# Proteggersi dagli attacchi ransomware

ASA r2

NetApp
February 11, 2026

# Sommario

# Proteggersi dagli attacchi ransomware

## Crea snapshot a prova di manomissione per proteggerti dagli attacchi ransomware sui sistemi di archiviazione ASA r2

Per una protezione avanzata contro gli attacchi ransomware, replica le snapshot su un cluster remoto, quindi blocca le snapshot di destinazione per renderle a prova di manomissione. Gli snapshot bloccati non possono essere eliminati accidentalmente o in modo pericoloso. Puoi utilizzare snapshot bloccate per ripristinare i dati, se un'unità di storage viene mai compromessa da un attacco ransomware.

### Inizializzare l'orologio SnapLock Compliance

Prima di poter creare snapshot a prova di manomissione, è necessario inizializzare il clock SnapLock Compliance sui cluster locali e di destinazione.

**Fasi**

1. Selezionare **Cluster > Overview** (Cluster > Panoramica).
2. Nella sezione **nodi**, selezionare **Inizializza orologio SnapLock Compliance**.
3. Selezionare **Inizializza**.
4. Verificare che l'orologio di conformità sia inizializzato.
   a. Selezionare **Cluster > Overview** (Cluster > Panoramica).
   b. Nella sezione **nodi**, selezionare ; quindi selezionare **SnapLock Compliance Clock**.

**Cosa succederà?**

Dopo aver inizializzato l'orologio SnapLock Compliance sui cluster locali e di destinazione, si è pronti per "creare una relazione di replica con gli snapshot bloccati".

## Abilita la protezione autonoma dal ransomware con l'intelligenza artificiale sui tuoi sistemi di archiviazione ASA r2

A partire da ONTAP 9.17.1, puoi utilizzare la protezione autonoma contro i ransomware con intelligenza artificiale (ARP/AI) per proteggere i dati sul tuo sistema ASA r2. ARP/AI rileva rapidamente potenziali minacce ransomware, crea automaticamente uno snapshot ARP per proteggere i tuoi dati e visualizza un messaggio di avviso in Gestione Sistema per avvisarti di attività sospette.

ARP migliora la resilienza informatica adottando un modello di apprendimento automatico per l'analisi anti-ransomware che rileva forme di ransomware in continua evoluzione con una precisione del 98% per gli ambienti SAN. Il modello di apprendimento automatico di ARP è pre-addestrato su un ampio set di dati di file sia prima che dopo un attacco ransomware simulato. Questa formazione ad alta intensità di risorse viene eseguita esternamente a ONTAP e il modello pre-addestrato che ne risulta è incluso on-box con ONTAP. Questo modello non è accessibile né modificabile. ARP/AI è attivo immediatamente dopo l'abilitazione; non è

presente alcun "periodo di apprendimento".

> Nessun sistema di rilevamento o prevenzione del ransomware può garantire completamente la sicurezza da un attacco ransomware. Sebbene un attacco possa passare inosservato, ARP/AI funge da importante ulteriore livello di difesa se il software antivirus non riesce a rilevare un'intrusione.

**A proposito di questa attività**

- Il supporto ARP/AI è incluso con "Licenza ONTAP One" .
- ARP/AI non è supportato su unità di archiviazione protette da SnapMirror active sync, SnapMirror synchronous o SnapLock.
- A partire da ONTAP 9.18.1, ARP/AI è abilitato per impostazione predefinita su tutte le unità di archiviazione appena create 12 ore dopo l'aggiornamento a ONTAP 9.18.1 o l'inizializzazione di un nuovo ONTAP 9.18.1 ASA r2 cluster.
- Dopo aver abilitato ARP/AI, dovresti "abilita gli aggiornamenti automatici per i tuoi file di sicurezza" per ricevere automaticamente i nuovi aggiornamenti di sicurezza.

## Abilita ARP/AI su tutte le unità di archiviazione nel cluster

Se si esegue ONTAP 9.17.1, è possibile abilitare ARP/AI su tutte le unità di archiviazione create nel cluster per impostazione predefinita.

In ONTAP 9.18.1 e versioni successive, ARP/AI è abilitato per impostazione predefinita su tutte le nuove unità di storage. Se si dispone di unità di storage create in ONTAP 9.17.1 per le quali ARP/AI non è abilitato, è possibile abilitarlo manualmente.

**Fasi**

1. In System Manager, selezionare **Cluster > Settings**.
2. Accanto a **Anti-ransomware**, seleziona ⋮ e poi seleziona **Abilita su tutte le unità di archiviazione esistenti**.
3. Selezionare **Abilita**.

## Abilita ARP/AI su tutte le unità di archiviazione in una VM di archiviazione

Se si esegue ONTAP 9.17.1, è possibile abilitare ARP/AI su tutte le unità di storage create in una storage virtual machine (VM) per impostazione predefinita. Ciò significa che qualsiasi nuova unità di storage creata nella storage VM avrà ARP/AI abilitato automaticamente. È anche possibile applicare ARP/AI alle unità di storage esistenti nella storage VM.

In ONTAP 9.18.1 e versioni successive, ARP/AI è abilitato per impostazione predefinita su tutte le nuove unità di storage. Se si dispone di unità di storage create in ONTAP 9.17.1 per le quali ARP/AI non è abilitato, è possibile abilitarlo manualmente.

**Fasi**

1. In System Manager, seleziona **Cluster > VM di archiviazione**.
2. Selezionare la VM di archiviazione su cui si desidera abilitare ARP/AI.
3. Nella sezione **Sicurezza**, accanto a **Anti-ransomware**, seleziona ⋮ ; quindi seleziona **Modifica impostazioni anti-ransomware**.
4. Seleziona **Abilita anti-ransomware**.

In questo modo, per impostazione predefinita, ARP/AI viene abilitato su tutte le future unità di archiviazione create sulla VM di archiviazione selezionata.

5. Per applicare ARP alle unità di archiviazione esistenti sulla VM di archiviazione selezionata, seleziona **Applica questa modifica a tutte le unità di archiviazione esistenti applicabili su questa VM di archiviazione**.
6. Selezionare **Salva**.

**Risultato**

Per impostazione predefinita, tutte le nuove unità di archiviazione create sulla VM di archiviazione sono protette dagli attacchi ransomware e le attività sospette vengono segnalate in System Manager.

## Abilita ARP/AI su unità di archiviazione specifiche in una VM di archiviazione

Se si esegue ONTAP 9.17.1 e non si desidera abilitare ARP/AI su tutte le unità di archiviazione in una storage VM, è possibile selezionare le unità specifiche che si desidera abilitare.

In ONTAP 9.18.1 e versioni successive, ARP/AI è abilitato per impostazione predefinita su tutte le nuove unità di storage. Se si dispone di unità di storage create in ONTAP 9.17.1 per le quali ARP/AI non è abilitato, è possibile abilitarlo manualmente.

**Fasi**

1. In System Manager, selezionare **Storage**.
2. Seleziona le unità di archiviazione per le quali desideri abilitare ARP/AI.
3. Selezionare ⋮ ; quindi seleziona **Abilita anti-ransomware**.
4. Selezionare **Abilita**.

**Risultato**

Le unità di archiviazione selezionate sono protette dagli attacchi ransomware e le attività sospette ti vengono segnalate in Gestione sistema.

# Disattiva la protezione ransomware autonoma predefinita sui tuoi sistemi di archiviazione ASA r2

Quando si inizializza un nuovo cluster ONTAP 9.18.1 ASA r2 o si aggiorna il cluster a ONTAP 9.18.1, ARP/AI viene automaticamente abilitato per impostazione predefinita su tutte le nuove unità di storage dopo un grace period di 12 ore. Se non si disabilita ARP/AI durante il grace period, viene abilitato a livello di cluster per le nuove unità di storage al termine del grace period.

Le unità di archiviazione create in ONTAP 9.17.1 devono essere "abilitato manualmente" per ARP/AI.

**Fasi**

È possibile disattivare l'abilitazione predefinita durante o dopo il grace period iniziale di 12 ore.

**System Manager**

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Disabilita ARP:
   - Per disattivare durante il grace period di 12 ore:
     i. In **Anti-ransomware**, seleziona **Don't enable** e poi seleziona **Disable**.
   - Per disattivare dopo il grace period di 12 ore:
     i. In **Anti-ransomware**, seleziona e poi deseleziona **Abilita per nuove unità di archiviazione**.
     ii. Seleziona **Save**

**CLI**

1. Verificare lo stato di abilitazione predefinito:

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

2. Disabilitare l'abilitazione predefinita per i volumi esistenti e nuovi:

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

# Modificare i periodi di conservazione degli snapshot ARP/AI sui sistemi di archiviazione ASA r2

Se la protezione autonoma dal ransomware con intelligenza artificiale (ARP/AI) rileva un'attività anomala su una o più unità di archiviazione del sistema ASA r2, crea automaticamente uno snapshot ARP per proteggere i dati dell'unità. A seconda della capacità di archiviazione e dei requisiti aziendali per i dati, potrebbe essere necessario aumentare o ridurre il periodo di conservazione predefinito degli snapshot ARP. Ad esempio, potrebbe essere necessario aumentare il periodo di conservazione per le applicazioni aziendali critiche in modo da avere, se necessario, periodi di conservazione più lunghi per il ripristino dei dati, oppure potrebbe essere necessario ridurre il periodo di conservazione per le applicazioni non critiche per risparmiare spazio di archiviazione.

Il periodo di conservazione predefinito per lo snapshot ARP varia a seconda dell'azione intrapresa in risposta all'attività anomala.

| Se intraprendi questa azione… | Per impostazione predefinita, gli snapshot ARP vengono conservati per… |
|---|---|
| Contrassegna come falso positivo | 12 ore |
| Contrassegna come potenziale attacco ransomware | 7 giorni |

| Se intraprendi questa azione… | Per impostazione predefinita, gli snapshot ARP vengono conservati per… |
|---|---|
| Non intraprendere azioni immediate | 10 giorni |

I periodi di conservazione predefiniti possono essere modificati utilizzando l'interfaccia della riga di comando (CLI) ONTAP . Vedere "Modifica le opzioni per gli snapshot automatici ONTAP" per conoscere i passaggi da seguire per modificare il periodo di conservazione predefinito.

# Rispondi alla protezione autonoma dal ransomware con avvisi AI sui sistemi di archiviazione ASA r2

Se la protezione autonoma dai ransomware con intelligenza artificiale (ARP/AI) rileva attività anomale su una o più unità di archiviazione del sistema ASA r2, viene generato un avviso nella dashboard di System Manager. È necessario visualizzare l'avviso, verificare l'attività e, se necessario, intervenire per bloccare qualsiasi potenziale minaccia ai dati.

Se viene visualizzato un messaggio di avviso ARP/AI, prima di intervenire è consigliabile utilizzare l'apposito strumento di controllo dell'integrità dell'applicazione per verificare l'integrità dei dati sull'unità di archiviazione. La verifica dell'integrità dei dati dell'unità di archiviazione aiuta a determinare se l'attività è accettabile o se si tratta di un potenziale attacco ransomware.

| Se l'attività anomala è … | Allora fai così… |
|---|---|
| Accettabile | Contrassegna l'attività come falso positivo. |
| Un potenziale attacco ransomware | Contrassegna l'attività come potenziale attacco ransomware. |
| Indeterminato | Non intervenire immediatamente. Monitorare l'unità di archiviazione fino a 7 giorni. Se l'unità di archiviazione continua a funzionare normalmente, contrassegnare l'attività come falso positivo. Se l'unità di archiviazione continua a presentare attività anomale, contrassegnare l'attività come potenziale attacco ransomware. |

**Fasi**

1. In System Manager, selezionare **Dashboard**.

   Se ARP ha rilevato un'attività anomala su una o più unità di archiviazione, viene visualizzato un messaggio in **Avvisi**.

2. Selezionare il messaggio di avviso.
3. In **Panoramica eventi**, seleziona il messaggio **Avvisi** che indica il numero di unità di archiviazione con attività anomala.
4. In **Unità di archiviazione con attività anomala**, seleziona l'unità di archiviazione.
5. Selezionare **Sicurezza**.

   Se si verifica un'attività anomala sull'unità di archiviazione, viene visualizzato un messaggio in **Anti-**

**ransomware**.

6. Seleziona **Scegli un'azione**.
7. Seleziona **Segnala come falso positivo** oppure **Segnala come potenziale attacco ransomware**.

**Quali sono le prossime novità?**

Se sei a conoscenza di picchi di attività nella tua unità di storage, che si tratti di picchi occasionali o di un picco tipico di una nuova normalità, dovresti segnalarli come sicuri. Segnalare manualmente questi picchi come sicuri aiuta a migliorare l'accuratezza delle valutazioni delle minacce di ARP. Scopri come "segnala picchi noti di ARP/AI".

# Metti in pausa o riprendi la protezione autonoma contro i ransomware con l'intelligenza artificiale sui tuoi sistemi di archiviazione ASA r2

A partire da ONTAP 9.17.1, è possibile utilizzare la protezione autonoma dai ransomware con intelligenza artificiale (ARP/AI) per proteggere i dati sul sistema ASA r2. Se si prevede un evento insolito relativo al carico di lavoro, è possibile sospendere temporaneamente l'analisi ARP/AI per prevenire rilevamenti di falsi positivi relativi ad attacchi ransomware. Al termine dell'evento, è possibile riprendere l'analisi ARP/AI.

## Pausa ARP/AI

Prima di iniziare un evento insolito del carico di lavoro, potrebbe essere necessario sospendere temporaneamente l'analisi ARP/AI per evitare rilevamenti falsi positivi di attacchi ransomware.

**Fasi**

1. In System Manager, selezionare **Storage**.
2. Seleziona le unità di archiviazione per le quali desideri mettere in pausa ARP/AI.
3. Seleziona **Sospendi anti-ransomware**.

**Risultato**

L'analisi ARP/AI viene sospesa per le unità di archiviazione selezionate e non ti verrà segnalata alcuna attività sospetta in System Manager finché non riprenderai ARP/AI.

## Riprendi ARP/AI

Se si mette in pausa ARP/AI durante un carico di lavoro insolito, è necessario riprenderlo una volta completato il carico di lavoro per proteggere i dati dagli attacchi ransomware.

**Fasi**

1. In System Manager, selezionare **Storage**.
2. Selezionare le unità di archiviazione per le quali si desidera riprendere ARP/AI.
3. Seleziona **Ripristina anti-ransomware**.

**Risultato**

L'analisi dei potenziali attacchi ransomware viene ripresa e le attività sospette vengono segnalate in Gestione sistema.

## Informazioni sul copyright



## Informazioni sul marchio commerciale