自主勒索軟體保護
ONTAP 9

NetApp
August 31, 2024

目錄

自主勒索軟體保護

自主勒索軟體保護總覽

從功能性的S廳9.10.1開始ONTAP 、自發勒索軟體保護（Arp）功能會在NAS（NFS和SMB）環境中使用工作負載分析功能、主動偵測可能表示勒索軟體攻擊的異常活動、並提出警示。

當懷疑有攻擊時、除了現有的Snapshot複本保護措施之外、Arp也會建立新的Snapshot複本。

授權與能力

ARP 需要授權。ARP 可與搭配使用 "ONTAP One 授權"。如果您沒有 ONTAP One 授權、則可使用其他授權來使用 ARP 、視您的 ONTAP 版本而定。

發行版**ONTAP**	授權
更新版本ONTAP	anti-勒索 軟體
零點9.10.1 ONTAP	Mt_E_Mgmt（多租戶金鑰管理）

- 如果您要升級ONTAP 至VMware 9.11.1或更新版本、且系統上已設定了Arp、則不需要購買新的勒索軟體授權。對於新的ARP組態、需要新的授權。
- 如果您要從ONTAP VMware版本9.11.1或更新版本還原ONTAP 至VMware版本9.10.1、且已啟用具有反勒索軟體授權的Arp、您將會看到一則警告訊息、可能需要重新設定Arp。 "瞭解如何還原Arp"。

您可以使用系統管理員或 ONTAP CLI 、以每個磁碟區為基礎來設定 ARP 。

勒索軟體保護策略**ONTAP**

有效的勒索軟體偵測策略應包含多個單一保護層。

類似的例子是車輛的安全功能。您不需要仰賴單一功能、例如安全帶、即可在意外中完全保護您的安全。安全袋、防鎖定煞車和前方撞擊警示都是額外的安全功能、可帶來更好的結果。勒索軟體保護應以相同方式檢視。

雖然 ONTAP 包含 FPolicy 、 Snapshot 複本、 SnapLock 和 Active IQ Digital Advisor 等功能、可協助防範勒索軟體、但下列資訊著重於具備機器學習能力的 ARP 隨裝即用功能。

若要深入瞭解 ONTAP 的其他反勒索軟體功能、請參閱"勒索軟體和 NetApp 的保護產品組合"。

ARP 偵測到什麼

ARP 旨在防範阻斷服務攻擊、攻擊者會在支付贖金之前、先竊取資料。ARP 會根據下列項目提供即時勒索軟體偵測：

- 將傳入資料識別為加密或純文字。
- 偵測到的分析

- **Entropy** ：評估檔案中資料的隨機性
- 檔案副檔名類型 ：不符合一般副檔名類型的副檔名
- 檔案 **IOPS** ：資料加密的異常 Volume 活動激增（從 ONTAP 9.11.1 開始）

在僅加密少數檔案、自動採取行動保護資料、並在發生可疑攻擊時發出警示、因此、ARP可以偵測大多數勒索軟體攻擊的擴散。

任何勒索軟體偵測或預防系統都無法完全保證勒索軟體攻擊的安全性。雖然攻擊可能無法被偵測到、但如果防毒軟體無法偵測到入侵、 ARP 就會成為重要的額外防禦層。

學習和作用中模式

ARP 有兩種模式：

- * 學習 * （或「乾跑」模式）
- * Active * （或「啟用」模式）

當您啟用 ARP 時、它會以 _ 學習模式 _ 執行。在學習模式中、 ONTAP 系統會根據分析領域來開發警示設定檔： Entropy 、檔案副檔名類型和檔案 IOPS 。在學習模式下執行Arp並有足夠時間評估工作負載特性之後、您可以切換至作用中模式、開始保護資料。一旦 ARP 切換至作用中模式、 ONTAP 就會建立 ARP Snapshot 複本、以便在偵測到威脅時保護資料。

建議您將 ARP 留在學習模式 30 天。從 ONTAP 9.13.1 開始、 ARP 會自動判斷最佳學習期間間隔、並將交換器自動化、這可能會在 30 天前發生。

在作用中模式中、如果檔案副檔名標示為異常、您應該評估警示。您可以對警示採取行動以保護資料、也可以將警示標記為誤報。將警示標記為誤報會更新警示設定檔。例如、如果警示是由新的副檔名觸發、而您將警示標記為誤判、則下次觀察到該副檔名時、您將不會收到警示。命令 `security anti-ransomware volume workload-behavior show` 顯示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表示、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。）

從 ONTAP 9.11.1 開始、您可以自訂 ARP 的偵測參數。如需詳細資訊、請參閱 管理 ARP 攻擊偵測參數。

威脅評估與 **ARP Snapshot** 複本

在作用中模式中、 ARP 會根據從學習到的分析中測得的傳入資料來評估威脅可能性。當 ARP 偵測到威脅時、就會指派測量值：

- 低 ：磁碟區最早偵測到異常狀況（例如、磁碟區中觀察到新的副檔名）。
- 中度 ：觀察到多個檔案副檔名之前從未見過的檔案。
  - 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。從 ONTAP 9.11.1 開始、檔案數量可修改、預設值為 20 。

在威脅較低的情況下、 ONTAP 會偵測異常狀況、並建立磁碟區的 Snapshot 複本、以建立最佳的還原點。ONTAP 會使用預先填入 ARP Snapshot 複本的名稱 `Anti-ransomware-backup` 例如、讓它易於識別 `Anti_ransomware_backup.2022-12-20_1248`。

ONTAP 執行分析報告、判斷異常狀況是否與勒索軟體設定檔相符、威脅就會升級至中度。低層級的威脅會記錄下來、並顯示在 System Manager 的 **EventS** 區段中。當攻擊可能性中等時、 ONTAP 會產生 EMS 通知、提示

您評估威脅。ONTAP 不會傳送低威脅的警示、但您可以從 ONTAP 9.14.1 開始 修改警示設定。如需詳細資訊、請參閱 回應異常活動。

您可以在 System Manager 的「 事件」 區段或與一起檢視威脅的相關資訊、無論其層級為何 `security anti-ransomware volume show` 命令。

ARP Snapshot 複本會保留至少兩天。從 ONTAP 9.11.1 開始、您可以修改保留設定。如需詳細資訊、請參閱 修改 Snapshot 複本選項。

如何在**ONTAP** 勒索軟體攻擊後恢復資料

如果懷疑有攻擊、系統會在該時間點製作Volume Snapshot複本、並鎖定該複本。如果稍後確認攻擊、則可使用 ARP Snapshot 複本還原磁碟區。

鎖定的Snapshot複本無法以正常方式刪除。不過、如果您稍後決定將攻擊標示為誤判、則鎖定的複本將會刪除。

在瞭解受影響的檔案和攻擊時間之後、您可以選擇性地從各種 Snapshot 複本恢復受影響的檔案、而不只是將整個 Volume 還原為 Snapshot 複本之一。

因此、Arp建置在獲證實ONTAP 的資料保護和災難恢復技術之上、以因應勒索軟體攻擊。如需恢復資料的詳細資訊、請參閱下列主題。

- "從Snapshot複本恢復（System Manager）"
- "從Snapshot複本（CLI）還原檔案"
- "智慧型勒索軟體還原"

自主勒索軟體保護的使用案例和考量

從 ONTAP 9.10.1 開始、 NAS 工作負載可使用自主 Ransomware Protection （ ARP ）。在部署 ARP 之前、您應該瞭解建議的用途和支援的組態、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：

- NFS儲存設備上的資料庫
- Windows或Linux主目錄

  由於使用者可以建立在學習期間未偵測到的副檔名檔案、因此此工作負載較可能出現誤報。

- 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 不適用於：

- 高檔案建立或刪除頻率的工作負載（數秒內就有數十萬個檔案、例如測試 / 開發工作負載）。
- ARP 的威脅偵測取決於其辨識出檔案建立、重新命名或刪除活動異常激增的能力。如果應用程式本身是檔案活動的來源、則無法有效地區別於勒索軟體活動。
- 應用程式或主機加密資料的工作負載。
  ARP 需要將傳入的資料識別為加密或未加密。如果應用程式本身正在加密資料、則此功能的有效性將會降低。不過、此功能仍可根據檔案活動（刪除、覆寫或建立、或以新副檔名建立或重新命名）和檔案類型運作。

支援的組態

從 ONTAP 9.10.1 開始、內部部署 ONTAP 系統中的 NFS 和 SMB 磁碟區可使用 ARP 。

下列 ONTAP 版本支援其他組態和磁碟區類型：

	ONTAP 9.15.1.1	**ONTAP 9.14.1.**	**ONTAP 9.13.1.12.9.11 .9.11.**	**ONTAP 9.12.1**	**零點9.11.1. ONTAP**	**零點9.10.1 ONTAP**
使用非同步 SnapMirror 保護磁碟區	✓	✓	✓	✓		
受異步 SnapMirror 保護的 SVM （ SVM 災難恢復）	✓	✓	✓	✓		
SVM資料移動性 (`vserver migrate`)	✓	✓	✓	✓		
資料量FlexGroup	✓	✓	✓			
多管理員驗證	✓	✓	✓			

SnapMirror與ARP互通性

從 ONTAP 9.12.1 開始、非同步 SnapMirror 目的地磁碟區支援 ARP 。SnapMirror Synchronous 不支援 ARP 。

如果SnapMirror來源磁碟區已啟用Arp、SnapMirror目的地磁碟區會自動取得來源磁碟區的Arp組態狀態（學習、啟用等）、Arp訓練資料、以及由Arp建立的Snapshot快照。不需要明確啟用。

雖然目的地Volume是由唯讀（RO）Snapshot複本所組成、但不會對其資料進行任何ARP處理。不過、當SnapMirror目的地Volume轉換為讀寫（RW）時、會自動在RW-轉換的目的地Volume上啟用ARP。除了已記錄在來源Volume上的內容、目的地Volume不需要任何額外的學習程序。

在版本號9.10.1和9.11.1中ONTAP 、SnapMirror不會將Arp組態狀態、訓練資料和Snapshot複本從來源磁碟區傳輸到目的地磁碟區。因此、當SnapMirror目的地Volume轉換為RW時、在轉換後、必須在學習模式中明確啟用目

的地Volume上的ARP。

ARP 和虛擬機器

虛擬機器（ VM ）支援 ARP 。ARP 偵測在 VM 內部和外部的變更時、行為會有所不同。不建議將 ARP 用於 VM 內部具有高 Entropy 檔案的工作負載。

VM 以外的變更

如果新的副檔名進入已加密的磁碟區、或是檔案副檔名變更、 ARP 就能偵測到 NFS 磁碟區上 VM 以外的檔案副檔名變更。可偵測的檔案副檔名變更包括：

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- NVRAM
- .vmem
- vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

VM 內部的變更

如果勒索軟體攻擊是針對 VM 內部的 VM 和檔案進行變更、而未在 VM 外部進行變更、則如果 VM 的預設 Entropy 低（例如 .txt 、 .docx 或 .mp4 檔案）、 ARP 會偵測到威脅。雖然 ARP 在這種情況下會建立保護性的 Snapshot 、但不會產生威脅警示、因為 VM 外部的副檔名並未遭到竄改。

如果檔案預設為高 Entropy （例如 .gzip 或密碼保護的檔案）、則 ARP 的偵測功能會受到限制。ARP 仍可在此執行個體中取得主動式快照、但如果檔案副檔名未遭到外部竄改、則不會觸發警示。

不支援的組態

下列系統組態不支援 ARP ：

- 不支援的S3環境ONTAP
- SAN環境

ARP 不支援下列 Volume 組態：

- FlexGroup Volume （ ONTAP 9.10.1 至 9.12.1 ）。從 ONTAP 9.13.1 開始、支援 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
- 純SAN磁碟區

- 資料量SnapLock
- SnapMirror同步
- 非同步 SnapMirror （僅在 ONTAP 9.10.1 和 9.11.1 中不受支援。從 ONTAP 9.12.1 開始支援非同步 SnapMirror 。如需詳細資訊、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

根據處理量和尖峰 IOPS 的測量結果、 ARP 對系統效能的影響最小。ARP 功能的影響取決於特定的 Volume 工作負載。對於一般工作負載、建議使用下列組態限制：

工作負載特性	每個節點的建議**Volume**限制	超過每節點磁碟區限制時效能降低：**[*]**
讀取密集或資料可以壓縮。	150	最高IOPS的4%
寫入密集、資料無法壓縮。	60	IOPS上限的10%

通過：[*]無論新增的磁碟區數量超過建議的限制、系統效能不會超過這些百分比。

由於 ARP 分析會依優先順序執行、因此當受保護的磁碟區數量增加時、分析會在每個磁碟區上執行的頻率較低。

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。瞭解操作方法 "為受 ARP 保護的磁碟區啟用 MAV"。

您需要定義 MAV 群組的管理員、並為建立 MAV 規則 `security anti-ransomware volume disable`、`security anti-ransomware volume pause`和 `security anti-ransomware volume attack clear-suspect` 您要保護的 ARP 命令。MAV 群組中的每位管理員都必須核准每個新的規則要求和 "再次新增 MAV 規則" 在 MAV 設定中。

從 ONTAP 9.14.1 開始、 ARP 會提供建立 ARP 快照和觀察新副檔名的警示。這些事件的警示預設為停用。警示可在 Volume 或 SVM 層級設定。您可以使用在 SVM 層級建立 MAV 規則 `security anti-ransomware vserver event-log modify` 或是在 Volume 層級使用 `security anti-ransomware volume event-log modify`。

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"

啟用自發勒索軟體保護

從ONTAP S廳9.10.1開始、可在新的或現有的磁碟區上啟用自發勒索軟體保護（Arp）。您

必須先在學習模式中啟用ARP、系統會分析工作負載以找出正常行為的特徵。您可以在現有的磁碟區上啟用Arp、也可以建立新的磁碟區、從頭開始啟用Arp。

關於這項工作

您應該一律在學習（或試運行）模式中啟用 ARP 。從使用中模式開始、可能會產生過多的誤報。

建議您讓 ARP 以學習模式執行至少 30 天。從 ONTAP 9.13.1 開始、 ARP 會自動判斷最佳學習期間間隔、並將交換器自動化、這可能會在 30 天前發生。如需詳細資訊、請參閱 "學習和作用中模式"。

> 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。

開始之前

- 您必須為 NFS 或 SMB （或兩者）啟用儲存 VM （ SVM ）。
- 。 正確授權 必須為您的 ONTAP 版本安裝。
- 您必須設定具有 NAS 工作負載的用戶端。
- 您想要設定 ARP 的磁碟區需要受到保護、而且必須有作用中的磁碟區 "交會路徑"。
- 磁碟區必須低於 100% 滿。
- 建議您將 EMS 系統設定為傳送電子郵件通知、其中包括 ARP 活動通知。如需詳細資訊、請參閱 "設定EMS事件以傳送電子郵件通知"。
- 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。如需詳細資訊、請參閱 "啟用多重管理驗證"。

啟用 **ARP**

您可以使用系統管理員或 ONTAP CLI 來啟用 ARP 。

系統管理員

步驟

1. 選取 * 儲存 > 磁碟區 * 、然後選取您要保護的磁碟區。
2. 在 * Volumes * （卷）總覽的 * Security （安全性） * 標籤中、在 * Anti-勒索 ware* （ * 反勒索軟體）方塊中、選取 * Status （狀態） * 以在學習模式中從 Disabled （已停用）切換為 Enabled （已啟用）。
3. 學習期間結束時、請將ARP切換至作用中模式。

   從 ONTAP 9.13.1 開始、 ARP 會自動判斷最佳學習期間間隔、並將交換器自動化。您可以 "在關聯的儲存 VM 上停用此設定" 如果您想要手動將學習模式控制為使用中模式切換。

   a. 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。
   b. 在 * Volumes * （卷）總覽的 * Security （安全性） * 索引標籤中、在 Anti-勒索 ware 方塊中選取 * Switch* to active mode （ * 切換 * 至作用中模式）。
4. 您可以在 * 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* （反勒索軟體）狀態。

CLI

如果您是在現有磁碟區上啟用 ARP 、而不是在新磁碟區上啟用 ARP 、則使用 CLI 啟用 ARP 的程序會有所不同。

在現有磁碟區上啟用 **ARP**

1. 修改現有磁碟區以在學習模式中啟用勒索軟體保護：

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

   如果您執行的是 ONTAP 9.13.1 或更新版本、則會啟用調適性學習、以便自動完成變更至作用中狀態。如果您不想自動啟用此行為、請變更所有相關磁碟區上 SVM 層級的設定：

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

2. 學習期間結束時、如果尚未自動完成、請修改受保護的磁碟區以切換至作用中模式：

   ```
   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
   active
   ```

3. 驗證磁碟區的ARP狀態。

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

在新磁碟區上啟用 **ARP**

1. 在資源配置資料之前、請先啟用反勒索軟體保護功能、建立新的 Volume 。

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

   如果您執行的是 ONTAP 9.13.1 或更新版本、則會啟用調適性學習、以便自動完成變更至作用中狀態。如果您不想自動啟用此行為、請變更所有相關磁碟區上 SVM 層級的設定：

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

2. 學習期間結束時、如果尚未自動完成、請修改受保護的磁碟區以切換至作用中模式：

   ```
   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
   active
   ```

3. 驗證磁碟區的ARP狀態。

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

在新磁碟區中預設啟用「自動勒索軟體保護」

從ONTAP S廳9.10.1開始、您可以設定儲存VM（SVM）、以便在學習模式中預設啟用新磁碟區、以進行自發勒索軟體保護（Arp）。

關於這項工作

根據預設、新的磁碟區會以停用模式使用 ARP 建立。您可以在 System Manager 和 CLI 中修改此設定。在學習（或試運行）模式下，默認情況下啓用的卷設置爲 ARP 。

只有在變更設定之後、才能在 SVM 中建立的磁碟區上啟用 ARP 。將不會在現有磁碟區上啟用 ARP 。瞭解操作方法 "在現有磁碟區中啟用ARP"。

從 ONTAP 9.13.1 開始、調適性學習已新增至 ARP 分析、從學習模式切換至主動模式即會自動完成。如需詳細資訊、請參閱 "學習和作用中模式"。

開始之前

- 。 正確授權 必須為您的 ONTAP 版本安裝。
- 磁碟區必須低於 100% 滿。
- 交會路徑必須為作用中。
- 從 ONTAP 9.13.1 開始、建議您啟用多重管理驗證（ MAV ）、以便在執行反勒索軟體作業時、需要兩個或多個已驗證的使用者管理員。 "深入瞭解"。

將 **ARP** 從學習模式切換至使用中模式

從 ONTAP 9.13.1 開始、調適性學習已新增至 ARP 分析。從學習模式切換至作用中模式會自動完成。ARP 自動從學習模式切換至使用中模式的自主決定、是根據下列選項的組態設定而定：

```
-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
```

學習 30 天之後、即使其中一或多個條件不滿足、 Volume 仍會自動切換至使用中模式。也就是說、如果啟用自動切換、則磁碟區最多會在 30 天之後切換至使用中模式。30 天的最大值是固定的、不可修改的。

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"。

步驟

您可以使用系統管理員或 ONTAP CLI 預設啟用 ARP 。

系統管理員

1. 選取 * 儲存 > 儲存 VM* 、然後選取包含您要使用 ARP 保護之磁碟區的儲存 VM 。
2. 瀏覽至 * 設定 * 索引標籤。在 * 安全 * 下、找到 防勒索軟體 磚、然後選取 
3. 核取方塊以啟用 NAS 磁碟區的 ARP 。勾選額外方塊、即可在儲存 VM 中所有符合資格的 NAS 磁碟區上啟用 ARP 。

> 如果您已升級至 ONTAP 9.13.1 、 * 自動啟用「充分學習 * 後自動切換為使用中模式」設定。這可讓 ARP 決定最佳學習週期間隔、並將交換器自動切換至作用中模式。如果您想要手動切換至使用中模式、請關閉設定。

CLI

1. 修改現有 SVM 、以在新磁碟區中預設啟用 ARP ：
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   在CLI中、您也可以針對新磁碟區建立新的SVM、並在預設情況下啟用Arp。
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

   如果您升級至 ONTAP 9.13.1 或更新版本、則會啟用調適學習功能、以便自動完成對作用中狀態的變更。如果您不想自動啟用此行為、請使用下列命令：

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

暫停勒索軟體保護、將工作負載事件排除在分析範圍之外

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"。

關於這項工作

在暫停ARP期間、不會記錄任何事件、也不會針對新的寫入動作進行任何動作。不過、分析作業會在背景中繼續進行、以處理較早的記錄。

> 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 Volumes （磁碟區）總覽的 **Security** （ 安全性） ***** 索引標籤中、在 *** Anti-**勒索 **ware** 方塊中選取 * Pause anti-勒索 ware* 。

> 從 ONTAP 9.13.1 開始、如果您使用 MAV 來保護您的 ARP 設定、暫停作業會提示您取得一或多個額外管理員的核准。 "必須收到所有管理員的核准" 與 MAV 核准群組相關聯、否則作業將會失敗。

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
```

3. * 如果您使用 MAV （從 ONTAP 9.13.1 開始的 ARP 提供）來保護您的 ARP 設定、 * 暫停作業會提示您取得一或多位其他管理員的核准。必須從與 MAV 核准群組相關的所有管理員處收到核准、否則作業將會失敗。

   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]
```

管理自主勒索軟體保護攻擊偵測參數

從 ONTAP 9.11.1 開始、您可以修改特定 Automware Protection 磁碟區上的勒索軟體偵測參數、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

當自主勒索軟體保護（ARP）處於學習模式時、它會為 Volume 行為開發基準值。這些是 Entropy 、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。如需這些條件的詳細資訊、請參閱 ARP 偵測到什麼。

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。）

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。如需詳細資訊、請參閱 [modify-alerts]

某些磁碟區和工作負載需要不同的偵測參數。例如、啟用 ARP 的磁碟區可能會裝載許多類型的副檔名、在這種情況下、您可能會想要將前所未見的副檔名臨界值數修改為大於預設值 20 的數字、或是根據前所未見的副檔名停用警告。從 ONTAP 9.11.1 開始、您可以修改攻擊偵測參數、使其更適合您的特定工作負載。

修改攻擊偵測參數

視您的 ARP 磁碟區預期行為而定、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
              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 : 20
         Never Seen before File Extensions Duration in Hour : 24
   ```

2. 所有顯示的欄位都可以使用布林值或整數值來修改。若要修改欄位、請使用 `security anti-ransomware volume attack-detection-parameters modify` 命令。

   如需參數的完整清單、請參閱 "指令參考資料ONTAP"。

回報已知的突波

即使處於作用中模式、 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（一次性突波或是新常態特徵的突波）、您應該將其回報為安全的。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
   ```

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
   ```

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 Snapshot

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。

事件警示可透過多重管理驗證來控制。如需詳細資訊、請參閱 使用 ARP 保護的磁碟區進行多重管理驗證。

系統管理員

設定磁碟區的警示

1. 瀏覽至 **Volumes** （磁碟區） 。選取您要修改設定的個別磁碟區。
2. 選擇「 安全性 」標籤、然後選擇「事件安全性設定 ** 」。
3. 若要接收關於「偵測到新的副檔名 」和「建立的勒索軟體快照 」的警示、請選取「 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 儲存 。

設定 **SVM** 的警示

1. 瀏覽至 儲存 **VM** 、然後選取您要啟用設定的 SVM 。
2. 在「 安全性 」標題下、找到「 防勒索軟體 」卡。接著選擇 ⋮ 「編輯勒索軟體事件嚴重性」 ** 。
3. 若要接收關於「偵測到新的副檔名 」和「建立的勒索軟體快照 」的警示、請選取「 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 儲存 。

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 -is
-enabled-on-new-file-extension-seen true
```

- 若要設定建立 ARP Snapshot 的警示：

```
security anti-ransomware volume event-log modify -vserver svm_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 Snapshot 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。

更多資訊

- "瞭解自主勒索軟體保護攻擊和自主勒索軟體保護快照"

回應異常活動

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。

關於這項工作

當Arp偵測到高資料Entropy、異常Volume活動與資料加密、以及異常檔案副檔名的任何組合時、會顯示可疑檔案的清單。

發出警告時、請以下列兩種方式之一來指定檔案活動：

- 誤判

  識別的檔案類型應在您的工作負載中使用、而且可以忽略。

- 可能的勒索軟體攻擊

  識別出的檔案類型在您的工作負載中是非預期的、應該視為潛在攻擊。

在這兩種情況下、更新和清除通知後、系統都會繼續正常監控。ARP 會將您的評估記錄在威脅評估設定檔中、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 必須以作用中模式執行。

步驟

您可以使用系統管理員或 ONTAP CLI 來回應異常工作。

系統管理員

1. 當您收到「異常活動」通知時、請點選連結。或者、瀏覽至 * Volumes * 總覽的 * Security * 標籤。

   警告會顯示在 * 事件 * 功能表的 * 總覽 * 窗格中。

2. 顯示「偵測到異常Volume活動」訊息時、請檢視可疑檔案。

   在 * 安全 * 標籤中、選取 * 檢視可疑的檔案類型 * 。

3. 在「可疑的檔案類型」對話方塊中、檢查每種檔案類型、並將其標示為「誤判」或「潛在勒索軟體攻擊」。

如果您選取此值...	請採取此行動...
誤判	選擇 * 更新 * 和 * 清除可疑檔案類型 * 、以記錄您的決定並恢復正常的 ARP 監控。 從 ONTAP 9.13.1 開始、如果您使用 MAV 來保護您的 ARP 設定、則清除可疑的作業會提示您取得一或多個額外管理員的核准。 "必須收到所有管理員的核准" 與 MAV 核准群組相關聯、否則作業將會失敗。
可能的勒索軟體攻擊	回應攻擊並還原受保護的資料。然後選擇 * 更新 * 和 * 清除可疑的檔案類型 * 來記錄您的決定並恢復正常的 ARP 監控。 如果還原整個磁碟區、則沒有可疑的檔案類型可清除。

CLI

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: 9/14/2021 01:03:23
   Number of Attacks: 1
   ```

   您也可以檢查EMS訊息：

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

2. 產生攻擊報告並記下輸出位置：

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

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：

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
```

4. 根據您對副檔名的評估、採取下列其中一項行動：

   - 誤判

     輸入下列命令以記錄您的決定、將新的副檔名新增至允許的項目清單、並恢復正常的反勒索軟體監控：
     `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`

     使用下列其中一個參數來識別副檔名：
     `[-seq-no` *`integer`*`]` 可疑清單中檔案的序號。
     `[-extension` *`text`*`, … ]` 副檔名
     `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` 要清除之檔案範圍的開始和結束時間、格式為「 MM/DD/YYYY HH ： MM ： SS 」。

   - 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"。恢復資料後、輸入下列命令以記錄您的決定、並恢復正常的 ARP 監控：

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

     使用下列其中一個參數來識別副檔名：
     `[-seq-no` *`integer`*`]` 可疑清單中檔案的序號
     `[-extension` *`text`*`, … ]` 副檔名
     `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` 要清除之檔案範圍的開始和結束時間、格式為「 MM/DD/YYYY HH ： MM ： SS 」。

   如果還原整個磁碟區、則沒有可疑的檔案類型可清除。將移除 ARP 建立的備份快照、並清除攻擊報告。

5. 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。

6. 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]
```

更多資訊

- "KB ：瞭解自主勒索軟體保護攻擊和自主勒索軟體保護快照"。

勒索軟體攻擊後還原資料

自主勒索軟體保護（ ARP ）會建立名為的 Snapshot 複本 `Anti_ransomware_backup` 當偵測到可能的勒索軟體威脅時。您可以使用這些 ARP Snapshot 複本或磁碟區的另一個 Snapshot 複本來還原資料。

關於這項工作

如果磁碟區具有SnapMirror關係、請在從Snapshot複本還原之後、立即手動複寫磁碟區的所有鏡射複本。否則可能導致無法使用的鏡像複本、必須刪除並重新建立。

從非的 Snapshot 還原 `Anti_ransomware_backup` 在識別出系統攻擊之後、您必須先發行 ARP Snapshot 。

如果未回報系統攻擊、您必須先從還原 `Anti_ransomware_backup` 然後、 Snapshot 複本會從您選擇的 Snapshot 複本完成磁碟區的後續還原。

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 Snapshot 還原、請跳至步驟二。若要從較早的 Snapshot 複本還原、您必須先釋放 ARP Snapshot 上的鎖定。
   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. 將檔案標示為「誤判」。
   d. 選擇 * 更新 * 和 * 清除可疑檔案類型 *
2. 在磁碟區中顯示Snapshot複本：

   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 Snapshot 複本旁邊的，然後選取 * Restore * 。

如果未識別出系統攻擊、請進行還原

1. 在磁碟區中顯示Snapshot複本：

   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 它們選擇 `Anti_ransomware_backup` 「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 Snapshot 複本。選擇*還原*。

CLI

系統攻擊後還原

1. 若要從 ARP Snapshot 複本還原、請跳至步驟二。若要還原舊版 Snapshot 複本的資料、您必須釋放 ARP Snapshot 上的鎖定。

   如果您使用的是、只有在從舊版 Snapshot 複本還原之前、才需要釋放反勒索軟體 SnapLock `volume snap restore` 命令、如下所述。 如果您要使用 Flex Clone 、單一檔案快照還原或其他方法還原資料、則不需要這麼做。

   將攻擊標示為「誤判」和「明確懷疑」：
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`
   使用下列其中一個參數來識別副檔名：
   `[-seq-no` *`integer`*`]` 可疑清單中檔案的序號。
   `[-extension` *`text`*`, … ]` 副檔名
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` 要清除之檔案範圍的開始和結束時間、格式為「 MM/DD/YYYY HH ： MM ： SS 」。
2. 列出Volume中的Snapshot複本：

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

下列範例顯示中的 Snapshot 複本 `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Snapshot複本還原磁碟區內容：

```
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Volume中的Snapshot複本：

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

下列範例顯示中的 Snapshot 複本 `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Snapshot複本還原磁碟區內容：

```
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
```

3. 重複步驟 1 和 2 、使用所需的 Snapshot 複本還原磁碟區。

更多資訊

- "KB ： ONTAP 中的勒索軟體預防與還原"

修改自動Snapshot複本的選項

從 ONTAP 9.11.1 開始、您可以使用 CLI 來控制自動勒索軟體保護（ ARP ） Snapshot 複本的保留設定、這些複本會自動產生、以因應可疑的勒索軟體攻擊。

開始之前

您只能修改節點 SVM 上的 ARP Snapshots 選項。

步驟

1. 若要顯示所有目前的 ARP Snapshot 複本設定、請輸入：
   `vserver options -vserver` *`svm_name`* `arw*`

。 `vserver options` 命令是隱藏的命令。若要檢視手冊頁、請輸入 `man vserver options` 在 ONTAP CLI 中。

2. 若要顯示選取的目前 ARP Snapshot 複本設定、請輸入：
   `vserver options -vserver svm_name -option-name arw_setting_name`
3. 若要修改 ARP Snapshot 複本設定、請輸入：
   `vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

   可修改下列設定：

ARW 設定	說明
`arw.snap.max.count`	指定在任何指定時間內、磁碟區中可存在的最大ARP Snapshot複本數。系統會刪除較舊的複本、以確保「ARP Snapshot複本」的總數達到此指定限制。 。 `-option-value` 參數接受介於 3 和 8 之間的整數（含 3 和 8 ）。預設值為 6 。
`arw.snap.create.interval.hours`	指定 ARP Snapshot 複本之間的時間間隔（以小時計）。當懷疑資料 Entropy 型攻擊、且最近建立的 ARP Snapshot 複本早於指定時間間隔時、就會建立新的 ARP Snapshot 複本。 。 `-option-value` 參數接受 1 到 48 之間的整數（含 1 到 48 ）。預設值為 4 。
`arw.snap.normal.retain.interval.hours`	指定保留 ARP Snapshot 複本的持續時間（以小時計）。當 ARP Snapshot 複本達到保留臨界值時、會在刪除之前建立任何其他 ARP Snapshot 複本。超過保留臨界值的 ARP Snapshot 複本不可能有多個。 。 `-option-value` 參數接受介於 4 到 96 之間的整數（含 4 到 96 ）。預設值為 48 。
`arw.snap.max.retain.interval.days`	指定可以保留 ARP Snapshot 複本的最長持續時間（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 Snapshot 複本。 如果偵測到中度威脅、就會忽略 ARP Snapshot 複本的最大保留時間間隔。針對威脅所建立的 ARP Snapshot 複本會保留、直到您回應威脅為止。將威脅標示為誤報、刪除磁碟區上的 ARP Snapshot 複本。 。 `-option-value` 參數接受 1 到 365 之間的整數（含 1 到 365 ）。預設值為 5 。
`arw.snap.create.interval.hours.post.max.count`	指定當磁碟區已包含最大 ARP Snapshot 複本數時、每個 ARP Snapshot 複本之間的時間間隔（以小時為單位）。當達到最大數量時、系統會刪除一個「ARP Snapshot複本」、以便為新的複本預作空間。使用此選項可降低新的「ARP Snapshot複本」複本建立速度、以保留舊版複本。如果磁碟區已包含 ARP Snapshot 複本的最大數量、則此選項中指定的時間間隔將用於下一次建立 ARP Snapshot 複本、而非 `arw.snap.create.interval.hours`。 。 `-option-value` 參數接受 4 到 48 之間的整數（含 4 到 48 ）。預設值為 8 。

ARW 設定	說明
`arw.surge.snap.interval.days`	指定為回應 IO 突波而建立的 ARP Snapshot 複本之間的間隔（以天為單位）。當 IO 流量激增且上次建立的 ARP Snapshot 複本早於此指定時間間隔時、ONTAP 會建立 ARP Snapshot 突波複本。此選項也會指定 ARP 喘振 Snapshot 複本的保留期間（以天為單位）。 。 `-option-value` 參數接受 1 到 365 之間的整數（含 1 到 365 ）。預設值為 5 。
`arw.snap.new.extns.interval.hours`	此選項指定偵測到新副檔名時所建立的 ARP Snapshot 複本之間的時間間隔（小時）。新的 ARP Snapshot 複本會在何時建立 會觀察到新的副檔名；觀察到新副檔名時所建立的上一個 Snapshot 會比這個指定的時間間隔還要舊。在經常建立新副檔名的工作負載上、此時間間隔有助於控制 ARP Snapshot 複本的頻率。此選項不受影響 `arw.snap.create.interval.hours`，指定資料 Entropy 型 ARP Snapshot 複本的時間間隔。 。 `-option-value` 參數接受介於 24 和 8760 之間的整數。預設值為 48 。

版權資訊

商標資訊