



防範勒索軟體攻擊 ASA r2

NetApp
February 11, 2026

目錄

防範勒索軟體攻擊	1
建立防篡改快照，以防止對ASA r2 儲存系統的勒索軟體攻擊	1
初始化 SnapLock Compliance 時鐘	1
在ASA r2 儲存系統上利用 AI 實現自主勒索軟體防護	1
在叢集中的所有儲存單元上啟用 ARP/AI	2
在儲存虛擬機器中的所有儲存單元上啟用 ARP/AI	2
在儲存虛擬機器中的特定儲存單元上啟用 ARP/AI	2
停用 ASA r2 儲存系統上的預設自主勒索軟體防護	3
修改ASA r2 儲存系統上的 ARP/AI 快照保留期	4
使用ASA r2 儲存系統上的 AI 警報來回應自主勒索軟體防護	4
在ASA r2 儲存系統上使用 AI 暫停或恢復自主勒索軟體防護	5
暫停ARP/AI	5
恢復ARP/AI	5

防範勒索軟體攻擊

建立防篡改快照，以防止對ASA r2 儲存系統的勒索軟體攻擊

為了加強防範勒索軟體攻擊、請將快照複寫到遠端叢集、然後鎖定目的地快照、使其防篡改。鎖定的快照無法意外或惡意刪除。如果儲存單元遭到勒索軟體攻擊、您可以使用鎖定的快照來恢復資料。

初始化 SnapLock Compliance 時鐘

在建立防篡改快照之前、您必須先在本機叢集和目的地叢集上初始化 SnapLock Compliance 時鐘。

步驟

1. 選擇*叢集>總覽*。
2. 在 * 節點 * 區段中、選取 * 初始化 SnapLock Compliance 時鐘 *。
3. 選擇 * 初始化 *。
4. 確認規範時鐘已初始化。
 - a. 選擇*叢集>總覽*。
 - b. 在 * 節點 * 區段中、選取；然後選取 * SnapLock Compliance 時鐘 *。

接下來呢？

在本地和目標叢集上初始化 SnapLock Compliance 時鐘之後"使用鎖定的快照建立複寫關係"、您就可以開始使用了。

在ASA r2 儲存系統上利用 AI 實現自主勒索軟體防護

從ONTAP 9.17.1 開始，您可以使用人工智慧自主勒索軟體防護 (ARP/AI) 來保護ASA r2 系統上的資料。ARP/AI 可以快速偵測潛在的勒索軟體威脅，自動建立 ARP 快照來保護您的數據，並在系統管理員中顯示警告訊息，提醒您注意可疑活動。

ARP 透過採用機器學習模式進行反勒索軟體分析，提升網路彈性，該模式能夠以 98% 的準確率檢測不斷演變的勒索軟體，尤其適用於 SAN 環境。ARP 的機器學習模型在模擬勒索軟體攻擊前後，均使用大型檔案資料集進行預訓練。這種資源密集訓練在 ONTAP 外部進行，訓練產生的預訓練模型已整合到 ONTAP 中。該模型不可存取或修改。ARP/AI 在啟用後立即生效；無需"學習期"。



沒有任何勒索軟體偵測或防禦系統能夠完全保證免受勒索軟體攻擊。即使攻擊可能無法被偵測到，ARP/AI 也能在防毒軟體未能偵測到入侵時，作為重要的額外防禦層。

關於這項工作

- ARP/AI 支援包含在"ONTAP One 許可證"。
- 受 SnapMirror 活動同步、SnapMirror 同步或 SnapLock 保護的儲存單元不支援 ARP/AI。
- 從 ONTAP 9.18.1 開始，升級到 ONTAP 9.18.1 或初始化新的 ONTAP 9.18.1 ASA r2 叢集 12 小時後，所有新建立的儲存單元預設會啟用 ARP/AI。

- 啟用 ARP/AI 後，您應該"為您的安全文件啟用自動更新"自動接收新的安全性更新。

在叢集中的所有儲存單元上啟用 **ARP/AI**

如果您執行的是 ONTAP 9.17.1，則可以預設在叢集中建立的所有儲存單元上啟用 ARP/AI。

在 ONTAP 9.18.1 及更高版本中，所有新建儲存單元預設為啟用 ARP/AI。如果您在 ONTAP 9.17.1 中建立了未啟用 ARP/AI 的儲存單元，則可以手動啟用它。

步驟

1. 在 System Manager 中、選取*叢集>設定*。
2. 在 **Anti-ransomware** 旁邊，選擇 ，然後選擇 **Enable on all existing storage units**。
3. 選擇*啟用*。

在儲存虛擬機器中的所有儲存單元上啟用 **ARP/AI**

如果您執行的是 ONTAP 9.17.1，則可以預設在儲存虛擬機器 (VM) 中建立的所有儲存單元上啟用 ARP/AI。這表示在儲存 VM 中建立的任何新儲存單元都將自動啟用 ARP/AI。您也可以將 ARP/AI 套用到儲存 VM 中現有的儲存單元。

在 ONTAP 9.18.1 及更高版本中，所有新建儲存單元預設為啟用 ARP/AI。如果您在 ONTAP 9.17.1 中建立了未啟用 ARP/AI 的儲存單元，則可以手動啟用它。

步驟

1. 在系統管理員中，選擇「叢集」>「儲存虛擬機器」。
2. 選擇要啟用 ARP/AI 的儲存虛擬機器。
3. 在「安全」部分的「反勒索軟體」旁邊，選擇 ；然後選擇*編輯反勒索軟體設定*。
4. 選擇*啟用反勒索軟體*。

這將預設在所選儲存虛擬機器上建立的所有未來儲存單元上啟用 ARP/AI。

5. 若要將 ARP 套用於所選儲存虛擬機器上的現有儲存單元，請選擇*將此變更套用至此儲存虛擬機器上所有適用的現有儲存單元*。
6. 選擇*保存*。

結果

預設情況下，您在儲存 VM 上建立的所有新儲存單元都受到保護，免受勒索軟體攻擊，可疑活動會在系統管理員中報告給您。

在儲存虛擬機器中的特定儲存單元上啟用 **ARP/AI**

如果您正在執行 ONTAP 9.17.1，且不想在儲存 VM 中的所有儲存單元上啟用 ARP/AI，則可以選擇要啟用的特定單元。

在 ONTAP 9.18.1 及更高版本中，所有新建儲存單元預設為啟用 ARP/AI。如果您在 ONTAP 9.17.1 中建立了未啟用 ARP/AI 的儲存單元，則可以手動啟用它。

步驟

1. 在 System Manager 中、選取 * Storage* 。
2. 選擇要啟用 ARP/AI 的儲存單元。
3. 選擇  ；然後選擇*啟用反勒索軟體*。
4. 選擇*啟用*。

結果

您選擇的儲存單元受到保護，免受勒索軟體攻擊，並且可疑活動會在系統管理員中向您報告。

停用 ASA r2 儲存系統上的預設自主勒索軟體防護

當您初始化新的 ONTAP 9.18.1 ASA r2 叢集或將叢集升級到 ONTAP 9.18.1 時，ARP/AI 會在 12 小時的寬限期後，預設在所有新儲存單元上自動啟用。如果您在寬限期內未停用 ARP/AI，則在寬限期結束時，新儲存單元會在整個叢集範圍內啟用。

在 ONTAP 9.17.1 中建立的儲存單元必須"手動啟用"用於 ARP/AI。

步驟

您可以在最初的 12 小時寬限期內或之後停用預設啟用功能。

系統管理員

1. 選擇*叢集>設定*。
2. 禁用 ARP：
 - 在 12 小時寬限期內停用：
 - i. 在 **Anti-ransomware** 下，選擇 **Don't enable**，然後選擇 **Disable**。
 - 若要在 12 小時寬限期過後停用：
 - i. 在 **Anti-ransomware** 下，選取 ，然後取消選取 **Enable for new storage units**。
 - ii. 選擇 **Save**

CLI

1. 檢查預設啟用狀態：

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

2. 停用現有磁碟區和新磁碟區的預設啟用功能：

```
security anti-ransomware auto-enable modify -default-existing-volume  
-state false -default-new-volume-state false
```

修改ASA r2 儲存系統上的 ARP/AI 快照保留期

如果人工智慧自主勒索軟體防護 (ARP/AI) 偵測到您的一個或多個ASA r2 系統儲存單元出現異常活動，它會自動建立 ARP 快照來保護儲存單元的資料。根據您的儲存容量和資料的業務需求，您可能需要增加或減少預設 ARP 快照保留期。例如，您可能希望增加業務關鍵型應用程式的保留期，以便在需要時獲得更長的資料復原保留期；或者，您可能希望減少非關鍵型應用程式的保留期以節省儲存空間。

ARP 快照的預設保留期取決於您針對異常活動所採取的措施。

如果您採取此行動...	ARP 快照預設保留...
標記為誤報	12小時
標記為潛在勒索軟體攻擊	7天
不立即採取行動	10天

您可以使用ONTAP命令列介面 (CLI) 修改預設保留期。請參閱 ["修改ONTAP自動快照的選項"](#)了解更改預設保留期的步驟。

使用ASA r2 儲存系統上的 AI 警報來回應自主勒索軟體防護

如果人工智慧自主勒索軟體防護 (ARP/AI) 偵測到您的一個或多個ASA r2 系統儲存單元存在異常活動，系統管理員儀表板上會產生警告。您應該查看警告，驗證活動，並在必要時採取措施阻止任何對您資料的潛在威脅。

如果顯示 ARP/AI 警告訊息，在採取措施之前，您應該使用適當的應用程式完整性檢查器來驗證儲存單元上資料的完整性。驗證儲存單元的資料完整性有助於您確定該活動是否可接受，或是否為潛在的勒索軟體攻擊。

如果出現異常活動...	然後這樣做...
可接受	將該活動標記為誤報。
潛在的勒索軟體攻擊	將該活動標記為潛在的勒索軟體攻擊。
不定	請勿立即採取措施。請監控儲存單元最多 7 天。如果儲存單元繼續正常運行，則將該活動標記為誤報。如果儲存單元繼續表現出異常活動，則將該活動標記為潛在的勒索軟體攻擊。

步驟

1. 在System Manager中、選取* Dashboard *。

如果 ARP 在一個或多個儲存單元上偵測到異常活動，則會在 警告 下顯示一則訊息。

2. 選擇警告訊息。
3. 在「事件概覽」下，選擇指示具有異常活動的儲存單元數量的「警告」訊息。
4. 在*具有異常活動的儲存單元*下，選擇儲存單元。
5. 選擇*安全*。

如果儲存單元上存在異常活動，則會在「反勒索軟體」下方顯示一則訊息。

6. 選擇“選擇一個操作”。
7. 選擇*標記為誤報*或選擇*標記為潛在勒索軟體攻擊*。

接下來呢？

如果您發現儲存單元活動出現激增，無論是單次激增還是某種新常態下的激增，都應將其報告為安全狀態。手動將這些激增報告為安全狀態有助於提高 ARP 威脅評估的準確性。了解如何[報告已知的 ARP/AI 激增](#)。

在ASA r2 儲存系統上使用 AI 暫停或恢復自主勒索軟體防護

從ONTAP 9.17.1 開始，您可以使用人工智慧自主勒索軟體防護 (ARP/AI) 來保護ASA r2 系統上的資料。如果您正在規劃異常工作負載事件，可以暫時暫停 ARP/AI 分析，以防止誤報勒索軟體攻擊。工作負載事件完成後，您可以還原 ARP/AI 分析。

暫停ARP/AI

在開始異常工作負載事件之前，您可能需要暫時暫停 ARP/AI 分析，以防止勒索軟體攻擊的誤報偵測。

步驟

1. 在 System Manager 中、選取 * Storage* 。
2. 選擇要暫停 ARP/AI 的儲存單元。
3. 選擇*暫停反勒索軟體*。

結果

所選儲存單元的 ARP/AI 分析已暫停，並且在您恢復 ARP/AI 之前，系統管理員不會向您報告任何可疑活動。

恢復ARP/AI

如果您在異常工作負載期間暫停 ARP/AI，則在工作負載完成後，您應該恢復它以保護您的資料免受勒索軟體攻擊。

步驟

1. 在 System Manager 中、選取 * Storage* 。
2. 選擇要復原 ARP/AI 的儲存單元。
3. 選擇*恢復反勒索軟體*。

結果

對潛在勒索軟體攻擊的分析已恢復，可疑活動將在系統管理員中向您報告。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。