自主勒索軟體保護
ONTAP 9

NetApp
February 26, 2026

目錄

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）

功能	ARP	ARP/AI
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
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	✓	✓	✓	✓	✓	✓	✓		

	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
SVM資料移動性 (`vserver migrate`)	✓	✓	✓	✓	✓	✓	✓		
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%
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"