# Protezione ransomware autonoma

## ONTAP 9

NetApp
August 31, 2024

# Sommario

# Protezione ransomware autonoma

## Panoramica della protezione ransomware autonoma

A partire da ONTAP 9.10.1, la funzionalità di protezione ransomware autonoma (ARP) utilizza l'analisi del carico di lavoro in ambienti NAS (NFS e SMB) per rilevare e avvisare in modo proattivo circa attività anomale che potrebbero indicare un attacco ransomware.

Quando si sospetta un attacco, ARP crea anche nuove copie Snapshot, oltre alla protezione esistente dalle copie Snapshot pianificate.

### Licenze e abilitazione

ARP richiede una licenza. ARP è disponibile con "Licenza ONTAP ONE". Se non si dispone della licenza ONTAP ONE, sono disponibili altre licenze per l'utilizzo di ARP, che variano a seconda della versione di ONTAP in uso.

| Release di ONTAP | Licenza |
|---|---|
| ONTAP 9.11.1 e versioni successive | Anti_ransomware |
| ONTAP 9.10.1 | MT_EK_MGMT (Gestione delle chiavi multi-tenant) |

- Se si esegue l'aggiornamento a ONTAP 9.11.1 o versione successiva e ARP è già configurato nel sistema, non è necessario acquistare la nuova licenza Anti-ransomware. Per le nuove configurazioni ARP, è necessaria la nuova licenza.
- Se si esegue il ripristino da ONTAP 9.11.1 o versione successiva a ONTAP 9.10.1 e si attiva ARP con la licenza Anti-ransomware, viene visualizzato un messaggio di avviso e potrebbe essere necessario riconfigurare ARP. "Scopri come ripristinare ARP".

È possibile configurare ARP per volume utilizzando Gestione sistema o l'interfaccia CLI di ONTAP.

### Strategia di protezione ransomware di ONTAP

Una strategia efficace di rilevamento ransomware dovrebbe includere più di un singolo livello di protezione.

Un'analogia sarebbe la sicurezza di un veicolo. Non ci si affida a una singola funzione, ad esempio una cintura di sicurezza, per proteggersi completamente in caso di incidente. Gli airbag, i freni antibloccaggio e l'allarme anticollisione anteriore sono tutte funzioni di sicurezza aggiuntive che consentono di ottenere risultati migliori. La protezione ransomware deve essere visualizzata nello stesso modo.

Mentre ONTAP include funzionalità come FPolicy, Snapshot Copies, SnapLock e Active IQ Digital Advisor per la protezione dal ransomware, le seguenti informazioni si concentrano sulla funzionalità ARP on-box con funzionalità di machine learning.

Per ulteriori informazioni sulle altre funzionalità anti-ransomware di ONTAP, consulta "Ransomware e il portfolio di protezione di NetApp".

## Cosa rileva ARP

ARP è progettato per proteggere da attacchi di tipo Denial-of-service in cui l'utente malintenzionato trattiene i dati fino a quando non viene pagato un riscatto. ARP offre il rilevamento del ransomware in tempo reale basato su:

- Identificazione dei dati in entrata come crittografati o non crittografati.
- Analytics, che rileva
  - **Entropia**: Una valutazione della casualità dei dati in un file
  - **Tipi di estensione del file**: Un'estensione non conforme al normale tipo di estensione
  - **IOPS del file**: Aumento dell'attività anomala del volume con crittografia dei dati (a partire da ONTAP 9.11.1)

ARP è in grado di rilevare la diffusione della maggior parte degli attacchi ransomware dopo la crittografia di un numero limitato di file, intraprendere azioni automatiche per proteggere i dati e avvisare l'utente che si sta verificando un attacco sospetto.

> Nessun sistema di rilevamento ransomware o prevenzione può garantire completamente la sicurezza da un attacco ransomware. Anche se è possibile che un attacco possa non essere rilevato, ARP agisce come un importante livello di difesa aggiuntivo se il software antivirus non è riuscito a rilevare un'intrusione.

## Modalità di apprendimento e attive

ARP dispone di due modalità:

- **Apprendimento** (o modalità "dry run")
- **Attivo** (o modalità "abilitato")

Quando si attiva ARP, viene eseguito in *modalità di apprendimento*. In modalità di apprendimento, il sistema ONTAP sviluppa un profilo di avviso basato sulle aree di analisi: Entropia, tipi di estensione dei file e IOPS dei file. Dopo aver eseguito ARP in modalità di apprendimento per un tempo sufficiente a valutare le caratteristiche del carico di lavoro, è possibile passare alla modalità attiva e iniziare a proteggere i dati. Una volta che ARP è passato alla modalità attiva, ONTAP crea copie snapshot ARP per proteggere i dati se viene rilevata una minaccia.

Si consiglia di lasciare ARP in modalità di apprendimento per 30 giorni. A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch, che può verificarsi prima di 30 giorni.

In modalità attiva, se un'estensione del file è contrassegnata come anomala, è necessario valutare l'avviso. Puoi agire sull'avviso per proteggere i tuoi dati o contrassegnarlo come falso positivo. Se si contrassegna un avviso come falso positivo, il profilo di avviso viene aggiornato. Ad esempio, se l'avviso viene attivato da una nuova estensione di file e l'utente contrassegna l'avviso come falso positivo, non verrà visualizzato alcun avviso alla successiva visualizzazione dell'estensione del file. Il comando `security anti-ransomware volume workload-behavior show` mostra le estensioni di file rilevate nel volume. (Se si esegue questo comando nelle prime fasi della modalità di apprendimento e viene visualizzata una rappresentazione accurata dei tipi di file, non utilizzare tali dati come base per passare alla modalità attiva, poiché ONTAP sta ancora raccogliendo altre metriche).

A partire da ONTAP 9.11.1, è possibile personalizzare i parametri di rilevamento per ARP. Per ulteriori informazioni, vedere Gestire i parametri di rilevamento degli attacchi ARP.

## Valutazione delle minacce e copie snapshot ARP

In modalità attiva, ARP valuta la probabilità di minaccia in base ai dati in entrata misurati in base alle analisi apprese. Viene assegnata una misurazione quando ARP rileva una minaccia:

- **Basso**: Il primo rilevamento di un'anomalia nel volume (ad esempio, una nuova estensione del file è osservata nel volume).
- **Moderato**: Si osservano più file con la stessa estensione mai vista prima.
  - In ONTAP 9.10.1, la soglia per l'escalation a moderate è di 100 o più file. A partire da ONTAP 9.11.1, è possibile modificare la quantità di file; il valore predefinito è 20.

In una situazione di basso rischio, ONTAP rileva un'anomalia e crea una copia Snapshot del volume per creare il punto di recovery migliore. ONTAP anticipa il nome della copia snapshot ARP con `Anti-ransomware-backup` per renderla facilmente identificabile, per esempio `Anti_ransomware_backup.2022-12-20_1248`.

Dopo che ONTAP ha eseguito un report di analytics, la minaccia passa a moderata. Ciò determina se l'anomalia corrisponde a un profilo ransomware. Le minacce che rimangono a basso livello sono registrate e visibili nella sezione **Eventi** di System Manager. Quando la probabilità di attacco è moderata, ONTAP genera una notifica EMS che richiede di valutare la minaccia. ONTAP non invia avvisi relativi a minacce basse, tuttavia, a partire da ONTAP 9.14.1, è possibile modificare le impostazioni degli avvisi. Per ulteriori informazioni, vedere Rispondere ad attività anomale.

È possibile visualizzare informazioni su una minaccia, indipendentemente dal livello, nella sezione **Eventi** di System Manager o con `security anti-ransomware volume show` comando.

Le copie Snapshot ARP vengono conservate per un minimo di due giorni. A partire da ONTAP 9.11.1, è possibile modificare le impostazioni di conservazione. Per ulteriori informazioni, vedere Modificare le opzioni per le copie Snapshot.

## Come ripristinare i dati in ONTAP dopo un attacco ransomware

Quando si sospetta un attacco, il sistema esegue una copia Snapshot del volume in quel momento e blocca tale copia. Se l'attacco viene confermato in seguito, il volume può essere ripristinato utilizzando la copia snapshot ARP.

Le copie Snapshot bloccate non possono essere eliminate con mezzi normali. Tuttavia, se in seguito decidi di contrassegnare l'attacco come falso positivo, la copia bloccata verrà eliminata.

Conoscendo i file interessati e il momento dell'attacco, è possibile recuperare in modo selettivo i file interessati da varie copie Snapshot, piuttosto che semplicemente riportare l'intero volume in una delle copie Snapshot.

ARP si basa quindi sulla comprovata tecnologia di protezione dei dati e disaster recovery di ONTAP per rispondere agli attacchi ransomware. Per ulteriori informazioni sul ripristino dei dati, consultare i seguenti argomenti.

- "Ripristino da copie Snapshot (System Manager)"
- "Ripristino dei file da copie Snapshot (CLI)"
- "Ripristino ransomware intelligente"

# Casi di utilizzo e considerazioni sulla protezione ransomware autonoma

La protezione autonoma ransomwware (ARP) è disponibile per i carichi di lavoro NAS a partire da ONTAP 9.10.1. Prima di distribuire ARP, è necessario conoscere gli utilizzi consigliati e le configurazioni supportate, nonché le implicazioni in termini di prestazioni.

## Configurazioni supportate e non supportate

Quando si decide di utilizzare l'ARP, è importante assicurarsi che il carico di lavoro del volume sia adatto all'ARP e che soddisfi le configurazioni di sistema richieste.

### Carichi di lavoro adatti

ARP è adatto per:

- Database sullo storage NFS
- Home directory Windows o Linux

  Poiché gli utenti potrebbero creare file con estensioni che non sono state rilevate durante il periodo di apprendimento, esiste una maggiore possibilità di falsi positivi in questo carico di lavoro.

- Immagini e video

  Ad esempio, le cartelle cliniche e i dati EDA (Electronic Design Automation)

### Carichi di lavoro non adatti

ARP non è adatto per:

- Carichi di lavoro con un'elevata frequenza di creazione o eliminazione di file (centinaia di migliaia di file in pochi secondi, ad esempio workload di test/sviluppo).
- Il rilevamento delle minacce di ARP dipende dalla sua capacità di riconoscere un aumento insolito delle attività di creazione, ridenominazione o eliminazione dei file. Se l'applicazione stessa è l'origine dell'attività del file, non è possibile distinguerla in modo efficace dall'attività ransomware.
- Carichi di lavoro in cui l'applicazione o l'host crittografa i dati.
  ARP dipende dalla distinzione dei dati in entrata come crittografati o non crittografati. Se l'applicazione stessa sta crittografando i dati, l'efficacia della funzione viene ridotta. Tuttavia, la funzionalità può ancora funzionare in base all'attività del file (eliminazione, sovrascrittura o creazione, creazione o ridenominazione con una nuova estensione del file) e al tipo di file.

### Configurazioni supportate

ARP è disponibile per i volumi NFS e SMB nei sistemi ONTAP on-premise a partire da ONTAP 9.10.1.

Il supporto per altre configurazioni e tipi di volume è disponibile nelle seguenti versioni di ONTAP:

| | ONTAP 9.15.1 | ONTAP 9.14.1 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 | ONTAP 9.10.1 |
|---|---|---|---|---|---|---|
| Volumi protetti con SnapMirror asincrono | ✓ | ✓ | ✓ | ✓ | | |
| SVM protette con SnapMirror asincrono (disaster recovery SVM) | ✓ | ✓ | ✓ | ✓ | | |
| Mobilità dei dati SVM (`vserver migrate`) | ✓ | ✓ | ✓ | ✓ | | |
| Volumi FlexGroup | ✓ | ✓ | ✓ | | | |
| Verifica multi-admin | ✓ | ✓ | ✓ | | | |

#### Interoperabilità di SnapMirror e ARP

A partire da ONTAP 9.12.1, ARP è supportato sui volumi di destinazione asincroni di SnapMirror. ARP è **non** supportato con SnapMirror Synchronous.

Se un volume di origine SnapMirror è abilitato per ARP, il volume di destinazione SnapMirror acquisisce automaticamente lo stato di configurazione ARP (apprendimento, abilitato, ecc.), i dati di training ARP e l'istantanea creata da ARP del volume di origine. Non è richiesta alcuna abilitazione esplicita.

Mentre il volume di destinazione è costituito da copie Snapshot di sola lettura (RO), non viene eseguita alcuna elaborazione ARP sui dati. Tuttavia, quando il volume di destinazione di SnapMirror viene convertito in lettura/scrittura (RW), ARP viene attivato automaticamente sul volume di destinazione convertito in RW. Il volume di destinazione non richiede ulteriori procedure di apprendimento oltre a quelle già registrate nel volume di origine.

In ONTAP 9.10.1 e 9.11.1, SnapMirror non trasferisce lo stato di configurazione ARP, i dati di training e le copie Snapshot dai volumi di origine a quelli di destinazione. Quindi, quando il volume di destinazione SnapMirror viene convertito in RW, ARP sul volume di destinazione deve essere esplicitamente abilitato in modalità di apprendimento dopo la conversione.

#### ARP e macchine virtuali

ARP è supportato con macchine virtuali (VM). Il rilevamento ARP si comporta in modo diverso per le modifiche all'interno e all'esterno della VM. L'ARP non è consigliato per i carichi di lavoro con file ad entropia elevata all'interno della VM.

**Modifiche esterne alla macchina virtuale**

ARP può rilevare le modifiche all'estensione di un file su un volume NFS esterno alla VM se una nuova estensione entra nel volume crittografato o se cambia l'estensione di un file. Le modifiche all'estensione dei file rilevabili sono:

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

**Modifiche all'interno della VM**

Se l'attacco ransomware riguarda la macchina virtuale e i file all'interno della macchina virtuale vengono alterati senza apportare modifiche all'esterno della macchina virtuale, ARP rileva la minaccia se l'entropia predefinita della macchina virtuale è bassa (ad esempio file .txt, .docx o .mp4). Anche se ARP crea un'istantanea di protezione in questo scenario, non genera un avviso di minaccia perché le estensioni di file esterne alla VM non sono state manomesse.

Se, per impostazione predefinita, i file sono ad entropia elevata (ad esempio file .gzip o protetti da password), le funzionalità di rilevamento di ARP sono limitate. ARP può comunque acquisire istantanee proattive in questo caso; tuttavia, non verrà attivato alcun avviso se le estensioni dei file non sono state manomesse esternamente.

### Configurazioni non supportate

ARP non è supportato nelle seguenti configurazioni di sistema:

- Ambienti ONTAP S3
- Ambienti SAN

ARP non supporta le seguenti configurazioni di volume:

- Volumi FlexGroup (in ONTAP da 9.10.1 a 9.12.1. A partire da ONTAP 9.13.1, sono supportati i volumi FlexGroup)
- FlexCache Volumes (ARP supportato sui volumi FlexVol di origine ma non sui volumi cache)
- Volumi offline
- Volumi solo SAN
- Volumi SnapLock
- SnapMirror sincrono
- SnapMirror asincrono (non supportato solo in ONTAP 9.10.1 e 9.11.1. SnapMirror asincrono è supportato a partire da ONTAP 9.12.1. Per ulteriori informazioni, vedere [snapmirror].)
- Volumi limitati
- Volumi root di storage VM

- Volumi di VM storage interrotte

## Considerazioni sulle performance e sulla frequenza ARP

ARP può avere un impatto minimo sulle prestazioni del sistema, misurato in termini di throughput e IOPS di picco. L'impatto della funzionalità ARP dipende dai carichi di lavoro dei volumi specifici. Per i carichi di lavoro comuni, si consigliano i seguenti limiti di configurazione:

| Caratteristiche del carico di lavoro | Limite di volume consigliato per nodo | Peggioramento delle performance con superamento del limite di volume per nodo:[*] |
|---|---|---|
| I dati possono essere compressi o a uso intensivo di lettura. | 150 | 4% degli IOPS massimi |
| I dati non possono essere compressi con un utilizzo intensivo di scrittura. | 60 | 10% degli IOPS massimi |

Superato:[*] le performance di sistema non vengono degradate oltre queste percentuali, indipendentemente dal numero di volumi aggiunti in eccesso rispetto ai limiti raccomandati.

Poiché gli analytics ARP vengono eseguiti in una sequenza con priorità, con l'aumentare del numero di volumi protetti, gli analytics vengono eseguiti su ciascun volume con minore frequenza.

## Verifica multi-admin con volumi protetti con ARP

A partire da ONTAP 9.13.1, è possibile attivare la verifica multi-admin (MAV) per una maggiore sicurezza con ARP. MAV garantisce che almeno due o più amministratori autenticati siano tenuti a disattivare ARP, sospendere ARP o contrassegnare un attacco sospetto come falso positivo su un volume protetto. Scopri come "Abilitare MAV per volumi protetti da ARP".

È necessario definire gli amministratori per un gruppo MAV e creare regole MAV per `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, e. `security anti-ransomware volume attack clear-suspect` Comandi ARP che si desidera proteggere. Ogni amministratore del gruppo MAV deve approvare ogni nuova richiesta di regola e. "Aggiungere nuovamente la regola MAV" Nelle impostazioni MAV.

A partire da ONTAP 9.14.1, ARP offre avvisi per la creazione di un'istantanea ARP e per l'osservazione di una nuova estensione di file. Gli avvisi per questi eventi sono disattivati per impostazione predefinita. Gli avvisi possono essere impostati a livello di volume o SVM. È possibile creare regole MAV a livello SVM utilizzando `security anti-ransomware vserver event-log modify` o al livello del volume con `security anti-ransomware volume event-log modify`.

**Passi successivi**

- "Attiva la protezione ransomware autonoma"
- "Abilita MAV per volumi protetti da ARP"

# Attiva la protezione ransomware autonoma

A partire da ONTAP 9.10.1, è possibile attivare la protezione ransomware autonoma (ARP) su volumi nuovi o esistenti. Per prima cosa, si attiva ARP in modalità di apprendimento, in cui il sistema analizza il carico di lavoro per caratterizzare il

comportamento normale. È possibile attivare ARP su un volume esistente oppure creare un nuovo volume e attivare ARP dall'inizio.

**A proposito di questa attività**

Si dovrebbe sempre abilitare ARP inizialmente in modalità di apprendimento (o dry-run). L'avvio in modalità attiva può causare un numero eccessivo di falsi positivi.

Si consiglia di far funzionare ARP in modalità di apprendimento per un minimo di 30 giorni. A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch, che può verificarsi prima di 30 giorni. Per ulteriori informazioni, vedere "Modalità di apprendimento e attive".

> Nei volumi esistenti, l'apprendimento e le modalità attive si applicano solo ai dati scritti di recente, non ai dati già esistenti nel volume. I dati esistenti non vengono sottoposti a scansione e analizzati, poiché le caratteristiche del traffico dati normale precedente vengono assunte in base ai nuovi dati dopo che il volume è stato abilitato per ARP.

**Prima di iniziare**

- Devi avere una macchina virtuale per lo storage (SVM) abilitata per NFS o SMB (o entrambi).
- Il licenza corretta Deve essere installato per la versione di ONTAP in uso.
- È necessario disporre di un carico di lavoro NAS con i client configurati.
- Il volume che si desidera impostare ARP deve essere protetto e deve avere un attivo "percorso di giunzione".
- Il volume deve essere pieno al di sotto del 100%.
- Si consiglia di configurare il sistema EMS per l'invio di notifiche e-mail, che includano avvisi relativi all'attività ARP. Per ulteriori informazioni, vedere "Configurare gli eventi EMS per l'invio di notifiche e-mail".
- A partire da ONTAP 9.13.1, si consiglia di attivare la verifica multi-admin (MAV) in modo che siano necessari due o più amministratori utente autenticati per la configurazione ARP (Autonomous ransomware Protection). Per ulteriori informazioni, vedere "Attiva la verifica multi-admin".

## Enable ARP (attiva ARP)

È possibile attivare ARP utilizzando Gestione di sistema o l'interfaccia CLI di ONTAP.

**System Manager**

**Fasi**

1. Selezionare **Storage > Volumes** (archiviazione > volumi), quindi selezionare il volume che si desidera proteggere.
2. Nella scheda **Security** della panoramica **Volumes**, selezionare **Status** per passare da Disabled (Disattivato) a Enabled (attivato) in Learning-mode (modalità apprendimento) nella casella **Anti-ransomware**.
3. Al termine del periodo di apprendimento, impostare ARP in modalità attiva.

   > A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch. È possibile "Disattivare questa impostazione sulla VM di storage associata" se si desidera controllare manualmente la modalità di apprendimento in modalità attiva, passare alla modalità attiva.

   a. Selezionare **Storage > Volumes** (archiviazione > volumi), quindi selezionare il volume pronto per la modalità attiva.
   b. Nella scheda **Security** della panoramica **Volumes**, selezionare **Switch** to Active mode nella casella Anti-ransomware.
4. È possibile verificare lo stato ARP del volume nella casella **Anti-ransomware**.

   Per visualizzare lo stato ARP per tutti i volumi: Nel riquadro **Volumes** (volumi), selezionare **Show/Hide** (Mostra/Nascondi), quindi assicurarsi che sia selezionato lo stato **Anti-ransomware**.

**CLI**

Il processo di abilitazione dell'ARP con la CLI differisce se lo si attiva su un volume esistente rispetto a un nuovo volume.

**Attivare ARP su un volume esistente**

1. Modificare un volume esistente per abilitare la protezione ransomware in modalità di apprendimento:

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

   Se si esegue ONTAP 9.13.1 o versione successiva, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera che questo comportamento venga attivato automaticamente, modificare l'impostazione a livello di SVM su tutti i volumi associati:

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

2. Al termine del periodo di apprendimento, modificare il volume protetto per passare alla modalità attiva, se non è già stato eseguito automaticamente:

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

   È anche possibile passare alla modalità attiva con il comando modify volume:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Verificare lo stato ARP del volume.

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

**Abilitare ARP su un nuovo volume**

1. Creare un nuovo volume con la protezione anti-ransomware abilitata prima del provisioning dei dati.

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

   Se si esegue ONTAP 9.13.1 o versione successiva, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera che questo comportamento venga attivato automaticamente, modificare l'impostazione a livello di SVM su tutti i volumi associati:

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

2. Al termine del periodo di apprendimento, modificare il volume protetto per passare alla modalità attiva, se non è già stato eseguito automaticamente:

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

   È anche possibile passare alla modalità attiva con il comando modify volume:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Verificare lo stato ARP del volume.

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

# Attiva la protezione ransomware autonoma per impostazione predefinita nei nuovi volumi

A partire da ONTAP 9.10.1, è possibile configurare le VM di storage in modo che i nuovi volumi siano attivati per impostazione predefinita per la protezione ransomware autonoma (ARP) in modalità di apprendimento.

**A proposito di questa attività**

Per impostazione predefinita, i nuovi volumi vengono creati con ARP in modalità disattivata. È possibile modificare questa impostazione in System Manager e con l'interfaccia CLI. I volumi abilitati per impostazione predefinita sono impostati su ARP in modalità di apprendimento (o dry-run).

ARP viene attivato solo sui volumi creati in SVM dopo aver modificato l'impostazione. ARP non verrà abilitato sui volumi esistenti. Scopri come "Abilitare ARP in un volume esistente".

A partire da ONTAP 9.13.1, l'apprendimento adattivo è stato aggiunto agli analytics ARP e il passaggio dalla modalità di apprendimento alla modalità attiva viene eseguito automaticamente. Per ulteriori informazioni, vedere "Modalità di apprendimento e attive".

**Prima di iniziare**

- Il licenza corretta Deve essere installato per la versione di ONTAP in uso.
- Il volume deve essere pieno al di sotto del 100%.
- I percorsi di giunzione devono essere attivi.
- A partire da ONTAP 9.13.1, si consiglia di attivare la verifica multi-admin (MAV) in modo che siano necessari due o più amministratori utente autenticati per le operazioni anti-ransomware. "Scopri di più".

**Passare dalla modalità di apprendimento alla modalità attiva**

A partire da ONTAP 9.13.1, l'apprendimento adattivo è stato aggiunto all'analisi ARP. Il passaggio dalla modalità di apprendimento alla modalità attiva viene eseguito automaticamente. La decisione autonoma di ARP di passare automaticamente dalla modalità di apprendimento alla modalità attiva si basa sulle impostazioni di configurazione delle seguenti opzioni:

```
-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
```

Dopo 30 giorni di apprendimento, un volume passa automaticamente alla modalità attiva anche se una o più di queste condizioni non sono soddisfatte. In altre parole, se la funzione di commutazione automatica è attivata, il volume passa alla modalità attiva dopo un massimo di 30 giorni. Il valore massimo di 30 giorni è fisso e non modificabile.

Per ulteriori informazioni sulle opzioni di configurazione ARP, compresi i valori predefiniti, consultare la "Riferimento al comando ONTAP".

**Fasi**

È possibile utilizzare Gestione di sistema o la CLI di ONTAP per attivare ARP per impostazione predefinita.

**System Manager**

1. Selezionare **Storage > Storage VM** (Storage VM > Storage VM), quindi selezionare la VM di storage contenente i volumi che si desidera proteggere con ARP.
2. Selezionare la scheda **Impostazioni**. In **sicurezza**, individuare il riquadro **Anti-ransomware**, quindi selezionare
3. Selezionare la casella per abilitare ARP per volumi NAS. Selezionare la casella aggiuntiva per abilitare ARP su tutti i volumi NAS idonei nella VM di storage.

> Se è stato eseguito l'aggiornamento a ONTAP 9.13.1, l'impostazione **passa automaticamente dalla modalità di apprendimento alla modalità attiva dopo un apprendimento sufficiente** viene attivata automaticamente. Ciò consente ad ARP di determinare l'intervallo ottimale del periodo di apprendimento e di automatizzare il passaggio alla modalità attiva. Disattivare l'impostazione se si desidera passare manualmente alla modalità attiva.

**CLI**

1. Modificare una SVM esistente per attivare ARP per impostazione predefinita nei nuovi volumi:
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   Nella CLI, è anche possibile creare una nuova SVM con ARP attivato per impostazione predefinita per i nuovi volumi.
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

   Se è stato eseguito l'aggiornamento a ONTAP 9.13.1 o versioni successive, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera attivare automaticamente questo comportamento, utilizzare il seguente comando:

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

# Sospendere la protezione ransomware autonoma per escludere gli eventi dei workload dall'analisi

Se si prevedono eventi insoliti relativi ai carichi di lavoro, è possibile sospendere temporaneamente e riprendere l'analisi ARP (Autonomous ransomware Protection) in qualsiasi momento.

A partire da ONTAP 9.13.1, è possibile attivare la verifica multi-admin (MAV) in modo che due o più amministratori utente autenticati siano necessari per mettere in pausa l'ARP. "Scopri di più".

**A proposito di questa attività**

Durante una pausa ARP, non vengono registrati eventi né vengono eseguite azioni per nuove scritture. Tuttavia, l'operazione di analisi continua per i log precedenti in background.

Non utilizzare la funzione di disattivazione ARP per mettere in pausa gli analytics. In questo modo si disattiva l'ARP sul volume e tutte le informazioni esistenti sul comportamento dei carichi di lavoro appresi vengono perse. Ciò richiederebbe un riavvio del periodo di apprendimento.

**Fasi**

È possibile utilizzare Gestione di sistema o la CLI di ONTAP per sospendere ARP.

**System Manager**

1. Selezionare **Storage > Volumes** (archiviazione > volumi*), quindi selezionare il volume in cui si desidera sospendere l'ARP.
2. Nella scheda **sicurezza** della panoramica dei volumi, seleziona **Pausa anti-ransomware** nella casella **Anti-ransomware**.

> A partire da ONTAP 9.13.1, se si utilizza MAV per proteggere le impostazioni ARP, l'operazione di pausa richiede di ottenere l'approvazione di uno o più amministratori aggiuntivi. "L'approvazione deve essere ricevuta da tutti gli amministratori" Associato al gruppo di approvazione MAV o l'operazione non riuscirà.

**CLI**

1. Pausa ARP su un volume:

   `security anti-ransomware volume pause -vserver` *`svm_name`* `-volume` *`vol_name`*

2. Per riprendere l'elaborazione, utilizzare `resume` comando:

   `security anti-ransomware volume resume -vserver` *`svm_name`* `-volume` *`vol_name`*

3. **Se si utilizza MAV (disponibile con ARP che inizia con ONTAP 9.13.1) per proteggere le impostazioni ARP,** l'operazione di pausa richiede l'approvazione di uno o più amministratori aggiuntivi. L'approvazione deve essere ricevuta da tutti gli amministratori associati al gruppo di approvazione MAV, altrimenti l'operazione non avrà esito positivo.

   Se si utilizza MAV e un'operazione di pausa prevista richiede ulteriori approvazioni, ciascun responsabile dell'approvazione del gruppo MAV esegue le seguenti operazioni:

   a. Mostra la richiesta:

      `security multi-admin-verify request show`

   b. Approvare la richiesta:

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

      La risposta dell'ultimo responsabile dell'approvazione del gruppo indica che il volume è stato modificato e che lo stato di ARP è in pausa.

      Se si utilizza MAV e si è un responsabile dell'approvazione del gruppo MAV, è possibile rifiutare una richiesta di operazione di pausa:

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

# Gestire i parametri di rilevamento degli attacchi tramite protezione autonoma dal ransomware

A partire da ONTAP 9.11.1, puoi modificare i parametri per il rilevamento del ransomware su un volume abilitato alla protezione autonoma contro il ransomware specifico e segnalare un picco noto come normale attività dei file. La regolazione dei parametri di rilevamento consente di migliorare l'accuratezza dei rapporti in base al carico di lavoro del volume specifico.

## Come funziona il rilevamento degli attacchi

Quando la protezione autonoma da ransomware (ARP) è in modalità di apprendimento, sviluppa valori di base per i comportamenti di volume. Si tratta di entropia, estensioni dei file e, a partire da ONTAP 9.11.1, IOPS. Queste baseline vengono utilizzate per valutare le minacce ransomware. Per ulteriori informazioni su questi criteri, vedere Cosa rileva ARP.

In ONTAP 9.10.1, ARP genera un avviso se rileva entrambe le seguenti condizioni:

- più di 20 file con estensioni non precedentemente osservate nel volume
- elevati dati di entropia

A partire da ONTAP 9.11.1, ARP emette un avviso di minaccia se *solo* viene soddisfatta una condizione. Ad esempio, se si osservano più di 20 file con estensioni che non sono state precedentemente osservate nel volume entro un periodo di 24 ore, ARP lo classificherà come una minaccia *indipendentemente* dall'entropia osservata. (I valori dei file 24 ore e 20 sono predefiniti, che possono essere modificati).

A partire da ONTAP 9.14.1, è possibile configurare gli avvisi quando ARP osserva una nuova estensione di file e quando ARP crea un'istantanea. Per ulteriori informazioni, vedere [modify-alerts]

Alcuni volumi e carichi di lavoro richiedono parametri di rilevamento diversi. Ad esempio, il volume abilitato per ARP può ospitare numerosi tipi di estensioni di file, nel qual caso è possibile modificare il conteggio delle soglie per le estensioni di file mai viste prima a un numero maggiore del valore predefinito di 20 o disattivare gli avvisi in base alle estensioni di file mai viste prima. A partire da ONTAP 9.11.1, puoi modificare i parametri di rilevamento degli attacchi per adattarli meglio ai tuoi carichi di lavoro specifici.

## Modificare i parametri di rilevamento degli attacchi

A seconda dei comportamenti previsti del volume abilitato per ARP, è possibile modificare i parametri di rilevamento degli attacchi.

**Fasi**

1. Visualizzare i parametri di rilevamento degli attacchi esistenti:

   ```
   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. Tutti i campi visualizzati sono modificabili con valori booleani o interi. Per modificare un campo, utilizzare `security anti-ransomware volume attack-detection-parameters modify` comando.

   Per un elenco completo dei parametri, vedere "Riferimento al comando ONTAP".

## Segnalare le sovratensioni note

ARP continua a modificare i valori di base per i parametri di rilevamento anche in modalità attiva. Se conoscete i picchi nella vostra attività di volume—o un aumento una volta o un aumento che è caratteristica di una nuova normale—dovreste segnalarlo come sicuro. La segnalazione manuale di questi picchi come sicuri aiuta a migliorare l'accuratezza delle valutazioni delle minacce di ARP.

#### Segnalare un aumento di una tantum

1. Se in circostanze note si verifica un picco una tantum e si desidera che ARP segnali un aumento simile in circostanze future, eliminare il picco dal comportamento del carico di lavoro:

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

#### Modificare il picco della linea di base

1. Se un picco segnalato deve essere considerato un normale comportamento dell'applicazione, riportare il picco in quanto tale per modificare il valore di picco della linea di base.

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

## Configurare gli avvisi ARP

A partire da ONTAP 9.14.1, ARP consente di specificare gli avvisi per due eventi ARP:

- Osservazione della nuova estensione di un file su un volume
- Creazione di un'istantanea ARP

È possibile impostare avvisi per questi due eventi su singoli volumi o per l'intera SVM. Se abiliti gli avvisi per la SVM, le impostazioni degli avvisi vengono ereditate solo dai volumi creati in seguito all'attivazione della funzione di avviso. Per impostazione predefinita, gli avvisi non sono attivati su alcun volume.

Gli avvisi di eventi possono essere controllati con verifica multi-admin. Per ulteriori informazioni, vedere Verifica multi-admin con volumi protetti con ARP.

**System Manager**

**Impostare gli avvisi per un volume**

1. Passare a **volumi**. Selezionare il singolo volume per il quale si desidera modificare le impostazioni.
2. Selezionare la scheda **sicurezza**, quindi **Impostazioni protezione eventi**.
3. Per ricevere avvisi relativi a **Nuova estensione rilevata** e **istantanea ransomware creata**, selezionare il menu a discesa sotto l'intestazione **gravità**. Modificare l'impostazione da **non generare evento** a **Avviso**.
4. Selezionare **Salva**.

**Impostare gli avvisi per una SVM**

1. Accedere a **Storage VM** quindi selezionare la SVM per la quale si desidera abilitare le impostazioni.
2. Sotto l'intestazione **sicurezza**, individuare la scheda **Anti-ransomware**. Selezionare ⋮ quindi **Modifica gravità evento ransomware**.
3. Per ricevere avvisi relativi a **Nuova estensione rilevata** e **istantanea ransomware creata**, selezionare il menu a discesa sotto l'intestazione **gravità**. Modificare l'impostazione da **non generare evento** a **Avviso**.
4. Selezionare **Salva**.

**CLI**

**Impostare gli avvisi per un volume**

- Per impostare gli avvisi per una nuova estensione file:

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

- Per impostare gli avvisi per la creazione di un'istantanea ARP:

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

- Confermare le impostazioni con `anti-ransomware volume event-log show` comando.

**Impostare gli avvisi per una SVM**

- Per impostare gli avvisi per una nuova estensione file:

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

- Per impostare gli avvisi per la creazione di un'istantanea ARP:

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

- Confermare le impostazioni con `security anti-ransomware vserver event-log show` comando.

**Ulteriori informazioni**

- "Comprendere gli attacchi di protezione autonoma da ransomware e lo snapshot di protezione autonoma da ransomware"

# Rispondere ad attività anomale

Quando la protezione ransomware autonoma (ARP) rileva attività anomale in un volume protetto, emette un avviso. È necessario valutare la notifica per determinare se l'attività è accettabile (falso positivo) o se un attacco sembra dannoso.

**A proposito di questa attività**

ARP visualizza un elenco di file sospetti quando rileva una combinazione di elevata entropia dei dati, attività anomale del volume con crittografia dei dati e estensioni di file insolite.

Quando viene emesso l'avviso, rispondere designando l'attività del file in uno dei due modi seguenti:

- **Falso positivo**

  Il tipo di file identificato è previsto nel carico di lavoro e può essere ignorato.

- **Potenziale attacco ransomware**

  Il tipo di file identificato non è previsto nel carico di lavoro e deve essere trattato come un potenziale attacco.

In entrambi i casi, il normale monitoraggio riprende dopo l'aggiornamento e la cancellazione degli avvisi. ARP registra la valutazione nel profilo di valutazione delle minacce, utilizzando la scelta dell'utente per monitorare le attività successive dei file.

In caso di attacco sospetto, è necessario determinare se si tratta di un attacco, rispondere al caso in cui si tratti e ripristinare i dati protetti prima di cancellare le notifiche. "Scopri di più su come eseguire il ripristino da un attacco ransomware".

Se si ripristina un intero volume, non vi sono avvisi da cancellare.

**Prima di iniziare**

ARP deve essere in esecuzione in modalità attiva.

**Fasi**

È possibile utilizzare Gestione sistema o l'interfaccia CLI di ONTAP per rispondere a un'attività anomala.

**System Manager**

1. Quando si riceve una notifica di "attività anomala", seguire il collegamento. In alternativa, accedere alla scheda **sicurezza** della panoramica **volumi**.

   Gli avvisi vengono visualizzati nel riquadro **Panoramica** del menu **Eventi**.

2. Quando viene visualizzato il messaggio "rilevata attività anomala del volume", visualizzare i file sospetti.

   Nella scheda **protezione**, selezionare **Visualizza tipi di file sospetti**.

3. Nella finestra di dialogo **tipi di file sospetti**, esaminare ciascun tipo di file e contrassegnarlo come "falso positivo" o "potenziale attacco ransomware".

| Se si seleziona questo valore… | Eseguire questa azione… |
|---|---|
| Falso positivo | Selezionare **Aggiorna** e **Cancella tipi di file sospetti** per registrare la decisione e riprendere il normale monitoraggio ARP.<br><br>A partire da ONTAP 9.13.1, se si utilizza MAV per proteggere le impostazioni ARP, l'operazione che si sospetta venga richiesta l'approvazione di uno o più amministratori aggiuntivi. "L'approvazione deve essere ricevuta da tutti gli amministratori" Associato al gruppo di approvazione MAV o l'operazione non riuscirà. |
| Potenziale attacco ransomware | Rispondere all'attacco e ripristinare i dati protetti. Quindi selezionare **Aggiorna** e **Cancella tipi di file sospetti** per registrare la decisione e riprendere il normale monitoraggio ARP.<br>Non esistono tipi di file sospetti da eliminare se è stato ripristinato un intero volume. |

**CLI**

1. Quando ricevi una notifica di un attacco ransomware sospetto, verifica l'ora e la gravità dell'attacco:

   `security anti-ransomware volume show -vserver` *`svm_name`* `-volume` *`vol_name`*

   Output di esempio:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

   È inoltre possibile controllare i messaggi EMS:

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

2. Generare un report sugli attacchi e prendere nota della posizione di output:

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

   Output di esempio:

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

3. Visualizzare il report su un sistema client di amministrazione. Ad esempio:

   ```
   [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. Eseguire una delle seguenti operazioni in base alla valutazione delle estensioni dei file:

   - Falso positivo

     Immettere il seguente comando per registrare la decisione, aggiungere il nuovo interno all'elenco di quelli consentiti e riprendere il normale monitoraggio anti-ransomware:
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

     Per identificare gli interni, utilizzare uno dei seguenti parametri:
     `[-seq-no integer]` Numero di sequenza del file nell'elenco dei file sospetti.
     `[-extension text, … ]` Estensioni di file
     `[-start-time date_time -end-time date_time]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".

   - Potenziale attacco ransomware

     Rispondere all'attacco e. "Recuperare i dati dallo snapshot di backup creato da ARP". Una volta ripristinati i dati, immettere il seguente comando per registrare la decisione e riprendere il normale monitoraggio ARP:

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

     Per identificare gli interni, utilizzare uno dei seguenti parametri:
     `[-seq-no integer]` Numero di sequenza del file nell'elenco dei file sospetti
     `[-extension text, … ]` Estensione del file
     `[-start-time date_time -end-time date_time]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".

Non esistono tipi di file sospetti da eliminare se è stato ripristinato un intero volume. Lo snapshot di backup creato da ARP verrà rimosso e il report dell'attacco verrà cancellato.

5. Se si sta utilizzando MAV e un previsto `clear-suspect` L'operazione richiede ulteriori approvazioni, ogni responsabile dell'approvazione del gruppo MAV deve:

   a. Mostra la richiesta:

      `security multi-admin-verify request show`

   b. Approvare la richiesta di riprendere il normale monitoraggio anti-ransomware:

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

   La risposta dell'ultimo responsabile dell'approvazione del gruppo indica che il volume è stato modificato e che viene registrato un falso positivo.

6. Se si utilizza MAV e si è un responsabile dell'approvazione del gruppo MAV, è anche possibile rifiutare una richiesta con un sospetto chiaro:

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

**Ulteriori informazioni**

- "KB: Comprendere gli attacchi di protezione ransomware autonoma e lo snapshot di protezione ransomware autonoma".

# Ripristinare i dati dopo un attacco ransomware

La protezione autonoma dal ransomware (ARP) crea copie Snapshot denominate `Anti_ransomware_backup` quando rileva una potenziale minaccia ransomware. È possibile utilizzare una di queste copie snapshot ARP o un'altra copia Snapshot del volume per ripristinare i dati.

**A proposito di questa attività**

Se il volume presenta relazioni SnapMirror, replicare manualmente tutte le copie mirror del volume immediatamente dopo il ripristino da una copia Snapshot. In caso contrario, le copie mirror non possono essere utilizzabili e devono essere eliminate e ricreate.

Per eseguire il ripristino da uno Snapshot diverso da `Anti_ransomware_backup` Snapshot dopo aver identificato un attacco di sistema, è necessario prima rilasciare lo snapshot ARP.

Se non è stato segnalato alcun attacco al sistema, è necessario prima eseguire il ripristino da `Anti_ransomware_backup` La copia Snapshot, quindi, completa un successivo ripristino del volume dalla copia Snapshot scelta.

**Fasi**

Per ripristinare i dati, è possibile utilizzare Gestione di sistema o l'interfaccia utente di ONTAP.

**System Manager**

**Ripristino dopo un attacco di sistema**

1. Per eseguire il ripristino dall'istantanea ARP, passare direttamente al punto 2. Per eseguire il ripristino da una copia Snapshot precedente, è necessario prima rilasciare il blocco sull'istantanea ARP.
   a. Selezionare **Storage > Volumes** (Storage > volumi).
   b. Selezionare **sicurezza**, quindi **Visualizza tipi di file sospetti**
   c. Contrassegnare i file come "False Positive" (Falso positivo).
   d. Selezionare **Aggiorna** e **Cancella tipi di file sospetti**
2. Visualizzare le copie Snapshot nei volumi:

   Selezionare **archiviazione > volumi**, quindi selezionare il volume e **Snapshot Copies**.
3. Selezionare ⋮ accanto alla copia istantanea che si desidera ripristinare, quindi **Restore**.

**Ripristinare se non è stato identificato un attacco di sistema**

1. Visualizzare le copie Snapshot nei volumi:

   Selezionare **archiviazione > volumi**, quindi selezionare il volume e **Snapshot Copies**.
2. Selezionarli e ⋮ scegliere l' `Anti_ransomware_backup` istantanea.
3. Selezionare **Restore** (Ripristina).
4. Tornare al menu **Snapshot Copies**, quindi scegliere la copia istantanea che si desidera utilizzare. Selezionare **Restore** (Ripristina).

**CLI**

**Ripristino dopo un attacco di sistema**

1. Per eseguire il ripristino dalla copia snapshot ARP, passare direttamente al punto 2. Per ripristinare i dati da copie Snapshot precedenti, è necessario rilasciare il blocco sullo snapshot ARP.

   ⓘ È necessario rilasciare il SnapLock anti-ransomware solo prima di eseguire il ripristino dalle copie Snapshot precedenti, se si utilizza `volume snap restore` come descritto di seguito. Se si ripristinano i dati utilizzando Flex Clone, Single file Snap Restore o altri metodi, ciò non è necessario.

   Contrassegnare l'attacco come "falso positivo" e "chiaro sospetto":
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`
   Per identificare gli interni, utilizzare uno dei seguenti parametri:
   `[-seq-no` *`integer`*`]` Numero di sequenza del file nell'elenco dei file sospetti.
   `[-extension` *`text`*`, … ]` Estensioni di file
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".
2. Elencare le copie Snapshot in un volume:

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

L'esempio seguente mostra le copie Snapshot in `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. Ripristinare il contenuto di un volume da una copia Snapshot:

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

Nell'esempio riportato di seguito viene ripristinato il contenuto di `vol1`:

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

**Ripristinare se non è stato identificato un attacco di sistema**

1. Elencare le copie Snapshot in un volume:

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

L'esempio seguente mostra le copie Snapshot in `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. Ripristinare il contenuto di un volume da una copia Snapshot:

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

Nell'esempio riportato di seguito viene ripristinato il contenuto di `vol1`:

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

3. Ripetere i passaggi 1 e 2 per ripristinare il volume utilizzando la copia Snapshot desiderata.

**Ulteriori informazioni**

- "KB: Prevenzione e recovery dal ransomware in ONTAP"

# Modificare le opzioni per le copie Snapshot automatiche

A partire da ONTAP 9.11.1, puoi utilizzare la CLI per controllare le impostazioni di conservazione per le copie Snapshot di protezione autonoma dal ransomware (ARP), generate automaticamente in risposta a sospetti attacchi ransomware.

**Prima di iniziare**

È possibile modificare solo le opzioni di ARP Snapshot su una SVM di nodo.

**Fasi**

1. Per visualizzare tutte le impostazioni di copia correnti di ARP Snapshot, immettere:
   `vserver options -vserver` *`svm_name`* `arw*`

Il `vserver options` command è un comando nascosto. Per visualizzare la pagina man, immettere `man vserver options` Nella CLI di ONTAP.

2. Per visualizzare le impostazioni di copia correnti di ARP Snapshot, immettere:
`vserver options -vserver svm_name -option-name arw_setting_name`
3. Per modificare le impostazioni di copia di ARP Snapshot, immettere:
`vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

   È possibile modificare le seguenti impostazioni:

| Impostazione ARW | Descrizione |
|---|---|
| `arw.snap.max.count` | Specifica il numero massimo di copie Snapshot ARP che possono esistere in un volume in qualsiasi momento. Le copie meno recenti vengono eliminate per garantire che il numero totale di copie Snapshot ARP rientri nel limite specificato.<br>Il `-option-value` il parametro accetta numeri interi compresi tra 3 e 8. Il valore predefinito è 6. |
| `arw.snap.create.interval.hours` | Specifica l'intervallo *in ore* tra le copie snapshot ARP. Una nuova copia snapshot ARP viene creata quando si sospetta un attacco basato sull'entropia dei dati e la copia snapshot ARP creata più di recente è precedente all'intervallo specificato.<br>Il `-option-value` il parametro accetta numeri interi compresi tra 1 e 48. Il valore predefinito è 4. |
| `arw.snap.normal.retain.interval.hours` | Specifica la durata *in ore* per la quale viene conservata una copia snapshot ARP. Quando una copia snapshot ARP raggiunge la soglia di conservazione, qualsiasi altra copia snapshot ARP creata prima di essere eliminata. Non può esistere più di una copia snapshot ARP precedente alla soglia di conservazione.<br>Il `-option-value` il parametro accetta numeri interi compresi tra 4 e 96. Il valore predefinito è 48. |
| `arw.snap.max.retain.interval.days` | Specifica la durata massima *in giorni* per la quale è possibile conservare una copia snapshot ARP. Qualsiasi copia snapshot ARP precedente a questa durata viene eliminata quando non viene riportato alcun attacco sul volume.<br>L'intervallo di conservazione massimo per le copie snapshot ARP viene ignorato se viene rilevata una minaccia moderata. La copia snapshot ARP creata in risposta alla minaccia viene conservata fino a quando non si risponde alla minaccia. Contrassegnare una minaccia come falso positivo eliminare le copie snapshot ARP sul volume.<br>Il `-option-value` il parametro accetta numeri interi compresi tra 1 e 365. Il valore predefinito è 5. |

| Impostazione ARW | Descrizione |
| --- | --- |
| `arw.snap.create.interval.hours.post.max.count` | Specifica l'intervallo *in ore* tra le copie snapshot ARP quando il volume contiene già il numero massimo di copie snapshot ARP. Una volta raggiunto il numero massimo di copie, una copia snapshot ARP viene eliminata per creare spazio per una nuova copia. È possibile ridurre la velocità di creazione delle nuove copie Snapshot ARP per conservare le copie meno recenti utilizzando questa opzione. Se il volume contiene già il numero massimo di copie snapshot ARP, l'intervallo specificato in questa opzione viene utilizzato per la successiva creazione di copie snapshot ARP anziché `arw.snap.create.interval.hours`.<br>Il `-option-value` il parametro accetta numeri interi compresi tra 4 e 48. Il valore predefinito è 8. |
| `arw.surge.snap.interval.days` | Specifica l'intervallo *in giorni* tra le copie snapshot ARP create in risposta ai picchi io. ONTAP crea una copia snapshot ARP surge quando c'è un aumento del traffico io e l'ultima copia snapshot ARP creata è precedente a questo intervallo specificato. Questa opzione specifica anche il periodo di conservazione *in giorno* per le copie snapshot di picco ARP.<br>Il `-option-value` il parametro accetta numeri interi compresi tra 1 e 365. Il valore predefinito è 5. |
| `arw.snap.new.extns.interval.hours` | Questa opzione specifica l'intervallo *in ore* tra le copie snapshot ARP create quando viene rilevata una nuova estensione file. Viene creata una nuova copia snapshot ARP quando<br>Viene osservata una nuova estensione del file; l'istantanea precedente creata dopo aver osservato una nuova estensione del file è precedente all'intervallo specificato. Su un carico di lavoro che spesso crea nuove estensioni di file, questo intervallo aiuta a controllare la frequenza delle copie snapshot ARP. Questa opzione è indipendente da `arw.snap.create.interval.hours`, Che specifica l'intervallo per le copie snapshot ARP basate sull'entropia dei dati.<br>Il `-option-value` il parametro accetta numeri interi compresi tra 24 e 8760. Il valore predefinito è 48. |

## Informazioni sul copyright



## Informazioni sul marchio commerciale