Schutz durch Ransomware

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

Schutz durch Ransomware

Autonome Ransomware-Schutz – Übersicht

Seit ONTAP 9.10.1 nutzt die Funktion Autonomous Ransomware Protection (ARP) Workload-Analysen in NAS-Umgebungen (NFS und SMB), um ungewöhnliche Aktivitäten, die auf einen Ransomware-Angriff hinweisen, proaktiv zu erkennen und zu warnen.

Wenn ein Angriff vermutet wird, erstellt ARP zusätzlich zu dem bestehenden Schutz vor geplanten Snapshot-Kopien auch neue Snapshot-Kopien.

Die ARP-Funktion ist mit den folgenden Lizenzen aktiviert.

ONTAP-Versionen	Lizenz
ONTAP 9.11.1 und höher	Anti_Ransomware
ONTAP 9.10.1	MT_EK_MGMT (mandantenfähiger Schlüsselmanagement)

- Wenn Sie ein Upgrade auf ONTAP 9.11.1 oder höher durchführen und ARP bereits auf Ihrem System konfiguriert ist, müssen Sie die neue Anti-Ransomware-Lizenz nicht erwerben. Für neue ARP-Konfigurationen ist die neue Lizenz erforderlich.
- Wenn Sie von ONTAP 9.11.1 oder höher auf ONTAP 9.10.1 zurücksetzen und ARP mit der Anti-Ransomware-Lizenz aktiviert haben, wird eine Warnmeldung angezeigt und muss unter Umständen ARP neu konfigurieren. "Erfahren Sie mehr über das Zurücksetzen von ARP".

Sie können ARP pro Volume konfigurieren, entweder mit ONTAP System Manager oder der ONTAP-Befehlszeilenschnittstelle (CLI).

ONTAP Strategie zum Schutz der Ransomware

Eine effektive Strategie zur Erkennung von Ransomware sollte mehr als nur eine einzige Sicherungsebene umfassen.

Eine Analogie wäre die Sicherheit eines Fahrzeugs. Sie möchten sich nicht auf eine einzige Funktion verlassen, wie z. B. einen Sicherheitsgurt, um Sie bei einem Unfall vollständig zu schützen. Airbags, Anti-Lock-Bremsen und Vorkollisionswarnung sind weitere Sicherheitsmerkmale, die zu einem viel besseren Ergebnis führen. Ransomware-Schutz sollte in der gleichen Weise betrachtet werden.

ONTAP umfasst Funktionen wie FPolicy, Snapshot Kopien, SnapLock und Active IQ Digital Advisor für den Schutz vor Ransomware. Die folgenden Informationen konzentrieren sich auf die integrierte ONTAP ARP Funktion mit Machine-Learning-Funktionen.

Weitere Informationen zu den anderen Anti-Ransomware-Funktionen von ONTAP finden Sie unter: "TR-4572: NetApp Lösung gegen Ransomware"

Was ONTAP ARP erkennt

Es gibt zwei Arten von Ransomware-Angriffen:

1. Denial-of-Service für Dateien durch Verschlüsselung von Daten Der Angreifer behält den Zugriff auf diese Daten vor, es sei denn, ein Lösegeld wird bezahlt.
2. Diebstahl sensibler proprietärer Daten. Der Angreifer droht, diese Daten der öffentlichen Domain freizugeben, wenn kein Lösegeld bezahlt wird.

ONTAP ARP löst den ersten Typ mit einem Anti-Ransomware-Erkennungsmechanismus, der auf folgenden basiert:

1. Identifizierung der eingehenden Daten als verschlüsselt oder als Klartext.
2. Analytics, die erkennt
   - Hohe Daten *Entropy* (eine Auswertung der Zufälligkeit von Daten in einer Datei)
   - Anstieg anormaler Volume-Aktivitäten bei der Datenverschlüsselung
   - Eine Erweiterung, die nicht dem normalen Erweiterungstyp entspricht

> Kein Ransomware-Erkennungs- oder Präventionssystem kann die Sicherheit bei einem Ransomware-Angriff vollständig gewährleisten. Möglicherweise wird ein Angriff nicht erkannt, doch NetApp ARP fungiert als wichtige zusätzliche Abwehrschicht, falls die Virenschutz-Software ein Intrusion nicht erkennt. ARP erkennt die Ausbreitung der meisten Ransomware-Angriffe, nachdem nur wenige Dateien verschlüsselt sind, automatisch Maßnahmen zur Datensicherung ergreifen und Sie darauf aufmerksam machen, dass im Verdacht stehende Angriffe auf einen Angriff stattfindet.

Wiederherstellung von Daten im ONTAP nach einem Ransomware-Angriff

Wenn ein Angriff vermutet wird, erstellt das System zu diesem Zeitpunkt eine Volume Snapshot Kopie und sperrt die Kopie. Wird der Angriff zu einem späteren Zeitpunkt bestätigt, kann das Volume auf diesen proaktiv aufgenommene Snapshot wiederhergestellt werden, wodurch der Datenverlust minimiert wird.

Gesperrte Snapshot Kopien können nicht auf normale Weise gelöscht werden. Wenn Sie sich jedoch später entscheiden, den Angriff als falsch positiv zu markieren, wird die gesperrte Kopie gelöscht.

Mit Kenntnis der betroffenen Dateien und dem Zeitpunkt des Angriffs können die betroffenen Dateien selektiv von verschiedenen Snapshot-Kopien wiederhergestellt werden, statt das gesamte Volume einfach auf einen der Snapshots zurücksetzen zu müssen.

ARP baut auf bewährte ONTAP-Technologie zur Datensicherung und Disaster Recovery auf, um auf Ransomware-Angriffe zu reagieren. Weitere Informationen zur Wiederherstellung von Daten finden Sie in den folgenden Themen.

- "Wiederherstellen von Snapshot-Kopien (System Manager)"
- "Wiederherstellen von Dateien aus Snapshot-Kopien (CLI)"
- "Intelligente Ransomware-Recovery"

Anwendungsfälle und Überlegungen zum autonomen Ransomware-Schutz

Unterstützung für ONTAP Plattformen:

- Die Funktion Autonomous Ransomware Protection (ARP) ist für alle lokalen ONTAP Systeme ab ONTAP 9.10.1 verfügbar.
- ARP ist derzeit für ONTAP Select nicht verfügbar.
- ARP steht derzeit nicht für Amazon FSX oder die folgenden Cloud Volumes ONTAP Umgebungen zur Verfügung:
  - AWS
  - Azure
  - Google Cloud

Geeignete Workloads:

- Datenbanken auf NFS-Storage
- Home Directorys für Windows oder Linux

  Da Benutzer Dateien mit Erweiterungen erstellen könnten, die nicht im Lernzeitraum erkannt wurden, gibt es eine größere Möglichkeit von False positive in diesem Workload.

- Bilder und Video

  Beispielsweise Daten aus dem Gesundheitswesen und EDA-Daten (Electronic Design Automation).

Ab ONTAP 9.12.1 ist ARP für die folgenden Konfigurationen verfügbar:

- Volumes sind mit SnapMirror geschützt
- SVMs sind durch SnapMirror geschützt
- Aktivierte SVMs für die Migration (SVM-Datenmobilität)

Ungeeignete Workloads:

- Workloads mit sehr hoher Häufigkeit zum Erstellen oder Löschen von Dateien (Hunderttausende Dateien in wenigen Sekunden, z. B. Workloads für Test/Entwicklung)
- ARP hängt von der Fähigkeit ab, einen ungewöhnlichen Anstieg in der Datei-Erzeugen oder -Löschung zu erkennen. Ist die Applikation die Quelle der Dateiaktivitäten, können sie nicht effektiv von Ransomware-Aktivitäten unterschieden werden
- Workloads, bei denen die Applikation oder der Host die Daten-ARP verschlüsselt, hängt von der Unterscheidung der eingehenden Daten als verschlüsselt oder unverschlüsselt ab. Wenn die Applikation selbst die Daten verschlüsselt, wird die Effektivität der Funktion verringert. Die Funktion kann jedoch weiterhin basierend auf Dateiaktivitäten (Erstellen, Löschen und Überschreiben) und Dateityp verwendet werden.

Nicht unterstützte Systemkonfigurationen:

- SAN-Umgebungen

- ONTAP S3-Umgebungen
- VMDKs auf NFS

Volume-Anforderungen:

- Weniger als 100 % voll
- Verbindungspfad muss aktiv sein

Nicht unterstützte Volume-Typen:

- Offline-Volumes
- Eingeschränkte Volumes
- SnapLock Volumes
- FlexGroup Volumes
- FlexCache Volumes (die Anti-Ransomware-Funktion wird auf FlexVol-Ursprungs-Volumes unterstützt, jedoch nicht auf Cache-Volumes).
- REINE SAN-Volumes
- Volumes von angestoppten Storage VMs
- Root-Volumes von Storage-VMs

SnapMirror und ARP-Interoperabilität

Ab ONTAP 9.12.1 wird ARP auf SnapMirror Ziel-Volumes unterstützt. Wenn ein SnapMirror Quell-Volume ARP-aktiviert ist, übernimmt das SnapMirror Ziel-Volume automatisch den ARP-Konfigurationsstatus (Learning, Enabled usw.), ARP-Trainingsdaten und ARP-erstellte Snapshots des Quell-Volume. Es ist keine explizite Aktivierung erforderlich.

Während das Zielvolume aus schreibgeschützten (RO) Snapshot Kopien besteht, wird auf seinen Daten keine ARP Verarbeitung durchgeführt. Wenn das SnapMirror Ziel-Volume jedoch in Read-Write (RW) konvertiert wird, wird ARP automatisch auf dem RW-konvertierten Zielvolume aktiviert. Das Zielvolumen erfordert neben dem, was bereits auf dem Quellvolumen aufgezeichnet wurde, keine zusätzlichen Lernverfahren.

In ONTAP 9.10.1 und 9.11.1 überträgt SnapMirror nicht den ARP-Konfigurationsstatus, die Trainingsdaten und Snapshot-Kopien von den Quell- auf Ziel-Volumes. Wenn also das SnapMirror Ziel-Volume in RW konvertiert wird, muss ARP auf dem Ziel-Volume nach der Konvertierung explizit in den Learning Mode aktiviert werden.

ARP-Performance- und Frequenzüberlegungen

Die ARP-Funktion kann, wie im Datendurchsatz und bei den IOPS-Spitzen gemessen, nur minimale Auswirkungen auf die System-Performance haben. Die Auswirkungen der Anti-Ransomware-Funktion sind stark von Volume-Workloads abhängig. Für die meisten typischen oder gängigen Workloads werden folgende Konfigurationsgrenzwerte empfohlen:

Workload-Merkmale	Empfohlene Volume-Beschränkung pro Node	Performance-Verschlechterung bei Überschreitung der Grenze des Volume pro Node:[*]
Leseintensiv oder die Daten komprimiert werden können.	150	4 % der maximalen IOPS

Workload-Merkmale	Empfohlene Volume-Beschränkung pro Node	Performance-Verschlechterung bei Überschreitung der Grenze des Volume pro Node:[*]
Schreibintensiv und die Daten können nicht komprimiert werden.	60	10 % der maximalen IOPS

Pass:[*] die Systemleistung wird unabhängig von der Anzahl der hinzugefügten Volumes, die über den empfohlenen Grenzwerten liegen, nicht über diesen Prozentwerten hinaus beeinträchtigt.

Da ARP-Analysen in einer priorisierten Reihenfolge ausgeführt werden, da sich die Anzahl der geschützten Volumes erhöht, werden die Analysen auf jedem Volume weniger häufig ausgeführt.

Automatische Snapshot-Kopien sind nötig, wenn Ransomware erkannt wird

Um den bestmöglichen Recovery-Punkt zu erhalten, erstellt ARP eine automatische Snapshot-Kopie, sobald anormale Dateiaktivitäten erkannt werden. ARP kennzeichnet jedoch nicht sofort eine Warnmeldung. Vielmehr müssen Analysen ausgeführt werden und bestätigen, dass die verdächtigen Aktivitäten mit einem Ransomware-Profil übereinstimmen, bevor eine Warnung erstellt wird. Dieser Vorgang kann bis zu 60 Minuten dauern. Wenn die Analyse feststellt, dass die Aktivität nicht verdächtig ist, wird keine Meldung generiert, die automatisch erstellte Snapshot Kopie jedoch mindestens zwei Tage lang im Filesystem vorhanden bleibt.

Ab ONTAP 9.11.1 können Sie die Anzahl und den Aufbewahrungszeitraum für ARP Snapshot-Kopien kontrollieren, die automatisch als Antwort auf vermutete Ransomware-Angriffe erzeugt werden. Erfahren Sie, wie Sie "Optionen für automatische Snapshot-Kopien ändern".

Autonomer Schutz Vor Ransomware

Ab ONTAP 9.10.1 kann der autonome Ransomware-Schutz (ARP) auf neuen oder bestehenden Volumes aktiviert werden. Sie aktivieren ARP zunächst im Lernmodus, in dem das System die Arbeitslast analysiert, um das normale Verhalten zu charakterisieren. Anschließend wechseln Sie in den aktiven Modus, in dem abnorme Aktivitäten für Ihre Bewertung markiert werden.

Was Sie benötigen

- Eine Storage-VM, die für NFS oder SMB (oder beides) aktiviert ist
- Für Ihre ONTAP-Version wird die korrekte Lizenz installiert.

ONTAP-Versionen	Lizenz
ONTAP 9.8-9.10.1	MT_EK_MGMT (mandantenfähiger Schlüsselmanagement)
ONTAP 9.11.1 und höher	Anti_Ransomware

- Ein NAS-Workload mit konfigurierten Clients.
- Das zu sicherende Volume muss über einen aktiven Verbindungspfad verfügen.
- Optional, aber empfohlen: Das EMS-System ist so konfiguriert, dass es E-Mail-Benachrichtigungen sendet, die Benachrichtigungen über ARP-Aktivitäten enthalten. Weitere Informationen finden Sie unter "Konfigurieren Sie EMS-Ereignisse zum Senden von E-Mail-Benachrichtigungen".

Über diese Aufgabe

NetApp ARP beinhaltet einen ersten Lernzeitraum (auch „dry run“ genannt), in dem ein ONTAP-System lernt, welche Dateiendungen gültig sind, und verwendet die analysierten Daten zur Entwicklung von Alarmprofilen. Nachdem Sie ARP im Learning-Modus ausreichend Zeit ausgeführt haben, um Workload-Merkmale zu bewerten, können Sie in den aktiven Modus wechseln und mit dem Schutz Ihrer Daten beginnen. Wenn im aktiven Modus eine Dateierweiterung als anormal markiert wird, Sie sie jedoch auswerten und als falsch positiv markieren, wird das Warnungsprofil so verfeinert, dass die Erweiterung in zukünftigen Warnmeldungen nicht als anormal gekennzeichnet wird.

Obwohl Sie jederzeit vom Lernmodus in den aktiven Modus wechseln können, wird eine Lerndauer von 30 Tagen empfohlen. Ein frühzeitiges Umschalten kann zu vielen Fehlalarmen führen. In der ONTAP-CLI können Sie den verwenden `security anti-ransomware volume workload-behavior show` Befehl zum Anzeigen der bisher erkannten Dateierweiterungen. Es wird empfohlen, dieses Tool nicht zur Verkürzung des Lernzeitraums zu verwenden.

Sie können ARP auf einem vorhandenen Volume aktivieren, oder Sie können ein neues Volume erstellen und ARP von Anfang an aktivieren.

> In vorhandenen Volumes gelten die Lern- und aktiven Modi nur für neu geschriebene Daten, nicht für bereits vorhandene Daten im Volume. Die vorhandenen Daten werden nicht gescannt und analysiert, da die Merkmale eines früheren normalen Datenverkehrs auf der Grundlage der neuen Daten angenommen werden, nachdem das Volume für ARP aktiviert wurde.

Zum Verwalten dieser Funktion in der ONTAP-CLI können Sie den verwenden `security anti-ransomware volume` Befehl. Sie können auch die verwenden `volume modify` Befehl mit dem `-anti-ransomware` Parameter.

Beispiel 1. Schritte

System Manager

1. Klicken Sie auf **Storage > Volumes** und wählen Sie dann das Volume aus, das Sie schützen möchten.
2. Klicken Sie auf der Registerkarte **Sicherheit** der **Volumes** Übersicht auf **Status**, um im Feld **Anti-Ransomware** von deaktiviert auf aktiviert zu wechseln.
3. Wenn der Lernzeitraum vorbei ist, schalten Sie ARP in den aktiven Modus um.
   a. Klicken Sie auf **Storage > Volumes** und wählen Sie dann das Volume aus, das für den aktiven Modus bereit ist.
   b. Klicken Sie auf der Registerkarte **Sicherheit** der **Bände** Übersicht in der Anti-Ransomware Box auf **Switch** to Active Mode.
4. Sie können den ARP-Zustand des Volumens immer in der **Anti-Ransomware** Box überprüfen. Um den ARP-Status für alle Volumes anzuzeigen: Klicken Sie im Fensterbereich **Volumes** auf **ein-/Ausblenden**, und stellen Sie dann sicher, dass der Status **Anti-Ransomware** aktiviert ist.

CLI

1. Ändern Sie ein vorhandenes Volume, um Ransomware-Schutz im Learning-Modus zu ermöglichen:

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

   Ransomware kann auch mit dem aktiviert werden `volume modify` Befehl:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   dry-run
   ```

   Zudem besteht die Möglichkeit, vor der Bereitstellung von Daten ein neues Volume mit aktivierter Ransomware-Sicherung zu erstellen.

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

   Sie sollten ARP immer zunächst im Status Dry-run aktivieren. Beginnend mit dem aktiven Zustand kann zu überhöhten falsch positiven Berichten führen.

2. Wenn der Lernzeitraum zu Ende ist, ändern Sie das geschützte Volume, um in den aktiven Modus zu wechseln:

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

   Sie können auch mit dem Befehl „Volume ändern“ in den aktiven Modus wechseln:

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

3. Überprüfen Sie den ARP-Status des Volumes.

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

Autonome Ransomware-Sicherung in neuen Volumes standardmäßig aktiviert

Ab ONTAP 9.10.1 können Sie Storage-VMs (SVMs) so konfigurieren, dass neue Volumes im Learning-Modus standardmäßig für Autonomous Ransomware Protection (ARP) aktiviert sind.

Was Sie benötigen

- Für Ihre ONTAP-Version wird die korrekte Lizenz installiert.

ONTAP-Versionen	Lizenz
ONTAP 9.11.1 und höher	Anti_Ransomware
ONTAP 9.8-9.10.1	MT_EK_MGMT (mandantenfähiger Schlüsselmanagement)

Über diese Aufgabe

Neue Volumes werden standardmäßig mit ARP im deaktivierten Modus erstellt, die Einstellung können Sie jedoch in System Manager und über die CLI ändern. Standardmäßig sind die Volumes, die aktiviert sind, im Lernmodus auf ARP eingestellt.

Durch die Aktivierung von ARP für neue Volumes in einer SVM wird ARP automatisch für vorhandene Volumes in dieser SVM nicht aktiviert. Erfahren Sie, wie Sie "Aktivieren Sie ARP in einem vorhandenen Volume".

Beispiel 2. Schritte

System Manager

1. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM für Standard-Antivirus.
2. Klicken Sie auf der Registerkarte **Einstellungen** [im Abschnitt **Sicherheit**] auf Aktivieren Sie im Feld **Anti-Ransomware** das Kontrollkästchen, um ARP für NAS-Volumes zu aktivieren.

CLI

1. Ändern Sie eine vorhandene SVM, um ARP standardmäßig in neuen Volumes zu aktivieren:
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   Über die CLI können Sie auch eine neue SVM erstellen, wobei ARP standardmäßig für neue Volumes aktiviert ist.
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

Unterbrechen Sie den autonomen Ransomware-Schutz, um Workload-Ereignisse aus der Analyse auszuschließen

Wenn Sie ungewöhnliche Workload-Ereignisse erwarten, können Sie die ARP-Analyse (Autonomous Ransomware Protection, Autonomous Ransomware Protection) jederzeit unterbrechen und wieder aufnehmen.

Was Sie benötigen

- ARP wird im Lern- oder aktiven Modus ausgeführt.

Über diese Aufgabe

Während einer ARP-Pause werden keine Ereignisse protokolliert oder sind Maßnahmen bei neuen Schreibvorgängen. Die Analyse wird jedoch für frühere Protokolle im Hintergrund fortgesetzt.

> Verwenden Sie nicht die Anti-Ransomware-Disable-Funktion, um die Analyse anzuhalten. Dadurch wird ARP auf dem Volume deaktiviert, und alle vorhandenen Informationen rund um das gelernte Workload-Verhalten sind verloren. Dies würde einen Neustart des Lernzeitraums erfordern.

Beispiel 3. Schritte

System Manager

1. Klicken Sie auf **Storage > Volumes** und wählen Sie dann das Volume aus, auf dem Sie ARP anhalten möchten.
2. Klicken Sie auf der Registerkarte Sicherheit der Volumeübersicht in der **Anti-Ransomware** Box* auf **Anti-Ransomware** anhalten.

CLI

ARP auf einem Volume anhalten:

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

Um die Verarbeitung fortzusetzen, verwenden Sie den `resume` Parameter.

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

Reagieren Sie auf ungewöhnliche Aktivitäten.

Wenn Autonomous Ransomware Protection (ARP) abnormale Aktivitäten in einem geschützten Volume erkennt, wird eine Warnung ausgegeben. Sie sollten die Benachrichtigung bewerten, um festzustellen, ob die Aktivität erwartet und akzeptabel ist oder ob ein Angriff in Angriff ist.

Was Sie benötigen

- ARP wird im aktiven Modus ausgeführt.

Über diese Aufgabe

ARP zeigt eine Liste der verdächtigen Dateien an, wenn sie eine beliebige Kombination von hoher

Datenentropie, abnormaler Volume-Aktivität mit Datenverschlüsselung und ungewöhnlichen Dateierweiterungen erkennt.

Wenn die Warnung ausgegeben wird, können Sie darauf reagieren, indem Sie die Dateiaktivität auf zwei Arten markieren:

- Falsch positiv

  Der identifizierte Dateityp wird für Ihren Workload erwartet und kann ignoriert werden.

- Möglicher Ransomware-Angriff

  Der identifizierte Dateityp ist bei Ihrer Workload unerwartet und sollte als potenzieller Angriff behandelt werden.

In beiden Fällen wird das normale Monitoring nach dem Aktualisieren und Löschen der Benachrichtigungen fortgesetzt. ARP zeichnet Ihre Bewertung auf, Protokolle werden mit den neuen Dateitypen aktualisiert und zur späteren Analyse verwendet. Im Falle eines vermuteten Angriffs müssen Sie jedoch feststellen, ob es sich um einen Angriff handelt, ob er darauf reagiert, ob er tatsächlich ist, und geschützte Daten wiederherstellen, bevor Sie die Benachrichtigungen löschen. "Erfahren Sie mehr darüber, wie Sie nach einem Ransomware-Angriff wiederherstellen können".

Es gibt keine Hinweise zum Löschen, wenn Sie ein gesamtes Volume wiederhergestellt haben.

Beispiel 4. Schritte

System Manager

1. Wenn Sie eine „anormale Aktivität“-Benachrichtigung erhalten, klicken Sie auf den Link oder navigieren Sie zur Registerkarte **Sicherheit** der **Bände**-Übersicht.

   Warnungen werden im Fenster Übersicht des Fensters Ereignisse angezeigt.

2. Wenn eine Meldung „erkannte anormale Volumenaktivität“ angezeigt wird, zeigen Sie die verdächtigen Dateien an.

   Klicken Sie auf der Registerkarte **Sicherheit** auf Anzeigen **Verdachtsdatei**.

3. Prüfen Sie im Dialogfeld * Verdachtsed File Types* jeden Dateityp und markieren Sie ihn entweder als „False positive“ oder „Potential Ransomware Attack“.

Wenn Sie diesen Wert ausgewählt haben…	Führen Sie diese Aktion durch…
Falsch Positiv	Klicken Sie auf **Update** und **Clear Suspect File Types**, um Ihre Entscheidung aufzuzeichnen und die normale Anti-Ransomware-Überwachung fortzusetzen.
Möglicher Angriff Durch Ransomware	Reagieren Sie auf den Angriff und stellen Sie geschützte Daten wieder her. Klicken Sie dann auf **Update** und **Clear Suspect File Types**, um Ihre Entscheidung aufzuzeichnen und die normale ARP-Überwachung fortzusetzen. + Es gibt keine verdächtigen Dateitypen zu löschen, wenn Sie ein ganzes Volumen wiederhergestellt.

CLI

1. Wenn Sie eine Benachrichtigung über einen vermuteten Ransomware-Angriff erhalten, überprüfen Sie die Zeit und den Schweregrad des Angriffs:

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

   Probenausgabe:

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

   Sie können auch EMS-Nachrichten überprüfen:

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

2. Erstellen Sie einen Angriffsbericht, und notieren Sie den Ausgabeland:

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

Probenausgabe:

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

3. Zeigt den Bericht auf einem Administrator-Client-System an. Beispiel:

```
[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. Nehmen Sie eine der folgenden Aktionen auf Grundlage Ihrer Bewertung der Dateiendungen:

   - Falsch positiv

     Geben Sie den folgenden Befehl ein, um Ihre Entscheidung aufzuzeichnen – indem Sie die neue Erweiterung zur Liste der zulässigen hinzufügen – und wieder normal Anti-Ransomware-Überwachung:
     `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`

     Verwenden Sie einen der folgenden Parameter, um die Erweiterungen zu identifizieren:
     `[-seq-no` *`integer`*`]` Sequenznummer der Datei in der Liste der Verdächtigen.
     `[-extension` *`text`*`, … ]` Dateierweiterungen
     `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` Start- und Endzeiten für den zu löhenden Bereich im Format „MM/TT/JJJJ HH:MM:SS“.

   - Möglicher Ransomware-Angriff

     Reagieren Sie auf den Angriff und stellen Sie Daten wieder her. Geben Sie dann den folgenden Befehl ein, um Ihre Entscheidung zu notieren und die normale ARP-Überwachung fortzusetzen:

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

     Verwenden Sie einen der folgenden Parameter, um die Erweiterungen zu identifizieren:
     `[-seq-no` *`integer`*`]` Sequenznummer der Datei in der Liste der Verdächtigen
     `[-extension` *`text`*`, … ]` Dateierweiterung
     `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` Start- und Endzeiten für den zu löhenden Bereich im Format „MM/TT/JJJJ HH:MM:SS“.

Es gibt keine verdächtigen Dateitypen, die gelöscht werden müssen, wenn Sie ein ganzes Volume wiederhergestellt haben.

Wiederherstellung von Daten nach einem Ransomware-Angriff

Snapshot-Kopien mit dem Namen „Anti_Ransomware_Backup“ werden erstellt, wenn Autonomous Ransomware Protection (ARP) einen potenziellen Angriff erkennt. Sie können Daten aus diesen ARP-Kopien oder aus anderen Snapshot-Kopien wiederherstellen.

Falls ein Ransomware-Angriff stattfindet, ist der Artikel der Knowledge Base zu entnehmen "Vorbeugung und Wiederherstellung von Ransomware in ONTAP" Weitere Informationen zur Wiederherstellung und Risikominimierung.

Über diese Aufgabe

Wenn das Volume über SnapMirror Beziehungen verfügt, replizieren Sie alle gespiegelten Kopien des Volumes unmittelbar nach der Wiederherstellung aus einer Snapshot Kopie manuell. Dadurch können nicht nutzbare Spiegelkopien erstellt werden, die gelöscht und neu erstellt werden müssen.

Was Sie benötigen

- ARP aktiviert
- Berichte zu potenziellen Ransomware-Angriffen

Schritte

Die Wiederherstellung von Daten kann mit System Manager oder der ONTAP CLI erfolgen.

System Manager

1. Wenn Sie Daten aus früheren Snapshot Kopien wiederherstellen möchten, anstatt von den ARP-Kopien, müssen Sie die Snapshot-Sperre gegen Ransomware wie folgt freigeben. Wenn Sie eine Wiederherstellung aus den ARP-Kopien durchführen möchten, ist es nicht erforderlich, die Sperre freizugeben, und Sie können diesen Schritt überspringen.

Wenn ein Systemangriff erkannt wurde, führen Sie dies durch…	Wenn ein Systemangriff nicht identifiziert wurde, führen Sie dies durch…
a. Klicken Sie Auf **Storage > Volumes**. b. Wählen Sie **Sicherheit** und klicken Sie auf **vermutete Dateitypen anzeigen** c. Markieren Sie die Dateien als "falsch positiv" . d. Klicken Sie auf **Update** und **Verdächtige Dateitypen löschen**	Zum Freigeben der Snapshot-Sperre müssen Sie die ARP-Kopien vor der Wiederherstellung aus früheren Snapshot-Kopien wiederherstellen. Befolgen Sie die Schritte 2-3, um Daten aus den ARP-Kopien wiederherzustellen, und wiederholen Sie dann den Prozess für die Wiederherstellung aus früheren Snapshot-Kopien.

2. Anzeige der Snapshot Kopien in Volumes:

   Klicken Sie auf **Speicher > Volumes**, wählen Sie das Volume aus und klicken Sie auf **Snapshot-Kopien**.

3. Klicken Sie Auf ⋮ Neben der Snapshot Kopie, die Sie wiederherstellen möchten, und wählen Sie **Wiederherstellen**.

CLI

1. Wenn Sie Daten aus früheren Snapshot Kopien wiederherstellen möchten, anstatt von den ARP-Kopien, müssen Sie die Snapshot-Sperre gegen Ransomware wie folgt freigeben. Wenn Sie eine Wiederherstellung aus den ARP-Kopien durchführen möchten, ist es nicht erforderlich, die Sperre freizugeben, und Sie können diesen Schritt überspringen.

```
It is only necessary to release the anti-ransomware Snaplock before
restoring from earlier Snapshot copies if you are using the `volume
snap restore`` command as outline below.  If you are restoring data
using Flex Clone, Single File Snap Restore or other methods, this is
not necessary.
```

Wenn ein Systemangriff erkannt wurde, führen Sie dies durch…	Wenn ein Systemangriff nicht identifiziert wurde, führen Sie dies durch…
Markieren Sie den Angriff als „falsch positiv“ und „eindeutig verdächtig“. `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true` Verwenden Sie einen der folgenden Parameter, um die Erweiterungen zu identifizieren: `[-seq-no` *`integer`*`]` Sequenznummer der Datei in der Liste der Verdächtigen. `[-extension` *`text`*`, … ]` Dateierweiterungen `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` Start- und Endzeiten für den zu löhenden Bereich im Format „MM/TT/JJJJ HH:MM:SS“.	Zum Freigeben der Snapshot-Sperre müssen Sie die ARP-Kopien vor der Wiederherstellung aus früheren Snapshot-Kopien wiederherstellen. Befolgen Sie die Schritte 2-3, um Daten aus den ARP-Kopien wiederherzustellen, und wiederholen Sie dann den Prozess für die Wiederherstellung aus früheren Snapshot-Kopien.

2. Listen Sie die Snapshot Kopien in einem Volume auf:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Im folgenden Beispiel werden die Snapshot Kopien in angezeigt `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. Stellen Sie den Inhalt eines Volumes aus einer Snapshot Kopie wieder her:

   `volume snapshot restore -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`*

   Im folgenden Beispiel wird der Inhalt von wiederhergestellt `vol1`:

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

Optionen für automatische Snapshot-Kopien ändern

Ab ONTAP 9.11.1 können Sie mithilfe der CLI die Anzahl und den Aufbewahrungszeitraum für ARP-Kopien (Autonomous Ransomware Protection, Autonomous Ransomware Protection) kontrollieren, die automatisch als Antwort auf vermutete Ransomware-Angriffe erzeugt werden.

Hinweis: Das `vserver options` Befehl ist ein verborgener Befehl. Um die man-Page anzuzeigen, geben Sie ein `man vserver options` Über die ONTAP CLI.

Die folgenden Optionen für automatische Snapshot Kopien können geändert werden:

arw.Snap.max.count

Gibt die maximale Anzahl von ARP Snapshot-Kopien an, die jederzeit in einem Volume vorhanden sein können. Ältere Kopien werden gelöscht, um sicherzustellen, dass die Gesamtzahl der ARP Snapshot Kopien innerhalb dieses festgelegten Limits liegt.

arw.snap.create.interval.hours

Gibt das Intervall (in Stunden) zwischen ARP Snapshot Kopien an. Wenn ein Angriff vermutet wird, wird eine neue Snapshot Kopie erstellt, die zuvor erstellt wurde, älter als dieses angegebene Intervall ist.

arw.snap.normal.retain.interval.hours

Gibt die Dauer (in Stunden) an, für die eine ARP Snapshot Kopie aufbewahrt wird. Wenn eine ARP Snapshot-Kopie diese alt wird, werden alle anderen ARP Snapshot-Kopien, die erstellt wurden, bevor die neueste Kopie, auf die dieses Alter zu erreichen, gelöscht. Keine ARP Snapshot Kopie kann älter als diese Dauer sein.

arw.snap.max.retain.interval.days

Gibt die maximale Dauer (in Tagen) an, für die eine ARP Snapshot-Kopie aufbewahrt werden kann. Alle ARP-Snapshot-Kopien, die älter als diese Dauer sind, werden gelöscht, wenn auf dem Volume kein Angriff gemeldet wird.

arw.snap.create.interval.hours.post.max.count

Gibt das Intervall (in Stunden) zwischen ARP Snapshot Kopien an, wenn das Volume bereits die maximale Anzahl von ARP Snapshot Kopien enthält. Wenn die Höchstzahl erreicht wird, wird eine ARP Snapshot-Kopie gelöscht, um Platz für eine neue Kopie zu schaffen. Die neue Erstellungsgeschwindigkeit von ARP Snapshot Kopien kann mit dieser Option die ältere Kopie beibehalten werden. Wenn das Volume bereits die maximale Anzahl von ARP Snapshot-Kopien enthält, wird dieses in dieser Option angegebene Intervall anstelle von arw.snap.create.interval.hours für die Erstellung der nächsten ARP Snapshot-Kopie verwendet.

arw.surge.snap.interval.days

Gibt das Intervall (in Tagen) zwischen ARP Surge Snapshot Kopien an. Eine neue ARP Snapshot Überspannungskopie wird erstellt, wenn ein Anstieg des I/O-Verkehrs auftritt und die zuletzt erstellte ARP Snapshot Kopie älter als dieses angegebene Intervall ist. Diese Option gibt außerdem die Dauer (in Tagen) an, für die eine ARP Surge Snapshot Kopie aufbewahrt wird.

CLI-Verfahren

Um alle aktuellen Einstellungen von ARP Snapshot Kopien anzuzeigen, geben Sie Folgendes ein:
`vserver options -vserver svm_name arw*`

Um die ausgewählten aktuellen Einstellungen von ARP Snapshot Kopien anzuzeigen, geben Sie Folgendes ein:
`vserver options -vserver svm_name -option-name arw_setting_name`

Geben Sie zum Ändern der Einstellungen für ARP Snapshot Kopien Folgendes ein:
`vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`