用自訂憑證授權單位 (CA)，則必須使用 `security certificate install -type server-ca -vserver <admin_svm>` 。

建立並啟動 **Barbican KMS** 配置

您可以為 SVM 建立新的 Barbican KMS 配置並將其啟動。一個 SVM 可以有多個非活動的 Barbican KMS 配置，但一次只能有一個處於活動狀態。

步驟

1. 為 SVM 建立新的非活動 Barbican KMS 配置：

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id`是 `Barbican 密鑰加密密鑰 (KEK) 的密鑰標識符。請輸入完整的 URL，包括 `https://` 。

     某些 URL 包含問號 (?)。問號用於啟動ONTAP命令列活動幫助。要輸入帶有問號的 URL，您需要先使用以下命令停用活動協助 `set -active-help false` 。稍後可以使用以下命令重新啟用主動協助 `set -active-help true`了解更多信息"指令參考資料ONTAP" 。

   - `-keystone-url`是 `OpenStack Keystone授權主機的 URL。請輸入完整的 URL，包括 `https://` 。

   - `-application-cred-id`是應用程式憑證 ID。

     輸入此命令後，系統將提示您輸入應用程式憑證金鑰。此指令將建立一個非活動的 Barbican KMS 配置。

     以下範例建立一個名為的非活動 Barbican KMS 配置 `config1`對於`SVM `svm1` ：

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. 啟動新的 Barbican KMS 配置：

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

您可以使用此命令在 Barbican KMS 配置之間切換。如果 SVM 上已存在活動的 Barbican KMS 配置，則該配置將處於非活動狀態，並啟動新的配置。

3. 驗證新的 Barbican KMS 配置是否處於活動狀態：

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

此指令將提供 SVM 或節點上活動的 Barbican KMS 配置的狀態。例如，如果 SVM `svm1`在節點上 `node1` 具有活動的 Barbican KMS 配置，以下命令將傳回該配置的狀態：

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

更新 **Barbican KMS** 配置的憑證和設置

您可以檢視和更新活動或非活動的 Barbican KMS 配置的目前設定。

步驟

1. 查看 SVM 的目前 Barbican KMS 配置：

```
security key-manager external barbican show -vserver <svm_name>
```

顯示 SVM 上每個 Barbican KMS 配置的金鑰 ID、OpenStack Keystone URL 和應用程式憑證 ID。

2. 更新 Barbican KMS 配置的設定：

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

此指令更新指定 Barbican KMS 設定的逾時和驗證設定。 `timeout`確定ONTAP在連線失敗前等待 Barbican 回應的時間（以秒為單位）。預設 `timeout`是十秒。 `verify`和 `verify-host`確定在連線之前是否應分別驗證 Barbican 主機的身份和主機名稱。預設情況下，這些參數設定為 `true`。這 `vserver`和 `config-name`參數是必需的。其他參數是可選的。

3. 如果需要，請更新活動或非活動的 Barbican KMS 配置的憑證：

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

輸入此命令後，系統將提示您輸入新的應用程式憑證金鑰。

4. 如果需要，為活動的 Barbican KMS 設定恢復遺失的 SVM 金鑰加密金鑰 (KEK)：
   a. 使用以下方式恢復遺失的 SVM KEK `security key-manager external barbican restore`：

```
security key-manager external barbican restore -vserver <svm_name>
```

此命令將透過與 Barbican 伺服器通訊來恢復活動 Barbican KMS 配置的 SVM KEK。

5. 如果需要，請為 Barbican KMS 設定重新金鑰 SVM KEK：
   a. 將權限層級設為進階：

```
set -privilege advanced
```

   b. 使用以下方式重新金鑰 SVM KEK `security key-manager external barbican rekey-internal`：

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

此指令會為指定的 SVM 產生新的 SVM KEK，並使用新的 SVM KEK 重新封裝磁碟區加密金鑰。新的 SVM KEK 將受到有效的 Barbican KMS 配置的保護。

在 **Barbican KMS** 和 **Onboard Key Manager** 之間遷移金鑰

您可以將密鑰從 Barbican KMS 遷移到板載密鑰管理器 (OKM)，反之亦然。要了解有關 OKM 的更多信息，請參閱"啟用更新版本的更新版本、以利執行內建金鑰管理ONTAP"。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 如果需要，將密鑰從 Barbican KMS 遷移到 OKM：

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name`是具有 Barbican KMS 配置的 SVM 的名稱。

3. 如果需要，將密鑰從 OKM 遷移到 Barbican KMS：

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

停用並刪除 **Barbican KMS** 配置

您可以停用沒有加密磁碟區的活動 Barbican KMS 配置，並且可以刪除非活動的 Barbican KMS 配置。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 禁用活動的 Barbican KMS 配置：

```
security key-manager keystore disable -vserver <svm_name>
```

如果 SVM 上存在 NVE 加密磁碟區，則必須解密它們，否則遷移金鑰在停用 Barbican KMS 配置之前。啟動新的 Barbican KMS 配置不需要解密 NVE 磁碟區或遷移金鑰，並且會停用目前活動的 Barbican KMS 配置。

3. 刪除不活動的 Barbican KMS 配置：

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

在**ONTAP 9.6** 及更高版本中啟用 **NVE** 的板載金鑰管理

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在存取加密磁碟區或自我加密磁碟的每個叢集上啟用 Onboard Key Manager 。

關於這項工作

您必須執行 `security key-manager onboard sync` 每次將節點新增至叢集時的命令。

如果您有 MetroCluster 組態、則必須執行 `security key-manager onboard enable` 命令先在本機叢集上執行、然後執行 `security key-manager onboard sync` 在遠端叢集上使用相同密碼的命令。當您執行時 `security key-manager onboard enable` 本機叢集的命令、然後在遠端叢集上進行同步處理、您不需要執行 `enable` 從遠端叢集再次執行命令。

詳細了解 `security key-manager onboard enable`和 `security key-manager onboard sync`在"指令參考資料ONTAP"。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。您可以使用 `cc-mode-enabled=yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `cc-mode-enabled=yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

在設定ONTAP資料加密時，為了滿足商業機密解決方案 (CSfC) 的要求，您必須將 NSE 與 NVE 一起使用，並確保在通用標準模式下啟用板載金鑰管理員。看"CSfC解決方案簡介"。

> 當「內建金鑰管理程式」在「一般條件」模式中啟用時 (`cc-mode-enabled=yes`）、系統行為會以下列方式變更：
>
> - 系統會監控在「一般準則」模式下運作時、連續嘗試失敗的叢集密碼。
>
> 如果 5 次輸入叢集密碼失敗，請等待 24 小時或重新啟動節點以重設限制。
>
> - 系統映像更新會使用NetApp RSA-3072程式碼簽署憑證搭配SHA-384程式碼簽署摘要、來檢查映像完整性、而非一般的NetApp RSA-2048程式碼簽署憑證和SHA-256程式碼簽署摘要。
>
> 升級命令透過檢查各種數位簽名來驗證影像內容是否已更改或損壞。如果驗證成功，系統將繼續進行影像更新過程的下一步；否則，影像更新失敗。詳細了解 `cluster image`在"指令參考資料ONTAP"。

> 板載密鑰管理器將密鑰儲存在揮發性記憶體中。當系統重新啟動或停止時，揮發性記憶體的內容將會被清除。系統停止後 30 秒內清除揮發性記憶體。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 在設定Onboard Key Manager之前、您必須先設定MetroCluster 這個靜態環境。

步驟

1. 啟動金鑰管理程式設定：

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

設定 `cc-mode-enabled=yes` 要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE `cc-mode-enabled=yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。。 `- cc-mode-enabled` MetroCluster 組態不支援此選項。 。 `security key-manager onboard enable` 命令會取代 `security key-manager setup` 命令。

2. 輸入一個介於 32 到 256 個字元之間的密碼，或對於“`cc-mode`”，輸入一個介於 64 到 256 個字元之間的密碼。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

3. 在通關密碼確認提示下、重新輸入通關密碼。
4. 確認已建立驗證金鑰：

   ```
   security key-manager key query -key-type NSE-AK
   ```

   命令會 `security key-manager key query`取代 `security key-manager query key`命令。

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

5. 您可以選擇將純文字磁碟區轉換為加密磁碟區。

   ```
   volume encryption conversion start
   ```

   在轉換磁碟區之前、必須先完整設定 Onboard Key Manager 。在 MetroCluster 環境中、兩個站台都必須設定內建金鑰管理員。

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

配置板載金鑰管理器密碼後，手動將資訊備份到儲存系統外部的安全位置。看"手動備份內建金鑰管理資訊"。

相關資訊

- "叢集影像命令"
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員金鑰查詢"
- "安全金鑰管理員板載啟用"

在**ONTAP 9.5** 及更早版本中為 **NVE** 啟用板載金鑰管理

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用Onboard Key Manager。

關於這項工作

您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。

如果您使用MetroCluster 的是「不確定」組態、請參閱下列準則：

- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

密碼嘗試失敗後、您必須重新啟動節點。

開始之前

- 如果您將 NSE 或 NVE 與外部金鑰管理 (KMIP) 伺服器一起使用，請刪除外部金鑰管理器資料庫。

  "從外部金鑰管理移轉至內建金鑰管理"

- 您必須是叢集管理員才能執行此工作。
- 在配置板載金鑰管理器之前，請先配置MetroCluster環境。

步驟

1. 啟動金鑰管理程式設定：

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 此選項可要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。

   下列範例會在叢集1上開始設定金鑰管理程式、而不要求在每次重新開機後輸入通關密碼：

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. 輸入 `yes` 在提示下設定內建金鑰管理。
3. 在通關密碼提示字元中、輸入32到256個字元之間的通關密碼、或輸入「'cc-mode'」（64到256個字元之間的通關密碼）。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

4. 在通關密碼確認提示下、重新輸入通關密碼。
5. 驗證是否已為所有節點設定金鑰：

   `security key-manager show-key-store`

   ```
   cluster1::> security key-manager show-key-store

   Node: node1
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK

   Node: node2
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK
   ```

   詳細了解 `security key-manager show-key-store`在"指令參考資料ONTAP"。

6. 也可以將純文字磁碟區轉換為加密磁碟區。

   `volume encryption conversion start`

   在轉換卷之前配置板載密鑰管理器。在MetroCluster環境中，在兩個站點上進行配置。

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

配置板載金鑰管理器密碼時，請將資訊備份到儲存系統外部的安全位置，以防災難發生。看"手動備份內建金鑰管理資訊"。

相關資訊

- "手動備份內建金鑰管理資訊"

- "從外部金鑰管理移轉至內建金鑰管理"
- "安全金鑰管理員顯示金鑰庫"

在新新增的**ONTAP**節點中啟用板載金鑰管理

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用Onboard Key Manager。

> 對於ONTAP 9.6 及更高版本，您必須執行 `security key-manager onboard sync` 每次向叢集新增節點時執行此命令。
>
> 若為 ONTAP 9.5 或更早版本、您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。
>
> 如果您將節點新增至具有板載金鑰管理的集群，請執行此命令來刷新遺失的金鑰。

如果您使用MetroCluster 的是「不確定」組態、請參閱下列準則：

- 從 ONTAP 9.6 開始、您必須執行 `security key-manager onboard enable` 先在本機叢集上執行 `security key-manager onboard sync` 在遠端叢集上、使用相同的複雜密碼。

  深入瞭解 `security key-manager onboard enable`及 `security key-manager onboard sync` "指令參考資料ONTAP"。

- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

> 如果密碼嘗試失敗，請重新啟動節點。重新啟動後，您可以再次嘗試輸入密碼。

相關資訊

- "叢集影像命令"
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員板載啟用"

使用 **NVE** 或 **NAE** 加密卷數據

了解如何使用 **NVE** 加密**ONTAP**磁碟區數據

從使用支援功能9.7開始ONTAP 、如果您擁有VE授權、以及內建或外部金鑰管理、則根據

預設會啟用Aggregate和Volume加密。對於支援更新版本的支援、您可以在新磁碟區或現有磁碟區上啟用加密功能。ONTAP您必須先安裝VE授權並啟用金鑰管理、才能啟用Volume加密。NVE符合FIPS-140-2第1級標準。

在 **ONTAP** 中啟用含 **VE** 授權的 **Aggregate** 層級加密

從 ONTAP 9 7 開始"VE 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。從ONTAP 功能區9.6開始、您可以使用Aggregate層級加密、將金鑰指派給內含的Aggregate、以便加密磁碟區。

關於這項工作

如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。NVE不支援Aggregate層級的重複資料刪除。

啟用Aggregate層級加密的Aggregate稱為_NAE Aggregate（適用於NetApp Aggregate Encryption）。NAE Aggregate中的所有磁碟區都必須使用NAE或NVE加密進行加密。使用Aggregate層級加密、您在Aggregate中建立的磁碟區預設會使用NAE加密進行加密。您可以置換預設值、改用NVE加密。

NAE Aggregate不支援純文字磁碟區。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 啟用或停用Aggregate層級加密：

至…	使用此命令…
使用ONTAP NetApp 9.7或更新版本建立NAE Aggregate	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
使用ONTAP NetApp 9.6建立NAE Aggregate	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
將非NAE Aggregate轉換為NAE Aggregate	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
將NAE Aggregate轉換為非NAE Aggregate	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

詳細了解 `storage aggregate modify`在"指令參考資料ONTAP" 。

下列命令可在上啟用彙總層級加密 `aggr1`：

- 更新版本：ONTAP

```
cluster1::> storage aggregate create -aggregate aggr1
```

- 更新版本：ONTAP

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

如"指令參考資料ONTAP"需詳細 `storage aggregate create`資訊，請參閱。

2. 確認已啟用Aggregate進行加密：

`storage aggregate show -fields encrypt-with-aggr-key`

下列命令會驗證是否存在此問題 `aggr1` 已啟用加密：

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `storage aggregate show`資訊，請參閱。

完成後

執行 `volume create` 建立加密磁碟區的命令。

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

在 **ONTAP** 的新磁碟區上啟用加密

您可以使用 `volume create` 在新磁碟區上啟用加密的命令。

關於這項工作

您可以使用NetApp Volume Encryption（NVE）加密磁碟區、從ONTAP NetApp Aggregate Encryption（NAE）開始加密磁碟區。若要深入瞭解NAE和NVE、請參閱 Volume加密總覽。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

啟用更新版本的加密程序ONTAP 會因ONTAP 您使用的版本和您的特定組態而有所不同：

- 如果ONTAP 啟用、請從支援的問題9.4開始 `cc-mode` 設定Onboard Key Manager時、您可以使用建立的磁碟區 `volume create` 無論您是否指定、命令都會自動加密 `-encrypt true`。

- 在更新版本的版本中、您必須使用ONTAP `-encrypt true` 與 `volume create` 啟用加密的命令（前提是您未啟用 `cc-mode`）。
- 如果您想要在ONTAP 32位址9.6中建立NAE Volume、則必須在Aggregate層級啟用NAE。請參閱 使用VE授權啟用Aggregate層級加密 以取得此工作的詳細資料。
- 從 ONTAP 9 7 開始"VE 授權"、新建立的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。根據預設、在NAE Aggregate中建立的新磁碟區將為NAE類型、而非NVE。
  - 如有新增、請參閱ONTAP 更新版本的 `-encrypt true` 至 `volume create` 命令若要在NAE Aggregate中建立磁碟區、該磁碟區將採用NVE加密、而非NAE。NAE Aggregate中的所有磁碟區都必須使用NVE或NAE進行加密。

NAE集合體不支援純文字磁碟區。

步驟

1. 建立新磁碟區、並指定是否在磁碟區上啟用加密。如果新磁碟區位於NAE Aggregate中、則根據預設、該磁碟區將是NAE磁碟區：

若要建立…	使用此命令…
NAE Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
NVE Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + 在不支援NAE的情況下、使用支援的版本為ONTAP `-encrypt true` 指定應使用NVE加密磁碟區。在以NAE集合體建立Volume的版本中ONTAP 、 `-encrypt true` 取代預設的NAE加密類型、改為建立NVE Volume。
純文字Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

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

2. 確認已啟用磁碟區進行加密：

   ```
   volume show -is-encrypted true
   ```

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

結果

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

在現有**ONTAP**磁碟區上啟用 **NAE** 或 **NVE**

您可以使用 `volume move start` 或 `volume encryption conversion start` 在

現有磁碟區上啟用加密的命令。

關於這項工作

您可以使用 `volume encryption conversion start`命令可以「就地」啟用現有磁碟區的加密，而無需將磁碟區移動到其他位置。或者，您可以使用 `volume move start`命令。

使用**Volume Encryption Conversion start**命令、在現有磁碟區上啟用加密

您可以使用 `volume encryption conversion start`命令來啟用現有磁碟區的「就地」加密，而無需將磁碟區移動到其他位置。

在您開始轉換作業之後、必須完成此作業。如果您在作業期間遇到效能問題、可以執行 `volume encryption conversion pause` 暫停作業的命令、以及 `volume encryption conversion resume` 命令以恢復作業。

您無法使用 `volume encryption conversion start` 轉換 SnapLock Volume 。

步驟

1. 在現有磁碟區上啟用加密：

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

   如"指令參考資料ONTAP"需詳細 `volume encryption conversion start`資訊，請參閱。

   下列命令可在現有磁碟區上啟用加密 `vol1`：

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   系統會為磁碟區建立加密金鑰。磁碟區上的資料已加密。

2. 確認轉換作業的狀態：

   `volume encryption conversion show`

   如"指令參考資料ONTAP"需詳細 `volume encryption conversion show`資訊，請參閱。

   下列命令會顯示轉換作業的狀態：

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume    Start Time           Status
   -------   ------    ------------------   ----------------------------
   vs1       vol1      9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 轉換作業完成後、請確認磁碟區已啟用加密功能：

   `volume show -is-encrypted true`

如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate   State   Type   Size   Available   Used
-------   ------   ---------   -----   ----   -----   ---------  ----
vs1       vol1     aggr2      online     RW   200GB     160.0GB   20%
```

結果

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

使用**Volume Move start**命令在現有磁碟區上啟用加密

您可以使用 `volume move start`命令來移動現有的磁碟區來啟用加密。您可以使用相同的Aggregate或不同的Aggregate。

關於這項工作

- 從 ONTAP 9.8 開始、您可以使用 `volume move start` 在 SnapLock 或 FlexGroup 磁碟區上啟用加密。
- 從 ONTAP 9.4 開始、如果您在設定內建金鑰管理程式時啟用「 cc 模式」、就會使用建立磁碟區 `volume move start` 命令會自動加密。您不需要指定 `-encrypt-destination true`。
- 從ONTAP 功能區9.6開始、您可以使用Aggregate層級的加密功能、將金鑰指派給內含的Aggregate、以供移動的磁碟區使用。使用唯一金鑰加密的磁碟區稱為 *NVE Volumes* （意指它使用 NetApp Volume Encryption ）。使用Aggregate層級金鑰加密的Volume稱為_NAE Volume（適用於NetApp Aggregate Encryption ）。NAE集合體不支援純文字磁碟區。
- 從 ONTAP 9.14.1 開始、您可以使用 NVE 加密 SVM 根 Volume 。如需詳細資訊、請參閱 在 SVM 根磁碟區上設定 NetApp Volume Encryption。

開始之前

您必須是叢集管理員才能執行此工作、或是叢集管理員已委派權限的SVM管理員。

"委派權限以執行Volume Move命令"

步驟

1. 移動現有磁碟區、並指定是否在磁碟區上啟用加密：

若要轉換…	使用此命令…
NVE Volume的純文字磁碟區	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`

NAE磁碟區的NVE或純文字磁碟區（假設目的地已啟用Aggregate層級加密）	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
NAE Volume至NVE Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
NAE磁碟區至純文字磁碟區	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
從NVE磁碟區移至純文字磁碟區	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

下列命令會轉換名為的純文字磁碟區 `vol1` 至 NVE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

假設目的地上已啟用 Aggregate 層級加密、下列命令會轉換名為的 NVE 或純文字磁碟區 `vol1` 至 NAE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

下列命令會轉換名為的 NAE Volume `vol2` 至 NVE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

下列命令會轉換名為的 NAE Volume `vol2` 至純文字磁碟區：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

下列命令會轉換名為的 NVE Volume `vol2` 至純文字磁碟區：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. 檢視叢集磁碟區的加密類型：

   `volume show -fields encryption-type none|volume|aggregate`

   ◦ `encryption-type` 欄位可在 ONTAP 9.6 及更新版本中取得。

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示中的磁碟區加密類型 `cluster2`：

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. 確認已啟用磁碟區進行加密：

   `volume show -is-encrypted true`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示上的加密磁碟區 `cluster2`：

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

結果

如果您使用 KMIP 伺服器來儲存節點的加密金鑰、 ONTAP 會在您加密磁碟區時自動將加密金鑰推送至伺服器。

在**ONTAP SVM** 根磁碟區上設定 **NVE**

從 ONTAP 9.14.1 開始、您可以在儲存 VM （ SVM ）根磁碟區上啟用 NetApp Volume Encryption （ NVE ）。透過 NVE 、根磁碟區會使用唯一金鑰進行加密、以提高 SVM 的安全性。

關於這項工作

只有在建立 SVM 之後、才能在 SVM 根 Volume 上啟用 NVE 。

開始之前

- SVM 根磁碟區不得位於使用 NetApp Aggregate Encryption （ NAE ）加密的 Aggregate 上。
- 您必須已啟用 Onboard Key Manager 或外部金鑰管理程式的加密。
- 您必須執行 ONTAP 9.14.1 或更新版本。
- 若要移轉包含使用 NVE 加密的根 Volume 的 SVM 、您必須在移轉完成後、將 SVM 根 Volume 轉換為純文字 Volume 、然後重新加密 SVM 根 Volume 。
  - 如果 SVM 移轉的目的地集合體使用 NAE 、則根磁碟區預設會繼承 NAE 。
- 如果 SVM 處於 SVM 災難恢復關係中：
  - 鏡射 SVM 上的加密設定不會複製到目的地。如果您在來源或目的地上啟用 NVE 、則必須在鏡射的 SVM 根 Volume 上個別啟用 NVE 。
  - 如果目的地叢集中的所有集合體都使用 NAE 、則 SVM 根 Volume 將使用 NAE 。

步驟

您可以使用 ONTAP CLI 或系統管理員、在 SVM 根磁碟區上啟用 NVE 。

CLI

您可以在 SVM 根磁碟區就地啟用 NVE 、或是在集合體之間移動磁碟區。

將根磁碟區加密到位

1. 將根磁碟區轉換為加密磁碟區：

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. 確認加密成功。。 `volume show -encryption-type volume` 顯示使用 NVE 的所有磁碟區清單。

移動 **SVM** 根 **Volume** 來加密它

1. 啟動磁碟區移動：

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   如"指令參考資料ONTAP"需詳細 `volume move`資訊，請參閱。

2. 確認 `volume move` 操作成功 `volume move show` 命令。。 `volume show -encryption-type volume` 顯示使用 NVE 的所有磁碟區清單。

系統管理員

1. 瀏覽至 儲存空間 > 磁碟區 。
2. 在您要加密的 SVM 根 Volume 名稱旁、選取「 編輯 」。
3. 在「 儲存與最佳化 」標題下、選取「 啟用加密 」。
4. 選擇 儲存 。

在**ONTAP**節點根磁碟區上配置 **NVE**

從功能介紹9.8開始ONTAP 、您可以使用NetApp Volume Encryption來保護節點的根磁碟區。

關於這項工作

此程序適用於節點根磁碟區。不適用於SVM根磁碟區。SVM 根磁碟區可透過集合體層級加密來保護、 從 ONTAP 9.14.1 開始、 NVE。

根磁碟區加密一旦開始、就必須完成。您無法暫停作業。加密完成後、您無法將新金鑰指派給根磁碟區、也無法執行安全清除作業。

開始之前

- 您的系統必須使用HA組態。
- 您的節點根磁碟區必須已建立。
- 您的系統必須具有內建金鑰管理程式、或是使用金鑰管理互通性傳輸協定（KMIP）的外部金鑰管理伺服器。

步驟

1. 加密根磁碟區：

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. 確認轉換作業的狀態：

   ```
   volume encryption conversion show
   ```

3. 完成轉換作業後、請確認磁碟區已加密：

   ```
   volume show -fields
   ```

   以下顯示加密Volume的輸出範例。

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

設定NetApp硬體加密

了解ONTAP基於硬體的加密

NetApp硬體式加密可在寫入資料時支援完整磁碟加密（FDE）。如果沒有儲存在韌體上的加密金鑰、就無法讀取資料。而加密金鑰則只能由驗證的節點存取。

瞭解NetApp硬體型加密

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、將自己驗證到自我加密磁碟機：

- 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）為節點提供金鑰。最佳實務做法是在不同的儲存系統上設定外部金鑰管理伺服器與資料。
- 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。

您可以使用NetApp Volume Encryption搭配硬體加密、在自我加密磁碟機上「雙重加密」資料。

啟用自我加密磁碟機時、核心傾印也會加密。

> 如果HA配對使用加密SAS或NVMe磁碟機（SED、NSE、FIPS）、您必須遵循主題中的指示 將FIPS磁碟機或SED恢復為無保護模式 在初始化系統之前、HA配對內的所有磁碟機（開機選項4或9）。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

支援的自我加密磁碟機類型

支援兩種自我加密磁碟機：

- 自我加密FIPS認證SAS或NVMe磁碟機可在FAS 所有的作業系統上支援AFF 。這些磁碟機稱為_FIPS磁碟

機_、符合美國聯邦資訊處理標準出版品1402、Level 2的要求。認證的功能除了提供加密保護之外、還能防止磁碟機遭受拒絕服務攻擊。FIPS磁碟機無法與同一個節點或HA配對上的其他類型磁碟機混合使用。

- 從ONTAP 推出支援不通過FIPS測試的自我加密NVMe磁碟機開始、AFF 支援在32、320及更新版本系統上執行。這些磁碟機稱為_SED__、提供與FIPS磁碟機相同的加密功能、但可以與同一個節點或HA配對上的非加密磁碟機混合使用。
- 所有FIPS驗證的磁碟機都使用已通過FIPS驗證的韌體密碼編譯模組。 FIPS磁碟機密碼編譯模組不會使用磁碟機外部產生的任何金鑰（磁碟機的韌體密碼編譯模組會使用輸入磁碟機的驗證密碼來取得金鑰加密金鑰）。

非加密磁碟機是不是SED或FIPS磁碟機的磁碟機。

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。

何時使用外部金鑰管理

雖然使用內建金鑰管理程式的成本較低、而且通常更方便、但如果下列任一項屬實、您應該使用外部金鑰管理：

- 貴組織的原則需要使用FIPS 140-2第2級（或更高版本）密碼編譯模組的金鑰管理解決方案。
- 您需要一套多叢集解決方案、集中管理加密金鑰。
- 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。

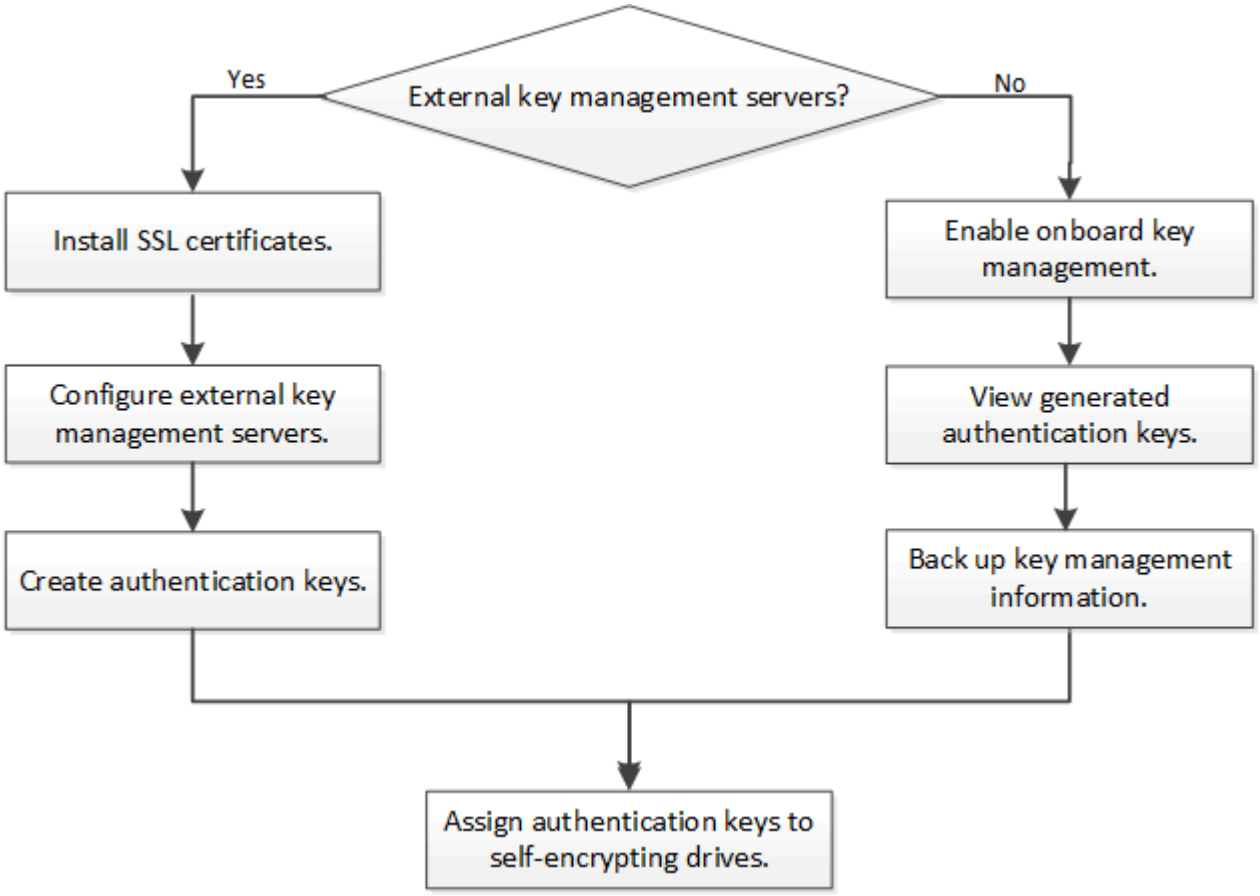
支援詳細資料

下表顯示重要的硬體加密支援詳細資料。如需支援的KMIP伺服器、儲存系統和磁碟櫃的最新資訊、請參閱互通性對照表。

資源或功能	支援詳細資料
非同質磁碟集	• FIPS磁碟機無法與同一個節點或HA配對上的其他類型磁碟機混合使用。符合的HA配對可與同一叢集中不符合要求的HA配對共存。 • SED可與同一節點或HA配對上的非加密磁碟機混合使用。
磁碟機類型	• FIPS磁碟機可以是SAS或NVMe磁碟機。 • SED必須是NVMe磁碟機。
10 Gb網路介面	KMIP金鑰管理組態從ONTAP 支援10 Gb網路介面開始、可與外部金鑰管理伺服器進行通訊。
用於與金鑰管理伺服器通訊的連接埠	從功能介紹9.3開始ONTAP 、您可以使用任何儲存控制器連接埠來與金鑰管理伺服器通訊。否則、您應該使用連接埠 e0M 與金鑰管理伺服器通訊。視儲存控制器機型而定、某些網路介面在開機程序期間可能無法用於與金鑰管理伺服器的通訊。
部分（MCC）MetroCluster	• NVMe磁碟機支援MCC。 • SAS磁碟機不支援MCC。

硬體型加密工作流程

您必須先設定金鑰管理服務、叢集才能將自己驗證到自我加密磁碟機。您可以使用外部金鑰管理伺服器或內建金鑰管理程式。



相關資訊

- "NetApp Hardware Universe"
- "NetApp Volume Encryption與NetApp Aggregate Encryption"

設定外部金鑰管理

了解如何設定**ONTAP**外部金鑰管理

您可以使用一或多個外部金鑰管理伺服器來保護叢集用來存取加密資料的金鑰。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）為節點提供金鑰。

NetApp Volume Encryption （ NVE ）可透過內建金鑰管理程式來實作。在更新版本的支援中、NVE可透過外部金鑰管理（KMIP）和內建金鑰管理程式來實作。ONTAP從 ONTAP 9.11.1 開始，您可以在叢集中設定多個外部金鑰管理員。請參閱 設定叢集式金鑰伺服器。

在**ONTAP**叢集上安裝 **SSL** 憑證

叢集與KMIP伺服器使用KMIP SSL憑證來驗證彼此的身分、並建立SSL連線。在使用KMIP伺服器設定SSL連線之前、您必須先安裝叢集的KMIP用戶端SSL憑證、以及KMIP伺服器

根憑證授權單位（CA）的SSL公開憑證。

關於這項工作

在HA配對中、兩個節點必須使用相同的公有和私有KMIP SSL憑證。如果您將多個HA配對連線至相同的KMIP伺服器、HA配對中的所有節點都必須使用相同的公有和私有KMIP SSL憑證。

開始之前

- 建立憑證、KMIP伺服器和叢集的伺服器上、必須同步時間。
- 您必須已取得叢集的公用SSL KMIP用戶端憑證。
- 您必須取得與叢集SSL KMIP用戶端憑證相關的私密金鑰。
- SSL KMIP用戶端憑證不得受密碼保護。
- 您必須已取得KMIP伺服器根憑證授權單位（CA）的SSL公開憑證。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

您可以在叢集上安裝憑證之前或之後、在KMIP伺服器上安裝用戶端和伺服器憑證。

步驟

1. 安裝叢集的SSL KMIP用戶端憑證：

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   系統會提示您輸入SSL KMIP公開和私有憑證。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. 安裝KMIP伺服器根憑證授權單位（CA）的SSL公開憑證：

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

相關資訊

- "安全性憑證安裝"

在**ONTAP 9.6** 及更高版本中啟用基於硬體的加密的外部金鑰管理

您可以使用一或多個KMIP伺服器來保護叢集用來存取加密資料的金鑰。您最多可將四個KMIP伺服器連線至一個節點。建議至少使用兩部伺服器來進行備援和災難恢復。

從 ONTAP 9.11.1 開始、每個主要金鑰伺服器最多可新增 3 個次要金鑰伺服器、以建立叢集金鑰伺服器。如需詳細資訊、請參閱 設定叢集式外部金鑰伺服器。

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- 您必須是叢集管理員才能執行此工作。

- 在MetroCluster環境中：
  - 在設定外部金鑰管理程式之前、您必須先設定MetroCluster 此解決方案。
  - 您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

步驟

1. 設定叢集的金鑰管理程式連線：

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

> ◦ 命令會 `security key-manager external enable`取代 `security key-manager setup`命令。您可以執行 `security key-manager external modify`命令來變更外部金鑰管理組態。如"指令參考資料ONTAP"需詳細 `security key-manager external enable`資訊，請參閱。
> ◦ 在支援管理SVM的環境中、如果您要設定外部金鑰管理、則必須重複執行MetroCluster `security key-manager external enable` 合作夥伴叢集上的命令。

下列命令可啟用的外部金鑰管理 `cluster1` 使用三個外部金鑰伺服器。第一個金鑰伺服器是使用其主機名稱和連接埠來指定、第二個金鑰伺服器是使用IP位址和預設連接埠來指定、第三個金鑰伺服器則是使用IPv6位址和連接埠來指定：

```
clusterl::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 確認所有已設定的KMIP伺服器均已連線：

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```

> 命令會 `security key-manager external show-status`取代 `security key-manager show -status`命令。如"指令參考資料ONTAP"需詳細 `security key-manager external show-status`資訊，請參閱。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

相關資訊

- 設定叢集式外部金鑰伺服器
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員外部顯示狀態"

在**ONTAP 9.5** 及更早版本中啟用基於硬體的加密的外部金鑰管理

您可以使用一或多個KMIP伺服器來保護叢集用來存取加密資料的金鑰。您最多可將四個KMIP伺服器連線至一個節點。建議至少使用兩部伺服器來進行備援和災難恢復。

關於這項工作

可為叢集中的所有節點設定KMIP伺服器連線。ONTAP

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- 您必須是叢集管理員才能執行此工作。
- 在設定外部金鑰管理程式之前、您必須先設定MetroCluster 此解決方案。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

步驟

1. 設定叢集節點的金鑰管理程式連線：

   ```
   security key-manager setup
   ```

   金鑰管理程式設定隨即開始。

在MetroCluster環境中，您必須在兩個叢集上執行此命令。詳細了解 `security key-manager setup`在"指令參考資料ONTAP"。

2. 在每個提示字元輸入適當的回應。
3. 新增KMIP伺服器：

   `security key-manager add -address key_management_server_ipaddress`

```
cluster1::> security key-manager add -address 20.1.1.1
```

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

4. 新增額外的KMIP伺服器以提供備援：

   `security key-manager add -address key_management_server_ipaddress`

```
cluster1::> security key-manager add -address 20.1.1.2
```

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

5. 確認所有已設定的KMIP伺服器均已連線：

   `security key-manager show -status`

   詳細了解此過程中所述的命令"指令參考資料ONTAP"。

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. 也可以將純文字磁碟區轉換為加密磁碟區。

   `volume encryption conversion start`

   在轉換磁碟區之前、必須先完整設定外部金鑰管理程式。在 MetroCluster 環境中、必須在兩個站台上設定外部金鑰管理員。

從ONTAP 9.11.1 開始，您可以在 SVM 上設定與叢集外部金鑰管理伺服器的連線。使用叢集金鑰伺服器，您可以在 SVM 上指定主金鑰伺服器和輔助金鑰伺服器。註冊或檢索金鑰時， ONTAP首先嘗試存取主密鑰伺服器，然後依序嘗試存取輔助伺服器，直到操作成功完成。

您可以使用外部金鑰伺服器來取得NetApp儲存加密 (NSE)、 NetApp磁碟區加密 (NVE) 和NetApp聚合加密 (NAE) 金鑰。一個 SVM 最多可以支援四個主外部 KMIP 伺服器。每個主伺服器最多可支援三個輔助密鑰伺服器。

關於這項工作

- 此程序僅支援使用KMIP的主要伺服器。如需支援的金鑰伺服器清單、請查看 "NetApp 互通性對照表工具"。

開始之前

- "必須為 SVM 啟用 KMIP 金鑰管理"。
- 叢集中的所有節點都必須執行ONTAP 版本不符合要求的9.11.1或更新版本。
- 伺服器的排列順序 `-secondary-key-servers`此參數反映了外部金鑰管理（KMIP）伺服器的存取順序。

建立叢集式金鑰伺服器

組態程序取決於您是否已設定主要金鑰伺服器。

將主要和次要金鑰伺服器新增至**SVM**

步驟

1. 確認叢集（admin SVM）未啟用任何金鑰管理功能：

   ```
   security key-manager external show -vserver <svm_name>
   ```

   如果 SVM 已啟用最多四個主金鑰伺服器，則必須先刪除一個現有的主金鑰伺服器，然後再新增新的主金鑰伺服器。

2. 啟用主密鑰管理器：

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - 如果您沒有在參數中指定端口， `-key-servers`如果使用參數，則預設使用連接埠 5696。

   > 如果你正在運行 `security key-manager external enable`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

3. 修改主密鑰伺服器，新增輔助密鑰伺服器。這 `-secondary-key-servers`此參數接受一個以逗號分隔的列表，最多可包含三個金鑰伺服器：

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 請勿在輔助密鑰伺服器中包含連接埠號碼。 `-secondary-key-servers`範圍。它使用與主密鑰伺服器相同的連接埠號碼。

   > 如果你正在運行 `security key-manager external`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

新增次要金鑰伺服器至現有的主要金鑰伺服器

步驟

1. 修改主密鑰伺服器，新增輔助密鑰伺服器。這 `-secondary-key-servers`此參數接受一個以逗號分隔的列表，最多可包含三個金鑰伺服器：

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 請勿在輔助密鑰伺服器中包含連接埠號碼。 `-secondary-key-servers`範圍。它使用與主密鑰伺服器相同的連接埠號碼。

如果你正在運行 `security key-manager external modify-server`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

有關輔助密鑰伺服器的更多信息，請參閱 [mod-secondary]。

修改叢集式金鑰伺服器

您可以透過新增和刪除輔助金鑰伺服器、變更輔助金鑰伺服器的存取順序或變更特定金鑰伺服器的指定（主金鑰伺服器或輔助金鑰伺服器）來修改叢集外部金鑰伺服器。如果在MetroCluster配置中修改叢集外部金鑰伺服器，NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

修改次要金鑰伺服器

使用 `security key-manager external modify-server` 指令的 `-secondary-key-servers` 參數來管理次要金鑰伺服器。這 `-secondary-key-servers` 參數接受以逗號分隔的清單。清單中輔助密鑰伺服器的指定順序決定了輔助密鑰伺服器的存取順序。您可以透過執行指令 `security key-manager external modify-server`，並以不同順序輸入次要金鑰伺服器，來修改存取順序。輔助密鑰伺服器無需提供連接埠號碼。

如果你正在運行 `security key-manager external modify-server`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。

若要移除輔助密鑰伺服器，請將要保留的密鑰伺服器新增至清單中。 `-secondary-key-servers`參數，並省略要刪除的參數。若要刪除所有輔助密鑰伺服器，請使用下列參數 `-`表示無。

轉換主要和次要金鑰伺服器

您可以使用下列步驟變更特定金鑰伺服器的指定（主金鑰伺服器或輔助金鑰伺服器）。

將主密鑰伺服器轉換為輔助密鑰伺服器

步驟

1. 從SVM中移除主密鑰伺服器：

```
security key-manager external remove-servers
```

> 如果你正在運行 `security key-manager external remove-servers`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。

2. 執行[建立叢集式金鑰伺服器]使用原主密鑰伺服器作為輔助密鑰伺服器進行此程序。

將輔助金鑰伺服器轉換為主金鑰伺服器

步驟

1. 從現有的主密鑰伺服器移除輔助密鑰伺服器：

```
security key-manager external modify-server -secondary-key-servers
```

- 如果你正在運行 `security key-manager external modify-server -secondary-key-servers`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。
- 如果在刪除現有密鑰伺服器的同時將輔助密鑰伺服器轉換為主密鑰伺服器，則在完成刪除和轉換之前嘗試新增新的密鑰伺服器可能會導緻密鑰重複。

1. 執行[建立叢集式金鑰伺服器]使用原輔助金鑰伺服器作為新叢集金鑰伺服器的主金鑰伺服器進行此程序。

請參閱[mod-secondary]了解更多。

相關資訊

- 了解更多 `security key-manager external`在"指令參考資料ONTAP"

建立**ONTAP** 驗證金鑰、請使用**32**個以上版本

您可以使用 `security key-manager key create` 命令可建立節點的驗證金鑰、並將其儲存在設定的 KMIP 伺服器上。

關於這項工作

如果您的安全性設定要求您使用不同的金鑰進行資料驗證和FIPS 140-2驗證、您應該為每個金鑰建立個別的金鑰。如果情況並非如此、您可以使用與資料存取相同的 FIPS 法規遵循驗證金鑰。

此功能可為叢集中的所有節點建立驗證金鑰。ONTAP

- 啟用Onboard Key Manager時、不支援此命令。不過、啟用Onboard Key Manager時、會自動建立兩個驗證金鑰。您可以使用下列命令來檢視金鑰：

```
security key-manager key query -key-type NSE-AK
```

- 如果設定的金鑰管理伺服器已儲存超過128個驗證金鑰、您會收到警告。
- 您可以使用 `security key-manager key delete`命令刪除任何未使用的金鑰。 `security key-manager key delete`如果指定金鑰目前正由 ONTAP 使用，則命令會失敗。（ Privileges 必須大於 `admin`才能使用此命令。）

> 在支援功能環境中、刪除金鑰之前、您必須先確定合作夥伴叢集上沒有使用金鑰MetroCluster。您可以在合作夥伴叢集上使用下列命令、檢查金鑰是否未被使用：
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 建立叢集節點的驗證金鑰：

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

> 此設定 `prompt-for-key=true`會讓系統提示叢集管理員在驗證加密磁碟機時使用複雜密碼。否則、系統會自動產生32位元組的通關密碼。命令會 `security key-manager key create`取代 `security key-manager create-key`命令。如"指令參考資料ONTAP"需詳細 `security key-manager key create`資訊，請參閱。

下列範例會建立的驗證金鑰 `cluster1`，自動產生 32 位元組的複雜密碼：

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. 確認已建立驗證金鑰：

```
security key-manager key query -node node
```

> 命令會 `security key-manager key query`取代 `security key-manager query key`命令。
>
> 輸出中顯示的金鑰ID是用來參照驗證金鑰的識別碼。它不是實際的驗證金鑰或資料加密金鑰。

下列範例會驗證是否已為建立驗證金鑰 `cluster1`：

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

相關資訊

- "儲存加密磁碟顯示"

在**ONTAP** 更新版本的版本中建立驗證金鑰

您可以使用 `security key-manager create-key` 命令可建立節點的驗證金鑰、並將其儲存在設定的 KMIP 伺服器上。

關於這項工作

如果您的安全性設定要求您使用不同的金鑰進行資料驗證和FIPS 140-2驗證、您應該為每個金鑰建立個別的金鑰。如果情況並非如此、您可以使用與資料存取相同的FIPS法規遵循驗證金鑰。

此功能可為叢集中的所有節點建立驗證金鑰。ONTAP

- 啟用內建金鑰管理時、不支援此命令。
- 如果設定的金鑰管理伺服器已儲存超過128個驗證金鑰、您會收到警告。

  您可以使用金鑰管理伺服器軟體刪除任何未使用的金鑰、然後再次執行命令。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 建立叢集節點的驗證金鑰：

   ```
   security key-manager create-key
   ```

   如"指令參考資料ONTAP"需詳細 `security key-manager create-key`資訊，請參閱。

   > 輸出中顯示的金鑰ID是用來參照驗證金鑰的識別碼。它不是實際的驗證金鑰或資料加密金鑰。

   下列範例會建立的驗證金鑰 `cluster1`：

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: <id_value>

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 確認已建立驗證金鑰：

   ```
   security key-manager query
   ```

   如"指令參考資料ONTAP"需詳細 `security key-manager query`資訊，請參閱。

   下列範例會驗證是否已為建立驗證金鑰 `cluster1`：

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

使用**ONTAP**外部金鑰管理將資料驗證金鑰指派給 **FIPS** 磁碟機或 **SED**

您可以使用 `storage encryption disk modify` 命令將資料驗證金鑰指派給 FIPS 磁碟機或 SED 。叢集節點使用此金鑰來鎖定或解除鎖定磁碟機上的加密資料。

關於這項工作

自我加密磁碟機只有在驗證金鑰ID設定為非預設值時、才會受到保護、不受未獲授權的存取。製造商安全ID（MSID）具有金鑰ID 0x0、是SAS磁碟機的標準預設值。對於NVMe磁碟機、標準預設值為null金鑰、表示為空白金鑰ID。當您將金鑰ID指派給自我加密磁碟機時、系統會將其驗證金鑰ID變更為非預設值。

此程序不會中斷營運。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 指派資料驗證金鑰給FIPS磁碟機或SED：

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   如"指令參考資料ONTAP"需詳細 `storage encryption disk modify`資訊，請參閱。

   > 您可以使用 `security key-manager query -key-type NSE-AK` 檢視金鑰ID的命令。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 確認已指派驗證金鑰：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

相關資訊

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

設定內建金鑰管理

啟用更新版本的更新版本、以利執行內建金鑰管理**ONTAP**

您可以使用Onboard Key Manager驗證FIPS磁碟機或SED的叢集節點。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。Onboard Key Manager符合FIPS-140-2第1級標準。

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用Onboard Key Manager。

關於這項工作

您必須執行 `security key-manager onboard enable` 每次將節點新增至叢集時的命令。在 MetroCluster 組態中、您必須執行 `security key-manager onboard enable` 先在本機叢集上執行 `security key-manager onboard sync` 在遠端叢集上、使用相同的複雜密碼。

詳細了解 `security key-manager onboard enable`和 `security key-manager onboard sync`在"指令參考資料ONTAP"。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。除了在 MetroCluster 中、您可以使用 `cc-`

`mode-enabled=yes` 選項要求使用者在重新開機後輸入複雜密碼。

當「內建金鑰管理程式」在「一般條件」模式中啟用時 (`cc-mode-enabled=yes`）、系統行為會以下列方式變更：

- 系統會監控在「一般準則」模式下運作時、連續嘗試失敗的叢集密碼。

  如果已啟用NetApp儲存加密（NSE）、且您在開機時未輸入正確的叢集密碼、則系統將無法驗證其磁碟機並自動重新開機。若要修正此問題、您必須在開機提示字元中輸入正確的叢集密碼。一旦開機、系統最多可連續5次嘗試在24小時內、針對任何需要叢集密碼作為參數的命令、正確輸入叢集密碼。如果達到限制（例如、您連續5次未正確輸入叢集密碼）、則必須等待24小時逾時期間、或是重新啟動節點、才能重設限制。

- 系統映像更新會使用NetApp RSA-3072程式碼簽署憑證搭配SHA-384程式碼簽署摘要、來檢查映像完整性、而非一般的NetApp RSA-2048程式碼簽署憑證和SHA-256程式碼簽署摘要。

  升級命令透過檢查各種數位簽名來驗證影像內容是否已更改或損壞。如果驗證有效，映像更新將進入下一步。如果驗證無效，則影像更新失敗。詳細了解 `cluster image`在"指令參考資料ONTAP"。

Onboard Key Manager可將金鑰儲存在揮發性記憶體中。當系統重新開機或停止時、揮發性記憶體內容會被清除。在正常操作條件下、系統停止時、揮發性記憶體內容將在30秒內清除。

開始之前

- 如果您使用NSE搭配外部金鑰管理（KMIP）伺服器、則必須刪除外部金鑰管理程式資料庫。

  "從外部金鑰管理移轉至內建金鑰管理"

- 您必須是叢集管理員才能執行此工作。
- 在設定Onboard Key Manager之前、您必須先設定MetroCluster 這個靜態環境。

步驟

1. 啟動金鑰管理程式設定命令：

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   設 `cc-mode-enabled=yes`為要求使用者在重新開機後輸入金鑰管理密碼。MetroCluster 組態不支援此 `- cc-mode-enabled`選項。命令會 `security key-manager onboard enable`取代 `security key-manager setup`命令。

   下列範例會在叢集1上啟動金鑰管理程式設定命令、而不要求在每次重新開機後輸入通關密碼：

2. 輸入一個介於 32 到 256 個字元之間的密碼，或對於“`cc-mode`”，輸入一個介於 64 到 256 個字元之間的密碼。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

3. 在通關密碼確認提示下、重新輸入通關密碼。

4. 驗證系統是否建立了身份驗證金鑰：

   ```
   security key-manager key query -node node
   ```

   命令會 `security key-manager key query`取代 `security key-manager query key`命令。

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

系統會自動將關鍵管理資訊備份到叢集的複製資料庫（RDB）。您還應該手動備份此資訊以用於災難復原。

相關資訊

- "叢集影像命令"
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員金鑰查詢"
- "安全金鑰管理員板載啟用"
- "從外部金鑰管理移轉至內建金鑰管理"

啟用更新版本的更新版本**ONTAP**

您可以使用Onboard Key Manager驗證FIPS磁碟機或SED的叢集節點。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。Onboard Key Manager符合FIPS-140-2第1級標準。

您可以使用板載金鑰管理器來保護叢集用於存取加密資料的金鑰。在存取加密磁碟區或自加密磁碟的每個叢集上啟用板載金鑰管理器。

關於這項工作

您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。

如果您使用MetroCluster 的是「不確定」組態、請參閱下列準則：

- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

密碼嘗試失敗後、您必須重新啟動節點。

開始之前

- 如果您將 NSE 與外部金鑰管理 (KMIP) 伺服器一起使用，請刪除外部金鑰管理器資料庫。

  "從外部金鑰管理移轉至內建金鑰管理"

- 您必須是叢集管理員才能執行此工作。
- 在配置板載金鑰管理器之前，請先配置MetroCluster環境。

步驟

1. 啟動金鑰管理程式設定：

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 此選項可要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。

   下列範例會在叢集1上開始設定金鑰管理程式、而不要求在每次重新開機後輸入通關密碼：

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. 輸入 `yes` 在提示下設定內建金鑰管理。
3. 在通關密碼提示字元中、輸入32到256個字元之間的通關密碼、或輸入「'cc-mode'」（64到256個字元之間的通關密碼）。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

4. 在通關密碼確認提示下、重新輸入通關密碼。
5. 驗證是否已為所有節點設定金鑰：

   ```
   security key-manager show-key-store
   ```

詳細了解 `security key-manager show-key-store`在"指令參考資料ONTAP"。

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

完成後

ONTAP會自動將金鑰管理資訊備份到叢集的複製資料庫 (RDB)。

設定板載金鑰管理器密碼後，請手動將資訊備份到儲存系統外部的安全位置。看"手動備份內建金鑰管理資訊"。

相關資訊

- "手動備份內建金鑰管理資訊"
- "安全金鑰管理程式設定"
- "安全金鑰管理員顯示金鑰庫"
- "從外部金鑰管理移轉至內建金鑰管理"

使用**ONTAP**板載金鑰管理將資料驗證金鑰指派給 **FIPS** 磁碟機或 **SED**

您可以使用 `storage encryption disk modify` 命令將資料驗證金鑰指派給 FIPS 磁碟機或 SED 。叢集節點使用此金鑰來存取磁碟機上的資料。

關於這項工作

自我加密磁碟機只有在驗證金鑰ID設定為非預設值時、才會受到保護、不受未獲授權的存取。製造商安全ID（MSID）具有金鑰ID 0x0、是SAS磁碟機的標準預設值。對於NVMe磁碟機、標準預設值為null金鑰、表示為空白金鑰ID。當您將金鑰ID指派給自我加密磁碟機時、系統會將其驗證金鑰ID變更為非預設值。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 指派資料驗證金鑰給FIPS磁碟機或SED：

   `storage encryption disk modify -disk *disk_ID* -data-key-id *key_ID*`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk modify`資訊，請參閱。

   > 您可以使用 `security key-manager key query -key-type NSE-AK` 檢視金鑰ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

2. 確認已指派驗證金鑰：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   [...]
   ```

相關資訊

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

將 FIPS 140-2 身份驗證金鑰指派給ONTAP FIPS 驅動器

您可以使用 `storage encryption disk modify` 命令 `-fips-key-id` 將 FIPS 140-2 驗證金鑰指派給 FIPS 磁碟機的選項。叢集節點將此金鑰用於資料存取以外的磁碟機作業、例如防止磁碟機遭受拒絕服務攻擊。

關於這項工作

您的安全設定可能需要使用不同的金鑰來進行資料驗證和FIPS 140-2驗證。如果情況並非如此、您可以使用與資料存取相同的FIPS法規遵循驗證金鑰。

此程序不會中斷營運。

開始之前

磁碟機韌體必須支援FIPS 140-2規範。。 "NetApp 互通性對照表工具" 包含支援磁碟機韌體版本的相關資訊。

步驟

1. 您必須先確定已指派資料驗證金鑰。您可以使用來完成這項作業 外部金鑰管理程式 或是 內建金鑰管理程式。確認已使用命令指派金鑰 `storage encryption disk show`。
2. 指派FIPS 140-2驗證金鑰給SED：

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. 確認已指派驗證金鑰：

   `storage encryption disk show -fips`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

   ```
   cluster1::> storage encryption disk show -fips
   Disk    Mode FIPS-Compliance Key ID
   ------  ----
   ------------------------------------------------------------------
   2.10.0  full <id_value>
   2.10.1  full <id_value>
   [...]
   ```

相關資訊

- "儲存加密磁碟修改"
- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

在 **ONTAP** 中啟用適用於 **KMIP** 伺服器連線的叢集範圍 **FIPS** 相容模式

您可以使用 `security config modify` 命令 `-is-fips-enabled` 選項可啟用全叢集

FIPS 相容模式、以供傳輸中的資料使用。如此會強制叢集在連接KMIP伺服器時、以FIPS模式使用OpenSSL。

關於這項工作

當您啟用全叢集FIPS相容模式時、叢集將只自動使用TLS1.2和FIPS驗證的密碼套件。預設會停用全叢集FIPS相容模式。

您必須在修改整個叢集的安全性組態之後、手動重新開機叢集節點。

開始之前

- 儲存控制器必須設定為FIPS相容模式。
- 所有KMIP伺服器都必須支援TLSv1.2。啟用叢集範圍FIPS相容模式時、系統需要TLSv1.2才能完成KMIP伺服器的連線。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 驗證是否支援TLSv1.2：

   ```
   security config show -supported-protocols
   ```

   如"指令參考資料ONTAP"需詳細 `security config show`資訊，請參閱。

   ```
   cluster1::> security config show
             Cluster                                                 Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                                !aNULL:!EXP:
                                                !eNULL
   ```

3. 啟用全叢集FIPS相容模式：

   ```
   security config modify -is-fips-enabled true -interface SSL
   ```

   如"指令參考資料ONTAP"需詳細 `security config modify`資訊，請參閱。

4. 手動重新啟動叢集節點。
5. 確認已啟用全叢集FIPS相容模式：

   ```
   security config show
   ```

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                              !aNULL:!EXP:
                                              !eNULL:!RC4
```

管理NetApp加密

取消 ONTAP 中的 Volume 資料加密

您可以使用 `volume move start` 用於移動和取消加密 Volume 資料的命令。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有的加密磁碟區、並取消加密磁碟區上的資料：

   `volume move start -vserver` *`SVM_name`* `-volume volume_name -destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume `vol1` 至目的地 Aggregate `aggr3` 並取消加密磁碟區上的資料：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   系統會刪除磁碟區的加密金鑰。磁碟區上的資料未加密。

2. 確認磁碟區已停用加密：

   `volume show -encryption`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示磁碟區是否開啟 `cluster1` 已加密：

```
cluster1::> volume show -encryption

Vserver  Volume   Aggregate   State    Encryption State
-------  ------   ---------   -----    ----------------
vs1      vol1     aggr1       online   none
```

在 **ONTAP** 中移動加密磁碟區

您可以使用 `volume move start` 用於移動加密磁碟區的命令。移動的磁碟區可以位於相同的集合體或不同的集合體上。

關於這項工作

如果目的地節點或目的地Volume不支援Volume加密、則移動將會失敗。

。 `-encrypt-destination` 的選項 `volume move start` 加密磁碟區的預設值為 true 。指定您不希望目的地 Volume 加密的要求、可確保您不會不小心將磁碟區上的資料解密。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有的加密磁碟區、並將磁碟區上的資料保持加密狀態：

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume `vol1` 至目的地 Aggregate `aggr3` 並將磁碟區上的資料加密：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. 確認磁碟區已啟用加密：

   `volume show -is-encrypted true`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
```

使用 **ONTAP** 中的 **Volume Encryption rekey start** 命令變更磁碟區的加密金鑰

定期變更磁碟區的加密金鑰是安全性最佳做法。從功能介紹9.3開始ONTAP 、您可以使用 `volume encryption rekey start` 變更加密金鑰的命令。

關於這項工作

重新輸入作業一旦開始、就必須完成。不會返回舊金鑰。如果您在作業期間遇到效能問題、可以執行 `volume encryption rekey pause` 暫停作業的命令、以及 `volume encryption rekey resume` 命令以恢復作業。

在重新輸入作業完成之前、磁碟區會有兩個按鍵。新的寫入及其對應的讀取將使用新的金鑰。否則、讀取將使用舊的金鑰。

您無法使用 `volume encryption rekey start` 重新輸入 SnapLock Volume 。

步驟

1. 變更加密金鑰：

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   下列命令會變更的加密金鑰 `vol1` 在 SVM 上`vs1`：

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. 確認重新輸入作業的狀態：

   `volume encryption rekey show`

   如"指令參考資料ONTAP"需詳細 `volume encryption rekey show`資訊，請參閱。

   下列命令會顯示重新輸入作業的狀態：

   ```
   cluster1::> volume encryption rekey show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 重新輸入作業完成後、請確認磁碟區已啟用加密功能：

   `volume show -is-encrypted true`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

   下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate   State   Type   Size   Available   Used
-------   ------   ---------   -----   ----   -----   ---------  ----
vs1       vol1     aggr2      online     RW   200GB     160.0GB   20%
```

使用**ONTAP**磁碟區移動啟動指令變更磁碟區的加密金鑰

定期變更磁碟區的加密金鑰是安全性最佳做法。您可以使用 `volume move start`命令來變更加密金鑰。移動的磁碟區可以位於相同的集合體或不同的集合體上。

關於這項工作

您無法使用 `volume move start` 重新輸入 SnapLock 或 FlexGroup 磁碟區。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有磁碟區並變更加密金鑰：

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume **`vol1`** 至目的地 Aggregate **`aggr2`** 並變更加密金鑰：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

   系統會為磁碟區建立新的加密金鑰。磁碟區上的資料仍保持加密狀態。

2. 確認磁碟區已啟用加密：

   `volume show -is-encrypted true`

   如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate    State   Type   Size  Available  Used
-------   ------   ---------    -----   ----   -----  ---------  ----
vs1       vol1     aggr2      online     RW   200GB     160.0GB  20%
```

輪換ONTAP NetApp儲存加密的驗證金鑰

使用NetApp儲存加密（NSE）時、您可以旋轉驗證金鑰。

關於這項工作

如果您使用外部金鑰管理程式（KMIP）、則可支援NSE環境中的旋轉驗證金鑰。

Onboard Key Manager（OKM）不支援NSE環境中的旋轉驗證金鑰。

步驟

1. 使用 `security key-manager create-key` 產生新驗證金鑰的命令。

   您必須先產生新的驗證金鑰、才能變更驗證金鑰。

2. 使用 `storage encryption disk modify -disk * -data-key-id` 變更驗證金鑰的命令。

相關資訊

- "儲存加密磁碟修改"

刪除 ONTAP 中的加密磁碟區

您可以使用 `volume delete` 刪除加密磁碟區的命令。

開始之前

- 您必須是叢集管理員才能執行此工作。
- Volume必須離線。

步驟

1. 刪除加密磁碟區：

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   如"指令參考資料ONTAP"需詳細 `volume delete`資訊，請參閱。

   下列命令會刪除名為的加密磁碟區 `vol1`：

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

輸入 `yes` 當系統提示您確認刪除時。

系統會在24小時後刪除磁碟區的加密金鑰。

與選項搭配 `-force true`使用 `volume delete`，可立即刪除磁碟區並銷毀對應的加密金鑰。此命令需要進階權限。如"指令參考資料ONTAP"需詳細 `volume delete`資訊，請參閱。

完成後

您可以使用 `volume recovery-queue` 發出後在保留期間內恢復已刪除磁碟區的命令 `volume delete` 命令：

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"如何使用Volume Recovery功能"

安全地清除加密磁碟區上的資料

了解如何安全地從加密**ONTAP**磁碟區中清除數據

從支援NVE的磁碟區開始、您可以使用安全清除功能、在不中斷營運的情況下清除資料。ONTAP加密磁碟區上的資料清理功能可確保資料無法從實體媒體中恢復、例如在「資源回收」的情況下、資料追蹤可能會在區塊遭到覆寫時留下、或是安全地刪除租戶的資料。

安全清除僅適用於已啟用NVE的磁碟區上先前刪除的檔案。您無法清理未加密的Volume。您必須使用KMIP伺服器來提供金鑰、而非內建金鑰管理程式。

使用安全清除的考量事項

- 在啟用NetApp Aggregate Encryption（NAE）的Aggregate中建立的磁碟區不支援安全清除。
- 安全清除僅適用於已啟用NVE的磁碟區上先前刪除的檔案。
- 您無法清理未加密的Volume。
- 您必須使用KMIP伺服器來提供金鑰、而非內建金鑰管理程式。

視ONTAP 您的版本而定、安全清除功能會有所不同。

更新版本**ONTAP**

- 支援安全清除MetroCluster 功能的不受支援。FlexGroup
- 如果要清除的磁碟區是SnapMirror關係的來源、您就不需要中斷SnapMirror關係、就能執行安全的清除。
- 對於使用SnapMirror資料保護的磁碟區而言、重新加密方法不同於未使用SnapMirror資料保護（DP）或使用SnapMirror延伸資料保護的磁碟區。
  - 根據預設、使用SnapMirror資料保護（DP）模式的磁碟區會使用Volume Move Re-Encryption方法重新加密資料。
  - 根據預設、未使用SnapMirror資料保護的磁碟區或使用SnapMirror延伸資料保護（XDP）模式的磁碟區、會使用就地重新加密方法。
  - 您可以使用變更這些預設值 `secure purge re-encryption-method [volume-move|in-place-rekey]` 命令。
- 根據預設， FlexVol 磁碟區中的所有快照都會在安全清除作業期間自動刪除。根據預設、FlexGroup 在安全清除作業期間、不會自動刪除使用SnapMirror資料保護的所有SnapMirror Volume和Snapshot快照。您可以使用命令變更這些預設值 `secure purge delete-all-snapshots [true|false]`。

更新版本：**ONTAP**

- 安全清除不支援下列項目：
  - FlexClone
  - SnapVault
  - FabricPool
- 如果要清除的磁碟區是SnapMirror關係的來源、您必須先中斷SnapMirror關係、才能清除該磁碟區。

  如果磁碟區中有忙碌的快照，您必須先釋放快照，才能清除磁碟區。例如、您可能需要從其父磁碟區分割FlexClone磁碟區。
- 成功叫用安全清除功能會觸發磁碟區移動、以新金鑰重新加密其餘未清除的資料。

  移動的磁碟區會保留在目前的Aggregate上。舊金鑰會自動銷毀、確保清除的資料無法從儲存媒體中恢復。

從沒有**SnapMirror**關係的加密**ONTAP**磁碟區中清理數據

從使用支援NVE的磁碟區開始、您可以使用安全清除功能、在不中斷營運的「crub」資料中進行安全清除。ONTAP

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

步驟

1. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
2. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

3. 如果您要安全清除的檔案位於快照中、請刪除快照：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. 安全地清除刪除的檔案：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   下列命令可安全地清除上刪除的檔案 `vol1` 在 SVM 上`vs1`：

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. 驗證安全清除作業的狀態：

   ```
   volume encryption secure-purge show
   ```

從具有**SnapMirror**非同步關係的加密**ONTAP**磁碟區中清理數據

從 ONTAP 9 8 開始、您可以在具有 SnapMirror 非同步關係且啟用 NVE 的磁碟區上、使用安全清除功能、以不中斷營運的「 crub 」資料。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

步驟

1. 在儲存系統上、切換至進階權限層級：

   ```
   set -privilege advanced
   ```

2. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
3. 在非同步關係中準備好要安全清除的目的地Volume：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   在 SnapMirror 非同步關係中的每個磁碟區上重複此步驟。

4. 如果您要安全清除的檔案位於快照中、請刪除快照：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. 如果您要安全清除的檔案位於基礎快照中，請執行下列步驟：
   a. 在 SnapMirror 非同步關係中的目的地磁碟區上建立快照：

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. 更新 SnapMirror 以向前移動基礎快照：

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   對 SnapMirror 非同步關係中的每個 Volume 重複此步驟。

   a. 重複步驟（a）和（b），等於基礎快照的數量加上 1 。

      例如，如果您有兩個基礎快照，則應重複步驟（a）和（b）三次。

   b. 確認基礎快照存在：
      `snapshot show -vserver SVM_name -volume volume_name`
   c. 刪除基礎快照：
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`
6. 安全地清除刪除的檔案：

   ```
   volume encryption secure-purge start -vserver svm_name -volume volume_name
   ```

在 SnapMirror 非同步關係中的每個磁碟區上重複此步驟。

下列命令可安全清除SVM「'VS1'」上「'vol1'」上的刪除檔案：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. 確認安全清除作業的狀態：

   ```
   volume encryption secure-purge show
   ```

相關資訊

- "SnapMirror 更新"

從具有**SnapMirror**同步關係的加密**ONTAP**磁碟區中清理數據

從 ONTAP 9 8 開始、您可以使用安全清除功能、在具有 SnapMirror 同步關係的 NVE 磁碟區上、不中斷地「清理」資料。

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

> 若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

步驟

1. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
3. 在非同步關係中準備好要安全清除的目的地Volume：

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   針對 SnapMirror 同步關係中的其他磁碟區重複此步驟。

4. 如果您要安全清除的檔案位於快照中、請刪除快照：

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

5. 如果安全清除檔案位於基礎快照或一般快照中，請更新 SnapMirror 以將一般快照向前移：

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   共有兩個常用快照，因此必須發出兩次此命令。

6. 如果安全清除檔案位於應用程式一致的快照中，請刪除 SnapMirror 同步關係中兩個磁碟區上的快照：

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   在兩個磁碟區上執行此步驟。

7. 安全地清除刪除的檔案：

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   在 SnapMirror 同步關係中的每個磁碟區上重複此步驟。

   下列命令可安全清除SVM「'VS1'」上「'vol1'」上的刪除檔案。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. 確認安全清除作業的狀態：

   ```
   volume encryption secure-purge show
   ```

相關資訊

- "SnapMirror 更新"

更改ONTAP板載密鑰管理密碼

NetApp建議您定期變更板載金鑰管理密碼。您必須將新密碼短語儲存在儲存系統之外的安全位置。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 此工作需要進階權限。
- 在MetroCluster環境中，在本地叢集上更新密碼短語後，同步夥伴叢集上的密碼短語更新。

步驟

1. 變更為進階權限層級：

```
set -privilege advanced
```

2. 更改機載密鑰管理密碼。您使用的命令取決於您執行的ONTAP版本。

   更新版本**ONTAP**

   ```
   security key-manager onboard update-passphrase
   ```

   不含更新版本**ONTAP**

   ```
   security key-manager update-passphrase
   ```

3. 輸入一個介於 32 到 256 個字元之間的密碼，或對於“cc-mode”，輸入一個介於 64 到 256 個字元之間的密碼。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

4. 在通關密碼確認提示下、重新輸入通關密碼。

5. 如果您使用的是MetroCluster配置，請在夥伴叢集上同步更新後的密碼短語。

   a. 透過選擇適合您ONTAP版本的正確指令，在夥伴叢集上同步密碼短語：

      更新版本**ONTAP**

      ```
      security key-manager onboard sync
      ```

      不含更新版本**ONTAP**

      - 在ONTAP 9.5 中，運行：

        ```
        security key-manager setup -sync-metrocluster-config
        ```

      - 在ONTAP 9.4 及更早版本中，更新本機叢集上的密碼短語後，等待 20 秒，然後在夥伴叢集上執行以下命令：

        ```
        security key-manager setup
        ```

   b. 出現提示時，請輸入新的密碼短語。

      兩個群集必須使用相同的密碼短語。

完成後

將板載金鑰管理密碼短語複製到儲存系統外部的安全位置，以備將來使用。

每次變更機載金鑰管理密碼時，請手動備份金鑰管理資訊。

相關資訊

- "手動備份內建金鑰管理資訊"
- "安全金鑰管理程式內建更新密碼"

設定Onboard Key Manager複雜密碼時、您應該將內建金鑰管理資訊複製到儲存系統外部的安全位置。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

關於這項工作

所有的金鑰管理資訊都會自動備份到叢集的複寫資料庫（RDB）。您也應該手動備份金鑰管理資訊、以便在發生災難時使用。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 顯示叢集的金鑰管理備份資訊：

此版本... ONTAP	使用此命令...
更新版本ONTAP	`security key-manager onboard show-backup`
不含更新版本ONTAP	`security key-manager backup show`

   以下 9.6 指令顯示金鑰管理備份訊息 `cluster1` ：

```
cluster1::> security key-manager onboard show-backup

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```


3. 將備份資訊複製到儲存系統以外的安全位置、以便在發生災難時使用。

相關資訊

- "安全金鑰管理程式內建show Backup"
- "安全金鑰管理程式的備份展示"

在 ONTAP 中還原內建金鑰管理加密金鑰

有時，您可能需要恢復板載金鑰管理加密金鑰。確認需要恢復密鑰後，您可以設定板載密鑰管理器來恢復密鑰。恢復板載金鑰管理加密金鑰所遵循的步驟因ONTAP版本的不同而不同。

開始之前

- 如果您將 NSE 與外部 KMIP 伺服器一起使用，請刪除外部金鑰管理員資料庫。有關詳細信息，請參閱"從外部金鑰管理過渡到ONTAP板載金鑰管理"。
- 您必須是叢集管理員才能執行此工作。

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。

更新版本**ONTAP**

如果您執行的是 ONTAP 9.8 或更新版本、而且根磁碟區已加密、請遵循的程序 [ontap-9-8]。

1. 確認金鑰需要還原：
   `security key-manager key query -node node`

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

2. 還原金鑰：
   `security key-manager onboard sync`

   如"指令參考資料ONTAP"需詳細 `security key-manager onboard sync`資訊，請參閱。

3. 在通關密碼提示字元下、輸入叢集的內建金鑰管理通關密碼。

ONTAP 9.8 或更新版本、含加密的根磁碟區

如果您執行ONTAP 的是更新版本的版本、而且根磁碟區已加密、則必須使用開機功能表設定內建金鑰管理還原密碼。如果您要更換開機媒體、也必須執行此程序。

1. 將節點開機至開機功能表、然後選取選項 `(10) Set onboard key management recovery secrets`。
2. 輸入 `y` 以使用此選項。
3. 出現提示時、輸入叢集的內建金鑰管理通關密碼。
4. 出現提示時、輸入備份金鑰資料。

   輸入備份金鑰資料後，節點返回啟動選單。

5. 從開機功能表中、選取選項 `(1) Normal Boot`。

不含更新版本**ONTAP**

1. 確認金鑰需要還原：
   `security key-manager key show`
2. 還原金鑰：
   `security key-manager setup -node node`

   詳細了解 `security key-manager setup`在"指令參考資料ONTAP"。

3. 在通關密碼提示字元下、輸入叢集的內建金鑰管理通關密碼。

恢復**ONTAP**外部金鑰管理加密金鑰

您可以手動還原外部金鑰管理加密金鑰、並將其推送到不同的節點。如果您重新啟動的節點在建立叢集的金鑰時暫時停機、您可能會想要這麼做。

關於這項工作

在 ONTAP 9.6 及更新版本中、您可以使用 `security key-manager key query -node node_name` 命令以驗證金鑰是否需要還原。

在 ONTAP 9.5 或更早版本中、您可以使用 `security key-manager key show` 命令以驗證金鑰是否需要還原。

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。

如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 如果您執行ONTAP 的是更新版本的版本、且根磁碟區已加密、請執行下列步驟：

   如果您執行ONTAP 的是更新版本的版本、或是執行ONTAP 的是版本不加密的版本、請跳過此步驟。

   a. 設定 bootargs ：

      ```
      setenv kmip.init.ipaddr <ip-address>

      setenv kmip.init.netmask <netmask>

      setenv kmip.init.gateway <gateway>

      setenv kmip.init.interface e0M

      boot_ontap
      ```

   b. 將節點開機至開機功能表、然後選取選項 `(11) Configure node for external key management`。

   c. 依照提示輸入管理憑證。

      輸入所有管理憑證資訊後、系統會返回開機功能表。

   d. 從開機功能表中、選取選項 `(1) Normal Boot`。

2. 還原金鑰：

此版本… ONTAP	使用此命令…

更新版本ONTAP	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	不含更新版本ONTAP

`node`預設為所有節點。

啟用內建金鑰管理時、不支援此命令。

下列 ONTAP 9.6 命令可將外部金鑰管理驗證金鑰還原至中的所有節點 `cluster1`：

```
clusterl::> security key-manager external restore
```

相關資訊

- "安全金鑰管理程式外部還原"

替換**ONTAP**叢集上的 **KMIP SSL** 憑證

所有SSL憑證都有到期日。您必須在憑證過期之前更新憑證、以避免喪失驗證金鑰的存取權。

開始之前

- 您必須已取得叢集的替代公開憑證和私密金鑰（KMIP用戶端憑證）。
- 您必須已取得KMIP伺服器（KMIP伺服器- CA憑證）的替代公共憑證。
- 您必須是叢集或SVM管理員、才能執行此工作。
- 如果您要在 MetroCluster 環境中更換 KMIP SSL 憑證、則必須在兩個叢集上安裝相同的置換 KMIP SSL 憑證。

您可以在叢集上安裝憑證之前或之後、在KMIP伺服器上安裝替換用戶端和伺服器憑證。

步驟

1. 安裝新的KMIP伺服器CA憑證：

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. 安裝新的KMIP用戶端憑證：

   ```
   security certificate install -type client -vserver <>
   ```

3. 更新金鑰管理程式組態以使用新安裝的憑證：

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   如果您在ONTAP 支援支援功能的環境中執行的是支援支援功能的版本9.6或更新版本MetroCluster 、而您想

要修改管理SVM上的金鑰管理程式組態、則必須在組態中的兩個叢集上執行命令。

如果新用戶端憑證的公鑰/私鑰與先前安裝的金鑰不同，則更新金鑰管理器設定以使用新安裝的憑證將傳回錯誤。查看"NetApp知識庫：新的用戶端憑證公鑰或私鑰與現有用戶端憑證不同"有關如何覆寫此錯誤的說明。

相關資訊

- "安全性憑證安裝"
- "安全金鑰管理程式外部修改"

更換 ONTAP 中的 FIPS 磁碟機或 SED

更換FIPS磁碟機或SED的方式與更換一般磁碟相同。請務必將新的資料驗證金鑰指派給更換的磁碟機。對於FIPS磁碟機、您可能也想指派新的FIPS 140-2驗證金鑰。

如果HA配對正在使用 "加密SAS或NVMe磁碟機（SED、NSE、FIPS）"、您必須遵循主題中的指示 "將FIPS磁碟機或SED恢復為無保護模式" 在初始化系統之前、HA配對內的所有磁碟機（開機選項4或9）。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

開始之前

- 您必須知道磁碟機使用的驗證金鑰金鑰ID。
- 您必須是叢集管理員才能執行此工作。

步驟

1. 確定磁碟已標示為故障：

   ```
   storage disk show -broken
   ```

   如"指令參考資料ONTAP"需詳細 `storage disk show`資訊，請參閱。

   ```
   cluster1::> storage disk show -broken
   Original Owner: cluster1-01
     Checksum Compatibility: block
                                                                      Usable
   Physical
       Disk   Outage Reason HA Shelf Bay Chan   Pool   Type    RPM     Size
   Size
       ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
   -------
       0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
   133.9GB
       0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
   134.2GB
   [...]
   ```

2. 請依照磁碟櫃模型硬體指南中的指示、移除故障磁碟、並以新的FIPS磁碟機或SED進行更換。
3. 指派新更換磁碟的擁有權：

   ```
   storage disk assign -disk disk_name -owner node
   ```

   如"指令參考資料ONTAP"需詳細 `storage disk assign`資訊，請參閱。

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. 確認已指派新磁碟：

   ```
   storage encryption disk show
   ```

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.0  data <id_value>
   1.10.1  data <id_value>
   2.1.1   open 0x0
   [...]
   ```

5. 將資料驗證金鑰指派給FIPS磁碟機或SED。

   "指派資料驗證金鑰給FIPS磁碟機或SED（外部金鑰管理）"

6. 如有必要、請指派FIPS 140-2驗證金鑰給FIPS磁碟機。

   "將FIPS 140-2驗證金鑰指派給FIPS磁碟機"

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"
- "儲存加密磁碟顯示"

使**FIPS**磁碟機或**SED**上的資料無法存取

了解如何使 **FIPS** 驅動器或 **SED** 上的**ONTAP**資料無法存取

如果您想要使FIPS磁碟機或SED上的資料永久無法存取、但要保留磁碟機未使用的空間以供新資料使用、您可以清理磁碟。如果您想要永久無法存取資料、而且不需要重複使用磁

碟機、可以將其銷毀。

- 磁碟資料抹除

  當您清理自我加密磁碟機時、系統會將磁碟加密金鑰變更為新的隨機值、將開機鎖定狀態重設為假、並將金鑰ID設為預設值、例如製造商安全ID 0x0（SAS磁碟機）或null金鑰（NVMe磁碟機）。這樣做會使磁碟上的資料無法存取、而且無法擷取。您可以將已消毒的磁碟重複使用為非零備援磁碟。

- 磁碟銷毀

  當您銷毀FIPS磁碟機或SED時、系統會將磁碟加密金鑰設為未知的隨機值、並以不可扭轉的方式鎖定磁碟。這樣做會使磁碟永遠無法使用、且上的資料永遠無法存取。

您可以清除或銷毀個別自我加密磁碟機、或是節點的所有自我加密磁碟機。

在 **ONTAP** 中清理 **FIPS** 磁碟機或 **SED**

如果您想讓 FIPS 磁碟機或 SED 上的資料永遠無法存取、並將磁碟機用於新資料、您可以使用 `storage encryption disk sanitize` 用於清理磁碟機的命令。

關於這項工作

當您清理自我加密磁碟機時、系統會將磁碟加密金鑰變更為新的隨機值、將開機鎖定狀態重設為假、並將金鑰ID設為預設值、例如製造商安全ID 0x0（SAS磁碟機）或null金鑰（NVMe磁碟機）。這樣做會使磁碟上的資料無法存取、而且無法擷取。您可以將已消毒的磁碟重複使用為非零備援磁碟。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將任何需要保留的資料移轉到另一個磁碟上的集合體。
2. 刪除FIPS磁碟機或SED上要消毒的Aggregate：

   ```
   storage aggregate delete -aggregate aggregate_name
   ```

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   如"指令參考資料ONTAP"需詳細 `storage aggregate delete`資訊，請參閱。

3. 識別要消毒的FIPS磁碟機或SED的磁碟ID：

   ```
   storage encryption disk show -fields data-key-id,fips-key-id,owner
   ```

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.2  data <id_value>
[...]
```

4. 如果FIPS磁碟機以FIPS相容模式執行、請將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. 為磁碟機消毒：

   `storage encryption disk sanitize -disk disk_id`

   您只能使用此命令來清除熱備援磁碟或中斷的磁碟。若要清理所有磁碟，無論其類型為何，請使用 `-force-all-state`選項。如"指令參考資料ONTAP"需詳細 `storage encryption disk sanitize`資訊，請參閱。

   ⓘ ONTAP 會提示您輸入確認片語、然後再繼續。輸入完全如畫面所示的詞彙。

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. 解除清理磁碟故障：
   `storage disk unfail -spare true -disk disk_id`
7. 檢查磁碟是否擁有擁有者：
   `storage disk show -disk disk_id`

如果磁碟沒有擁有者、請指派一個擁有者。
`storage disk assign -owner node -disk disk_id`

8. 輸入要清理磁碟的節點節點節點的節點節點節點：

   `system node run -node node_name`

   執行 `disk sanitize release` 命令。

9. 離開 nodesdroand 。再次解除磁碟故障：
   `storage disk unfail -spare true -disk disk_id`
10. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用：
    `storage disk show -disk disk_id`

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"
- "儲存磁碟未故障"
- "儲存加密磁碟修改"
- "儲存加密磁碟清理"
- "儲存加密磁碟顯示狀態"

在 **ONTAP** 中銷毀 **FIPS** 磁碟機或 **SED**

如果您想讓 FIPS 磁碟機或 SED 上的資料永遠無法存取、而且不需要重複使用磁碟機、您可以使用 `storage encryption disk destroy` 破壞磁碟的命令。

關於這項工作

當您銷毀FIPS磁碟機或SED時、系統會將磁碟加密金鑰設為未知的隨機值、並以不可扭轉的方式鎖定磁碟機。這樣做會使磁碟幾乎無法使用、且上的資料永遠無法存取。不過、您可以使用印在磁碟標籤上的實體安全ID（PSID）、將磁碟重設為原廠設定的設定。如需詳細資訊、請參閱 "當驗證金鑰遺失時、將FIPS磁碟機或SED恢復服務"。

除非您擁有不可傳的Disk Plus服務（NRD Plus）、否則請勿銷毀FIPS磁碟機或SED。銷毀磁碟會使其保固失效。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將任何需要保留的資料移轉到另一個不同磁碟上的集合體。
2. 刪除FIPS磁碟機或SED上要銷毀的Aggregate：

   `storage aggregate delete -aggregate aggregate_name`

```
cluster1::> storage aggregate delete -aggregate aggr1
```

如"指令參考資料ONTAP"需詳細 `storage aggregate delete`資訊，請參閱。

3. 識別要銷毀的FIPS磁碟機或SED的磁碟ID：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.2  data <id_value>
[...]
```

4. 銷毀磁碟：

   `storage encryption disk destroy -disk disk_id`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk destroy`資訊，請參閱。

   系統會提示您輸入確認短句、然後再繼續。輸入完全如畫面所示的詞彙。

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

相關資訊

- "儲存加密磁碟銷毀"

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

ONTAP 中的 **FIPS** 磁碟機或 **SED** 上的緊急資料會被粉碎

發生安全性緊急情況時、即使儲存系統或KMIP伺服器無法使用電源、您仍可立即防止存取FIPS磁碟機或SED。

開始之前

- 如果您使用的KMIP伺服器沒有可用的電源、則KMIP伺服器必須設定容易銷毀的驗證項目（例如智慧卡或USB磁碟機）。
- 您必須是叢集管理員才能執行此工作。

步驟

1. 緊急銷毀FIPS磁碟機或SED上的資料：

如果…	然後…

儲存系統可提供電力、您也有時間讓儲存系統正常離線	a. 如果儲存系統設定為HA配對、請停用接管功能。
	b. 使所有集合體離線並加以刪除。
	c. 將權限層級設為進階：
	`set -privilege advanced`
	d. 如果磁碟機處於FIPS相容模式、請將節點的FIPS驗證金鑰ID設回預設MSID：
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. 停止儲存系統。
	f. 開機進入維護模式。
	g. 清理或銷毀磁碟：
	◦ 如果您想讓磁碟上的資料無法存取、但仍能重複使用磁碟、請清理磁碟：
	`disk encrypt sanitize -all`
	◦ 如果您想讓磁碟上的資料無法存取、而且不需要儲存磁碟、請銷毀磁碟：
	`disk encrypt destroy disk_id1 disk_id2 …`
	ⓘ ◦ `disk encrypt sanitize` 和 `disk encrypt destroy` 命令僅保留用於維護模式。這些命令必須在每個HA節點上執行、而且無法用於中斷的磁碟。
	h. 針對合作夥伴節點重複這些步驟。
	如此一來、儲存系統就會處於永久停用狀態、並清除所有資料。若要再次使用系統、您必須重新設定。
		儲存系統可提供電力、您必須立即切斷資料

a. 如果您想要使磁碟上的資料無法存取且仍能重複使用磁碟、請清理磁碟：
b. 如果儲存系統設定為HA配對、請停用接管功能。
c. 將權限層級設為進階：
`set -privilege advanced`
d. 如果磁碟機處於FIPS相容模式、請將節點的FIPS驗證金鑰ID設回預設MSID：
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. 清理磁碟：
`storage encryption disk sanitize -disk * -force-all-states true`
	a. 如果您想要使磁碟上的資料無法存取、而且不需要儲存磁碟、請銷毀磁碟：
	b. 如果儲存系統設定為HA配對、請停用接管功能。
	c. 將權限層級設為進階：
	`set -privilege advanced`
	d. 銷毀磁碟：
	`storage encryption disk destroy -disk * -force-all-states true`
		儲存系統會出現問題、使系統處於永久停用狀態、並清除所有資料。若要再次使用系統、您必須重新設定。

KMIP伺服器可供電、但儲存系統無法供電	a. 登入 KMIP 伺服器。 b. 銷毀與FIPS磁碟機或SED相關的所有金鑰、這些金鑰包含您要防止存取的資料。 如此可防止儲存系統存取磁碟加密金鑰。	KMIP伺服器或儲存系統無法使用電源

相關資訊

- "儲存加密磁碟銷毀"
- "儲存加密磁碟修改"
- "儲存加密磁碟清理"

當**ONTAP**中的驗證金鑰遺失時，將 **FIPS** 磁碟機或 **SED** 還原服務

如果您永久遺失FIPS磁碟機或SED的驗證金鑰、而且無法從KMIP伺服器擷取、系統會將其視為中斷。雖然您無法存取或恢復磁碟上的資料、但您可以採取步驟、讓SED的未使用空間再次可供資料使用。

開始之前

您必須是叢集管理員才能執行此工作。

關於這項工作

只有當您確定FIPS磁碟機或SED的驗證金鑰已永久遺失、而且無法還原時、才應使用此程序。

如果磁碟已分割、則必須先取消磁碟分割、才能開始此程序。

取消磁碟分割的命令僅在診斷層級可用，且只能在NetApp支援監督下執行。強烈建議您在繼續操作之前聯繫**NetApp**支援。 您也可以參考"NetApp知識庫：如何在ONTAP中取消對備用磁碟機的分割區"。

步驟

1. 將FIPS磁碟機或SED送回服務：

如果SED是…	請使用下列步驟…

未處於FIPS相容模式、或處於FIPS相容模式、且FIPS金鑰可供使用	a. 將權限層級設為進階：
	`set -privilege advanced`
	b. 將 FIPS 金鑰重設為預設製造安全 ID 0x0 ：
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 確認作業成功：
	`storage encryption disk show-status`
	如果作業失敗、請使用本主題中的 PSID 程序。
	d. 清理損壞的磁碟：
	`storage encryption disk sanitize -disk disk_id`
	使用命令驗證作業是否成功 `storage encryption disk show-status` 繼續下一步之前。
	e. 解除清理磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	f. 檢查磁碟是否擁有擁有者：
	`storage disk show -disk disk_id`
	如果磁碟沒有擁有者、請指派一個擁有者。
	`storage disk assign -owner node -disk disk_id`
	i. 輸入要清理磁碟的節點節點節點的節點節點節點：
	`system node run -node node_name`
	執行 `disk sanitize release` 命令。
	g. 離開 nodesdroand 。再次解除磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	h. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用：
	`storage disk show -disk disk_id`

在FIPS相容模式中、FIPS金鑰無法使用、且SED標籤上印有PSID	a. 從磁碟標籤取得磁碟的PSID。
	b. 將權限層級設為進階：
	`set -privilege advanced`
	c. 將磁碟重設為原廠設定的設定：
	`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`
	使用命令驗證作業是否成功 `storage encryption disk show-status` 繼續下一步之前。
	d. 如果您執行的是 ONTAP 9.8P5 或更早版本、請跳至下一步。如果您執行的是 ONTAP 9.8P6 或更新版本、請將已清理的磁碟恢復故障。
	`storage disk unfail -disk disk_id`
	e. 檢查磁碟是否擁有擁有者：
	`storage disk show -disk disk_id`
	如果磁碟沒有擁有者、請指派一個擁有者。
	`storage disk assign -owner node -disk disk_id`
	i. 輸入要清理磁碟的節點節點節點的節點節點節點：
	`system node run -node node_name`
	執行 `disk sanitize release` 命令。
	f. 離開 nodesdroe ..再次解除磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	g. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用：
	`storage disk show -disk disk_id`

相關資訊

- "儲存加密磁碟修改"
- "儲存加密磁碟恢復到原始狀態"
- "儲存加密磁碟清理"
- "儲存加密磁碟顯示狀態"

在**ONTAP**中將 **FIPS** 驅動器或 **SED** 恢復為不受保護的模式

僅當節點的驗證金鑰ID設為預設值以外的值時、FIPS磁碟機或SED才會受到保護、不受未獲授權的存取。您可以使用命令將金鑰 ID 設為預設值，將 FIPS 磁碟機或 SED 恢復為未受保護模式 `storage encryption disk modify`。未受保護模式下的 FIPS 磁碟機或 SED 使用預設加密金鑰，而受保護模式下的 FIPS 磁碟機或 SED 則使用提供的加密金鑰。如果磁碟機上有加密資料，而且磁碟機重設為未受保護模式，則資料仍會加密，不會公開。

按照此程序確保 FIPS 驅動器或 SED 返回到不受保護的模式後任何加密資料都變得無法存取。一旦重置 FIPS 和資料金鑰 ID，任何現有資料都無法解密，且無法訪問，除非恢復原始金鑰。

如果HA配對使用加密SAS或NVMe磁碟機（SED、NSE、FIPS）、則在初始化系統之前、您必須針對HA配對內的所有磁碟機（開機選項4或9）執行此程序。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 如果FIPS磁碟機以FIPS相容模式執行、請將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   使用以下命令確認作業成功：

   ```
   storage encryption disk show-status
   ```

   重複 show-status 指令，直到「Disks Begun」和「Disks Done」中的數字相同。

   ```
   cluster1:: storage encryption disk show-status

              FIPS    Latest   Start               Execution   Disks
   Disks Disks
   Node       Support Request  Timestamp           Time (sec)  Begun
   Done  Successful
   -------    ------- -------- ------------------  ---------- ------
   ------  ----------
   cluster1   true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. 將節點的資料驗證金鑰ID設回預設的MSID 0x0：

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   的價值 `-data-key-id` 無論您要將 SAS 或 NVMe 磁碟機恢復為未受保護模式、都應該設定為 0x0 。

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   使用以下命令確認作業成功：

   `storage encryption disk show-status`

   重複 show-status 指令，直到數字相同。當“disks began”和“disks done”中的數字相同時，操作完成。

維護模式

從支援功能9.7開始ONTAP 、您可以從維護模式重新輸入FIPS磁碟機的金鑰。只有在ONTAP 無法使用上一節中的指令時、才應使用維護模式。

步驟

1. 將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

   `disk encrypt rekey_fips 0x0 disklist`

2. 將節點的資料驗證金鑰ID設回預設的MSID 0x0：

   `disk encrypt rekey 0x0 disklist`

3. 確認FIPS驗證金鑰已成功重新輸入：

   `disk encrypt show_fips`

4. 確認資料驗證金鑰已成功重新輸入：

   `disk encrypt show`

   您的輸出可能會顯示預設的MSID 0x0金鑰ID或金鑰伺服器所保留的64個字元值。。 `Locked?` 欄位是指資料鎖定。

```
Disk        FIPS Key ID                  Locked?
----------- ---------------------------- -------
0a.01.0     0x0                           Yes
```

相關資訊

- "儲存加密磁碟修改"
- "儲存加密磁碟顯示狀態"

移除 **ONTAP** 中的外部金鑰管理程式連線

當不再需要服務器時、您可以從節點中斷KMIP伺服器的連線。例如、當您轉換至Volume加密時、可能會中斷KMIP伺服器的連線。

關於這項工作

當您中斷KMIP伺服器與HA配對中某個節點的連線時、系統會自動中斷伺服器與所有叢集節點的連線。

> 如果您打算在中斷KMIP伺服器連線後繼續使用外部金鑰管理、請確定另一部KMIP伺服器可用於提供驗證金鑰。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 中斷KMIP伺服器與目前節點的連線：

此版本... ONTAP	使用此命令...
更新版本ONTAP	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,...`	不含更新版本ONTAP

在支援支援資源的環境中MetroCluster 、您必須在兩個叢集上為管理SVM重複執行這些命令。

下列 ONTAP 9.6 命令會停用連線至的兩個外部金鑰管理伺服器 `cluster1`，第一個命名的 `ks1`接聽預設連接埠 5696 、第二個連接埠的 IP 位址為 10.0.0.20 、接聽連接埠 24482 ：

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

深入瞭解 `security key-manager external remove-servers`及 `security key-manager delete` "指令參考資料ONTAP"。

從 ONTAP 9.6 開始、您可以使用 `security key-manager external modify-server` 變更外部金鑰管理伺服器 I/O 逾時和使用者名稱的命令。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 此工作需要進階權限。
- 在這個支援對象環境中MetroCluster 、您必須在兩個叢集上為管理SVM重複這些步驟。

步驟

1. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 修改叢集的外部金鑰管理程式伺服器內容：

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   超時值以秒表示。如果您修改使用者名稱、系統會提示您輸入新密碼。 如果您在叢集登入提示字元中執行命令、 *admin_SVM* 預設為目前叢集的管理SVM。您必須是叢集管理員、才能修改外部金鑰管理程式伺服器內容。

   下列命令會將的逾時值變更為 45 秒 `cluster1` 偵聽預設連接埠 5696 的外部金鑰管理伺服器：

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. 修改SVM的外部金鑰管理程式伺服器內容（僅限NVE）：

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   超時值以秒表示。如果您修改使用者名稱、系統會提示您輸入新密碼。 如果您在 SVM 登入提示字元下執行命令、 *SVM* 預設為目前的 SVM 。您必須是叢集或SVM管理員、才能修改外部金鑰管理程式伺服器內容。

   下列命令會變更的使用者名稱和密碼 `svm1` 偵聽預設連接埠 5696 的外部金鑰管理伺服器：

   ```
   svml::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. 針對任何其他SVM重複最後一個步驟。

相關資訊

- "安全金鑰管理程式外部修改伺服器"

從 **ONTAP** 的內建金鑰管理移轉至外部金鑰管理

如果您想從內建金鑰管理切換至外部金鑰管理、則必須先刪除內建金鑰管理組態、才能啟用外部金鑰管理。

開始之前

- 對於硬體型加密、您必須將所有FIPS磁碟機或SED的資料金鑰重設為預設值。

  "將FIPS磁碟機或SED恢復為無保護模式"

- 對於軟體型加密、您必須取消加密所有磁碟區。

  "取消Volume資料加密"

- 您必須是叢集管理員才能執行此工作。

步驟

1. 刪除叢集的內建金鑰管理組態：

此版本... ONTAP	使用此命令...
更新版本ONTAP	`security key-manager onboard disable -vserver SVM`
不含更新版本ONTAP	`security key-manager delete-key-database`

深入瞭解 `security key-manager onboard disable`及 `security key-manager delete-key-database` "指令參考資料ONTAP"。

從外部金鑰管理切換到**ONTAP**板載金鑰管理

若要切換至板載金鑰管理，請在啟用板載金鑰管理之前刪除外部金鑰管理配置。

開始之前

- 對於硬體型加密、您必須將所有FIPS磁碟機或SED的資料金鑰重設為預設值。

  "將FIPS磁碟機或SED恢復為無保護模式"

- 您必須刪除所有外部金鑰管理程式連線。

  "刪除外部金鑰管理程式連線"

- 您必須是叢集管理員才能執行此工作。

步驟

轉換金鑰管理的步驟取決於您所使用的 ONTAP 版本。

更新版本**ONTAP**

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 使用命令：

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   在支援支援資源的環境中MetroCluster 、您必須在兩個叢集上重複執行命令、才能使用管理SVM。

詳細了解 `security key-manager external disable`在"指令參考資料ONTAP"。

不含更新版本**ONTAP**

使用命令：

```
security key-manager delete-kmip-config
```

詳細了解 `security key-manager delete-kmip-config`在"指令參考資料ONTAP"。

相關資訊

- "安全金鑰管理員外部使用"

如果在**ONTAP**啟動過程中無法存取金鑰管理伺服器，會發生什麼情況

在開機期間、若為NSE設定的儲存系統無法觸及任何指定的金鑰管理伺服器、則執行某些預防措施以避免不必要的行為。ONTAP

如果儲存系統已設定為使用NSE、系統會重新鎖定SED、並開啟SED電源、則儲存系統必須從金鑰管理伺服器擷取所需的驗證金鑰、以驗證自己是否能存取資料。

儲存系統會嘗試聯絡指定的金鑰管理伺服器、最多三小時。如果之後儲存系統仍無法連絡到任何儲存系統、則開機程序會停止、儲存系統也會停止。

如果儲存系統成功連絡任何指定的金鑰管理伺服器、則會嘗試建立長達15分鐘的SSL連線。如果儲存系統無法與任何指定的金鑰管理伺服器建立SSL連線、開機程序會停止、儲存系統也會停止。

當儲存系統嘗試聯絡並連線至主要管理伺服器時、會在CLI中顯示失敗聯絡嘗試的詳細資訊。您可以隨時按Ctrl-C中斷聯絡活動嘗試

為了安全起見、SED僅允許有限數量的未授權存取嘗試、之後會停用對現有資料的存取。如果儲存系統無法連絡任何指定的金鑰管理伺服器以取得適當的驗證金鑰、則只能嘗試使用預設金鑰進行驗證、導致嘗試失敗並造成恐慌。如果儲存系統設定為在發生緊急情況時自動重新開機、則會進入開機迴圈、導致SED持續嘗試驗證失敗。

在這些情況下停止儲存系統的設計、是為了防止儲存系統進入開機迴圈、以及可能因超過某個連續驗證嘗試失敗次數的安全限制而永久鎖定的SED而導致意外的資料遺失。鎖定保護的限制和類型取決於製造規格和SED類型：

SED 類型	導致鎖定的連續驗證嘗試失敗次數	達到安全限制時的鎖定保護類型
HDD	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
X440_PHM2800MCTO 800GB NSE SSD搭配韌體版本NA00或NA01	5.	暫時性。鎖定功能只會在磁碟重新開機之前生效。
具有韌體版本NA00或NA01的X577_PHM2800MCTO 800GB NSE SSD	5.	暫時性。鎖定功能只會在磁碟重新開機之前生效。
X440_PHM2800MCTO 800GB NSE SSD、韌體版本更高	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
具有較高韌體版本的X577_PHM2800MCTO 800GB NSE SSD	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
所有其他SSD機型	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。

對於所有SED類型、成功驗證會將試用數重設為零。

如果您遇到儲存系統因為無法連線至任何指定的金鑰管理伺服器而停止運作的情況、則必須先識別並修正通訊故障的原因、然後再嘗試繼續開機儲存系統。

預設禁用**ONTAP**加密

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAP如有必要、您可以依預設停用整個叢集的加密功能。

開始之前

您必須是叢集管理員才能執行此工作、或是叢集管理員已委派權限的SVM管理員。

步驟

1. 若要在ONTAP 預設情況下停用對整個叢集的加密功能、請執行下列命令：

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```