



Schutz vor Ransomware

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Schutz vor Ransomware 1
 - Autonome Ransomware-Schutz – Übersicht 1
 - Anwendungsfälle und Überlegungen zum autonomen Ransomware-Schutz 4
 - Autonomer Schutz Vor Ransomware 7
 - Autonome Ransomware-Sicherung in neuen Volumes standardmäßig aktiviert 10
 - Unterbrechen Sie den autonomen Ransomware-Schutz, um Workload-Ereignisse aus der Analyse auszuschließen 12
 - Managen Sie die Parameter für die Erkennung von Angriffen gegen autonomen Ransomware-Schutz ... 15
 - Reagieren Sie auf ungewöhnliche Aktivitäten 19
 - Wiederherstellung von Daten nach einem Ransomware-Angriff 22
 - Optionen für automatische Snapshot-Kopien ändern 26

Schutz vor 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.

Lizenzen und Enablement

ARP erfordert eine Lizenz. ARP ist mit dem verfügbar ["ONTAP ONE Lizenz"](#). Wenn Sie nicht über die ONTAP One-Lizenz verfügen, stehen andere Lizenzen zur Verfügung, um ARP zu verwenden. Diese unterscheiden sich je nach Ihrer ONTAP-Version.

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 entweder mit System Manager oder mit der ONTAP CLI für einzelne Volumes konfigurieren.

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 verlassen sich nicht auf eine einzelne Funktion, wie einen Sicherheitsgurt, um Sie bei einem Unfall komplett 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.

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

Weitere Informationen zu den weiteren Anti-Ransomware-Funktionen von ONTAP finden Sie unter ["TR-4572: NetApp Lösung gegen Ransomware"](#)

Was ARP erkennt

ARP wurde zum Schutz vor Denial-of-Service-Angriffen entwickelt, bei denen der Angreifer Daten zurückhält, bis ein Lösegeld bezahlt wird. ARP bietet die Erkennung von Ransomware auf der Basis von:

- Identifizierung der eingehenden Daten als verschlüsselt oder als Klartext.
- Analytics, die erkennt
 - **Entropie:** Eine Auswertung der Zufälligkeit der Daten in einer Datei
 - **Dateierweiterungstypen:** Eine Erweiterung, die nicht dem normalen Erweiterungstyp entspricht
 - **Datei-IOPS:** Ein Anstieg der anormalen Volume-Aktivität mit Datenverschlüsselung (ab ONTAP 9.11.1)

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.



Kein Ransomware-Erkennungs- oder Präventionssystem kann die Sicherheit bei einem Ransomware-Angriff vollständig gewährleisten. Obwohl es möglich ist, dass ein Angriff unentdeckt bleibt, fungiert ARP als wichtige zusätzliche Verteidigungsschicht, wenn Antivirensoftware einen Angriff nicht erkennt.

Lernen und aktive Modi

ARP verfügt über zwei Modi:

- **Learning** (oder „Dry Run“-Modus)
- **Aktiv** (oder „aktiviert“-Modus)

Wenn Sie ARP aktivieren, wird es im *Learning Mode* ausgeführt. Im Lernmodus entwickelt das ONTAP System ein Warnmeldungsprofil auf der Grundlage der Analysebereiche Entropie, Dateierweiterungstypen und Datei-IOPS. 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. Sobald ARP in den aktiven Modus gewechselt ist, erstellt ONTAP ARP Snapshot Kopien, um die Daten zu schützen, wenn eine Bedrohung erkannt wird.

Es wird empfohlen, ARP 30 Tage lang im Lernmodus zu belassen. Ab ONTAP 9.13.1 bestimmt ARP automatisch das optimale Lernintervall und automatisiert den Switch, der vor 30 Tagen auftreten kann.

Wenn im aktiven Modus eine Dateierweiterung als anormal gekennzeichnet ist, sollten Sie die Warnmeldung auswerten. Sie können auf die Warnung reagieren, um Ihre Daten zu schützen, oder Sie können die Warnung als falsch positiv markieren. Wenn Sie eine Warnung als falsch positiv markieren, wird das Warnungsprofil aktualisiert. Wenn die Warnmeldung beispielsweise durch eine neue Dateierweiterung ausgelöst wird und Sie die Warnmeldung als falsch positiv markieren, erhalten Sie beim nächsten Mal keine Warnmeldung, wenn diese Dateierweiterung beobachtet wird. Der Befehl `security anti-ransomware volume workload-behavior show` Zeigt Dateierweiterungen an, die im Volume erkannt wurden. (Wenn Sie diesen Befehl zu Beginn des Lernmodus ausführen und er eine genaue Darstellung der Dateitypen anzeigt, sollten Sie diese Daten nicht als Grundlage für den Wechsel in den aktiven Modus verwenden, da ONTAP weiterhin andere Metriken sammelt.)

Ab ONTAP 9.11.1 können Sie die Erkennungsparameter für ARP anpassen. Weitere Informationen finden Sie unter [Verwalten von ARP-Angriffserkennungsparametern](#).

Bedrohungsbewertung und ARP Snapshot Kopien

Im aktiven Modus bewertet ARP die Bedrohungswahrscheinlichkeit anhand eingehender Daten, die mit gelernten Analysen gemessen werden. Eine Messung wird zugewiesen, wenn ARP eine Bedrohung erkennt:

- **Low:** Früheste Erkennung einer Anomalie im Volume (z.B. wird eine neue Dateierweiterung im Volume beobachtet).
- **Mittel:** Es werden mehrere Dateien mit derselben nie zuvor gesehenen Dateierweiterung beobachtet.
 - In ONTAP 9.10.1 liegt der Schwellenwert für die Eskalation auf moderat bei 100 oder mehr Dateien. Ab ONTAP 9.11.1 kann die Dateimenge geändert werden; der Standardwert ist 20.

In einer Situation mit geringen Bedrohungen erkennt ONTAP eine Auffälligkeit und erstellt eine Snapshot Kopie des Volumes, um den bestmöglichen Recovery-Punkt zu erreichen. ONTAP übergibt den Namen der ARP Snapshot Kopie mit `Anti-ransomware-backup` Um es leicht zu identifizieren, zum Beispiel `Anti_ransomware_backup.2022-12-20_1248`.

Die Bedrohung wird eskaliert und mäßig, nachdem ONTAP einen Analysebericht ausgeführt hat und festgestellt hat, ob die Anomalie mit einem Ransomware-Profil übereinstimmt. Bedrohungen, die auf der niedrigen Ebene bleiben, werden protokolliert und im Abschnitt **Ereignisse** von System Manager sichtbar. Wenn die Angriffswahrscheinlichkeit mäßig ist, generiert ONTAP eine EMS-Benachrichtigung, in der Sie aufgefordert werden, die Bedrohung zu bewerten. ONTAP sendet keine Warnungen über geringe Bedrohungen, aber ab ONTAP 9.14.1 können Sie [Ändern Sie die Einstellungen für Warnmeldungen](#). Weitere Informationen finden Sie unter [Reagieren Sie auf ungewöhnliche Aktivitäten](#).

Sie können Informationen zu einer Bedrohung, unabhängig von der Ebene, im System Manager **Ereignisse** Abschnitt oder mit dem anzeigen `security anti-ransomware volume show` Befehl.

ARP Snapshot Kopien werden mindestens zwei Tage aufbewahrt. Ab ONTAP 9.11.1 können Sie die Aufbewahrungseinstellungen ändern. Weitere Informationen finden Sie unter [Ändern Sie Optionen für Snapshot Kopien](#).

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. Wenn der Angriff später bestätigt wird, kann das Volume mithilfe der ARP Snapshot Kopie wiederhergestellt werden.

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.

Durch das Wissen über die betroffenen Dateien und den Zeitpunkt eines Angriffs können betroffene Dateien selektiv von verschiedenen Snapshot Kopien wiederhergestellt werden, anstatt das gesamte Volume einfach auf eine der Snapshot Kopien zurückzugreifen.

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

Autonomous Ransomware Protection (ARP) ist ab ONTAP 9.10.1 für NAS-Workloads verfügbar. Vor der Bereitstellung von ARP sollten Sie die empfohlenen Verwendungszwecke und unterstützten Konfigurationen sowie die Auswirkungen auf die Performance kennen.

Unterstützte und nicht unterstützte Konfigurationen

Bei der Entscheidung, ARP zu verwenden, ist es wichtig sicherzustellen, dass die Arbeitslast Ihres Volumes für ARP geeignet ist und dass sie die erforderlichen Systemkonfigurationen erfüllt.

Geeignete Workloads

ARP eignet sich für:

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

Da Benutzer Dateien mit Erweiterungen erstellen können, die während des Lernzeitraums nicht erkannt wurden, besteht eine größere Möglichkeit von False-positive-Meldungen in diesem Workload.

- Bilder und Video

Beispielsweise Gesundheitsdaten und EDA-Daten (Electronic Design Automation)

Ungeeignete Workloads

ARP ist nicht geeignet für:

- Workloads mit hoher Frequenz, die Dateien erstellen oder löschen (Hunderttausende Dateien in wenigen Sekunden, z. B. Test-/Entwicklungs-Workloads).
- Die Erkennung von ARP-Bedrohungen hängt von der Fähigkeit ab, einen ungewöhnlichen Anstieg bei der Erstellung, Umbenennung oder Löschung von Dateien zu erkennen. Wenn die Anwendung selbst die Quelle der Dateiaktivität ist, kann sie nicht effektiv von Ransomware-Aktivitäten unterschieden werden.
- Workloads, bei denen die Anwendung oder der Host Daten verschlüsselt.
ARP hängt davon ab, dass eingehende Daten als verschlüsselt oder unverschlüsselt unterschieden werden. Wenn die Applikation selbst die Daten verschlüsselt, wird die Effektivität der Funktion verringert. Die Funktion kann jedoch immer noch basierend auf den Dateiaktivitäten (Löschen, Überschreiben, Erstellen, Erstellen oder Erstellen von Dateien oder Erstellen oder Umbenennen mit einer neuen Dateierweiterung) und dem Dateityp funktionieren.

Unterstützte Konfigurationen

ARP ist ab ONTAP 9.10.1 für NFS und SMB Volumes in lokalen ONTAP Systemen verfügbar.

Andere Konfigurationen und Volume-Typen werden in den folgenden ONTAP-Versionen unterstützt:

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes sind mit asynchronem SnapMirror geschützt	✓	✓	✓		
SVMs gesichert mit asynchronem SnapMirror (SVM Disaster Recovery)	✓	✓	✓		
SVM-Datenmobilität (vserver migrate)	✓	✓	✓		
FlexGroup Volumes	✓	✓			
Überprüfung durch mehrere Administratoren	✓	✓			

SnapMirror und ARP-Interoperabilität

Ab ONTAP 9.12.1 wird ARP auf asynchronen SnapMirror Ziel-Volumes unterstützt. ARP ist **nicht** mit SnapMirror Synchronous 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 und Virtual Machines

ARP wird mit Virtual Machines (VMs) unterstützt. Die ARP-Erkennung verhält sich bei Änderungen innerhalb und außerhalb der VM unterschiedlich. ARP wird nicht für Workloads mit entropischen Dateien innerhalb der VM empfohlen.

Änderungen außerhalb der VM

ARP kann Änderungen an Dateierweiterungen auf einem NFS-Volume außerhalb der VM erkennen, wenn eine neue Erweiterung verschlüsselt in das Volume eintritt oder sich eine Dateierweiterung ändert. Nachweisbare Änderungen an Dateierweiterungen:

- .Vmx

- .vmxf
- .Vmdk
- -Flat.vmdk
- .nvram
- .Vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .Log
- -\#.log

Änderungen innerhalb der VM

Wenn der Ransomware-Angriff auf die VM zielt und Dateien innerhalb der VM geändert werden, ohne Änderungen außerhalb der VM vorzunehmen, erkennt ARP die Bedrohung, wenn die Standard-Entropie der VM gering ist (z. B. .txt-, .docx- oder .mp4-Dateien). Obwohl ARP in diesem Szenario einen Schutz-Snapshot erstellt, generiert es keine Bedrohungswarnung, da die Dateierweiterungen außerhalb der VM nicht manipuliert wurden.

Wenn es sich bei den Dateien standardmäßig um Dateien mit hoher Entropie handelt (z. B. .gzip- oder passwortgeschützte Dateien), sind die Erkennungsfunktionen von ARP begrenzt. ARP kann in dieser Instanz immer noch proaktive Snapshots machen, es werden jedoch keine Warnmeldungen ausgelöst, wenn die Dateierweiterungen nicht extern manipuliert wurden.

Nicht unterstützte Konfigurationen

ARP wird in den folgenden Systemkonfigurationen nicht unterstützt:

- ONTAP S3-Umgebungen
- SAN-Umgebungen

ARP unterstützt die folgenden Volume-Konfigurationen nicht:

- FlexGroup Volumes (in ONTAP 9.10.1 bis 9.12.1) Ab ONTAP 9.13.1 werden FlexGroup Volumes unterstützt)
- FlexCache Volumes (ARP wird auf Ursprungs-FlexVol Volumes unterstützt, jedoch nicht auf Cache Volumes)
- Offline-Volumes
- REINE SAN-Volumes
- SnapLock Volumes
- SnapMirror Synchronous
- Asynchronous SnapMirror (nur in ONTAP 9.10.1 und 9.11.1 unterstützt Asynchrones SnapMirror wird ab ONTAP 9.12.1 unterstützt. Weitere Informationen finden Sie unter [\[snapmirror\]](#).)
- Eingeschränkte Volumes
- Root-Volumes von Storage-VMs

- Volumes von angestoppten Storage VMs

ARP-Performance- und Frequenzüberlegungen

ARP kann die System-Performance im Hinblick auf den Durchsatz und die IOPS-Spitzenwerte minimal beeinträchtigen. Die Auswirkungen der ARP-Funktion hängen von den spezifischen Volume Workloads ab. Für gängige Workloads werden die folgenden 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
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 und die Anzahl der geschützten Volumes zunimmt, werden die Analysen auf jedem Volume weniger häufig ausgeführt.

Verifizierung mehrerer Administratoren mit Volumes, die mit ARP gesichert sind

Ab ONTAP 9.13.1 können Sie die Multi-Admin-Verifizierung (MAV) aktivieren, um zusätzliche Sicherheit mit ARP zu gewährleisten. MAV stellt sicher, dass mindestens zwei oder mehr authentifizierte Administratoren erforderlich sind, um ARP zu deaktivieren, ARP zu unterbrechen oder einen vermuteten Angriff als falsch positiv auf einem geschützten Volume zu markieren. Erfahren Sie, wie Sie ["Aktivieren Sie MAV für ARP-geschützte Volumes"](#).

Sie müssen Administratoren für eine MAV-Gruppe definieren und MAV-Regeln für das erstellen `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, und `security anti-ransomware volume attack clear-suspect` ARP-Befehle, die Sie schützen möchten. Jeder Administrator in der MAV-Gruppe muss jede neue Regelanforderung und genehmigen ["Fügen Sie die MAV-Regel erneut hinzu"](#) Innerhalb der MAV-Einstellungen.

Ab ONTAP 9.14.1 bietet ARP Warnungen für die Erstellung eines ARP-Snapshot und für die Beobachtung einer neuen Dateierweiterung an. Warnmeldungen für diese Ereignisse sind standardmäßig deaktiviert. Alarmer können auf Volume- oder SVM-Ebene festgelegt werden. Mit können Sie MAV-Regeln auf SVM-Ebene erstellen `security anti-ransomware vserver event-log modify` Oder auf Lautstärkeregelung mit `security anti-ransomware volume event-log modify`.

Nächste Schritte

- ["Autonomer Schutz Vor Ransomware"](#)
- ["Aktivieren Sie MAV für ARP-geschützte Volumes"](#)

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

Über diese Aufgabe

Sie sollten ARP zunächst immer im Lern- (oder Dry-Run-) Modus aktivieren. Wenn Sie im aktiven Modus beginnen, kann dies zu überhöhten falsch-positiven Berichten führen.

Es wird empfohlen, ARP mindestens 30 Tage im Lernmodus laufen zu lassen. Ab ONTAP 9.13.1 bestimmt ARP automatisch das optimale Lernintervall und automatisiert den Switch, der vor 30 Tagen auftreten kann. Weitere Informationen finden Sie unter "[Lernen und aktive Modi](#)".



In bestehenden Volumes gelten der Lern- und der aktiv-Modus 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.

Bevor Sie beginnen

- Sie müssen eine Storage-VM (SVM) für NFS oder SMB (oder beides) aktivieren.
- Der [Korrekte Lizenz](#) Muss für Ihre ONTAP-Version installiert sein.
- Sie müssen NAS-Workloads und Clients konfiguriert haben.
- Das Volumen, auf dem Sie ARP setzen möchten, muss geschützt sein und über einen aktiven verfügen "[Verbindungspfad](#)".
- Das Volumen muss zu weniger als 100 % voll sein.
- Es wird empfohlen, das EMS-System so zu konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden, die Hinweise auf ARP-Aktivitäten enthalten. Weitere Informationen finden Sie unter "[Konfigurieren Sie EMS-Ereignisse zum Senden von E-Mail-Benachrichtigungen](#)".
- Ab ONTAP 9.13.1 wird empfohlen, die Multi-Admin-Verifizierung (MAV) zu aktivieren, sodass für die ARP-Konfiguration (Autonomous Ransomware Protection) mindestens zwei authentifizierte Benutzeradministratoren erforderlich sind. Weitere Informationen finden Sie unter "[Aktivieren Sie die Verifizierung durch mehrere Administratoren](#)".

Aktivieren Sie ARP

Sie können ARP mit System Manager oder der ONTAP CLI aktivieren.

System Manager

Schritte

1. Wählen Sie **Storage > Volumes** und dann das zu schützende Volume aus.
2. Wählen Sie im Register **Sicherheit** der **Volumes**-Übersicht **Status** aus, um im Lernmodus im Feld **Anti-Ransomware** von deaktiviert zu aktiviert zu wechseln.
3. Wenn der Lernzeitraum vorbei ist, schalten Sie ARP in den aktiven Modus um.



Ab ONTAP 9.13.1 bestimmt ARP automatisch das optimale Lernintervall und automatisiert den Switch. Das können Sie ["Deaktivieren Sie diese Einstellung auf der zugehörigen Speicher-VM"](#) Wenn Sie den Lernmodus manuell auf den aktiven Modus umschalten möchten.

- a. Wählen Sie **Storage > Volumes** und dann das Volume aus, das für den aktiven Modus bereit ist.
 - b. Wählen Sie im Register **Sicherheit** der Übersicht **Volumes** im Feld Anti-Ransomware **Switch** in den aktiven Modus.
4. Sie können den ARP-Status des Volumes im Feld **Anti-Ransomware** überprüfen.

Um den ARP-Status für alle Volumes anzuzeigen, wählen Sie im Bereich **Volumes ein/Ausblenden** aus, und stellen Sie dann sicher, dass der Status **Anti-Ransomware** aktiviert ist.

CLI

Der Prozess der Aktivierung von ARP mit der CLI unterscheidet sich, wenn sie es auf einem vorhandenen Volume und nicht auf einem neuen Volume aktivieren.

Aktivieren Sie ARP auf einem vorhandenen Volume

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
```

Wenn Sie ONTAP 9.13.1 oder höher ausführen, ist das adaptive Lernen aktiviert, sodass die Änderung des aktiven Status automatisch erfolgt. Wenn Sie nicht möchten, dass dieses Verhalten automatisch aktiviert wird, ändern Sie die Einstellung auf SVM-Ebene für alle zugehörigen Volumes:

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

2. Wenn der Lernzeitraum vorbei ist, ändern Sie das geschützte Volume, um in den aktiven Modus zu wechseln, falls nicht bereits automatisch ausgeführt:

```
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
```

Aktivieren Sie ARP auf einem neuen Volume

1. Erstellen Sie ein neues Volume mit aktiviertem Ransomware-Schutz, bevor Sie Daten bereitstellen.

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

Wenn Sie ONTAP 9.13.1 oder höher ausführen, ist das adaptive Lernen aktiviert, sodass die Änderung des aktiven Status automatisch erfolgt. Wenn Sie nicht möchten, dass dieses Verhalten automatisch aktiviert wird, ändern Sie die Einstellung auf SVM-Ebene für alle zugehörigen Volumes:

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

2. Wenn der Lernzeitraum vorbei ist, ändern Sie das geschützte Volume, um in den aktiven Modus zu wechseln, falls nicht bereits automatisch ausgeführt:

```
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.

Über diese Aufgabe

Standardmäßig werden neue Volumes mit ARP im deaktivierten Modus erstellt. Sie können diese Einstellung in System Manager und mit der CLI ändern. Standardmäßig aktivierte Volumes sind im Lern- (oder Dry-Run-) Modus auf ARP eingestellt.

ARP wird nur auf Volumes aktiviert, die in der SVM erstellt wurden, nachdem Sie die Einstellung geändert haben. ARP wird auf vorhandenen Volumes nicht aktiviert. Erfahren Sie, wie Sie ["Aktivieren Sie ARP in einem vorhandenen Volume"](#).

Ab ONTAP 9.13.1 wurde das adaptive Lernen zu ARP-Analysen hinzugefügt und der Wechsel vom Lernmodus zum aktiven Modus erfolgt automatisch. Weitere Informationen finden Sie unter ["Lernen und aktive Modi"](#).

Bevor Sie beginnen

- Der [Korrekte Lizenz](#) Muss für Ihre ONTAP-Version installiert sein.
- Das Volumen muss zu weniger als 100 % voll sein.

- Verbindungspfade müssen aktiv sein.
- Ab ONTAP 9.13.1 wird empfohlen, die Multi-Admin-Verifizierung (MAV) zu aktivieren, sodass für Ransomware-Vorgänge mindestens zwei authentifizierte Benutzeradministratoren erforderlich sind. ["Weitere Informationen ."](#)

Schalten Sie ARP vom Lernen in den aktiven Modus

Ab ONTAP 9.13.1 wurde das adaptive Lernen zu ARP-Analysen hinzugefügt. Der Wechsel vom Lernmodus in den aktiven Modus erfolgt automatisch. Die autonome Entscheidung von ARP, automatisch vom Lernmodus in den aktiven Modus zu wechseln, basiert auf den Konfigurationseinstellungen der folgenden Optionen:

```
-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
```


Nach 30 Lerntagen wird ein Volumen automatisch in den aktiven Modus geschaltet, auch wenn eine oder mehrere dieser Bedingungen nicht erfüllt sind. Das heißt, wenn die automatische Umschaltung aktiviert ist, wechselt die Lautstärke nach maximal 30 Tagen in den aktiven Modus. Der Maximalwert von 30 Tagen ist festgelegt und kann nicht geändert werden.

Weitere Informationen zu ARP-Konfigurationsoptionen, einschließlich Standardwerten, finden Sie im ["Befehlsreferenz für ONTAP"](#).

Schritte

Sie können System Manager oder die ONTAP-CLI verwenden, um ARP standardmäßig zu aktivieren.

System Manager

1. Wählen Sie **Speicher > Speicher-VMs** und wählen Sie dann die Speicher-VM aus, die Volumes enthält, die Sie mit ARP schützen möchten.
2. Navigieren Sie zur Registerkarte **Einstellungen**. Suchen Sie unter **Sicherheit** die **Anti-Ransomware**-Kachel und wählen Sie aus 
3. Aktivieren Sie das Kontrollkästchen, um ARP für NAS-Volumes zu aktivieren. Aktivieren Sie das Zusatzfeld, um ARP auf allen in Frage kommenden NAS-Volumes in der Speicher-VM zu aktivieren.



Wenn Sie ein Upgrade auf ONTAP 9.13.1 durchgeführt haben, wird die Einstellung **nach ausreichend Lernen automatisch vom Lernmodus zum aktiven Modus wechseln** automatisch aktiviert. Auf diese Weise kann ARP das optimale Lernintervall bestimmen und den Wechsel zum aktiven Modus automatisieren. Deaktivieren Sie die Einstellung, wenn Sie manuell in den aktiven Modus wechseln möchten.

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]
```

Wenn Sie ein Upgrade auf ONTAP 9.13.1 oder höher durchgeführt haben, ist das adaptive Lernen aktiviert, sodass die Änderung des aktiven Status automatisch erfolgt. Wenn dieses Verhalten nicht automatisch aktiviert werden soll, verwenden Sie den folgenden Befehl:

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

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.

Ab ONTAP 9.13.1 können Sie die Multi-Admin-Verifizierung (MAV) aktivieren, sodass mindestens zwei authentifizierte Benutzeradministratoren zum Anhalten des ARP erforderlich sind. "[Weitere Informationen](#)".

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 die ARP-Deaktivierungsfunktion nicht, 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.

Schritte

Sie können System Manager oder die ONTAP-CLI verwenden, um ARP anzuhalten.

System Manager

1. Wählen Sie **Speicher > Volumes** und wählen Sie dann das Volume aus, auf dem Sie ARP anhalten möchten.
2. Wählen Sie auf der Registerkarte **Sicherheit** der Volumes-Übersicht **Anti-Ransomware anhalten** im Feld **Anti-Ransomware** aus.



Wenn Sie ab ONTAP 9.13.1 MAV zum Schutz Ihrer ARP-Einstellungen verwenden, werden Sie durch den Pause-Vorgang aufgefordert, die Genehmigung eines oder mehrerer zusätzlicher Administratoren einzuholen. **"Die Genehmigung muss von allen Administratoren eingeholt werden"** Der MAV-Genehmigungsgruppe zugeordnet oder der Vorgang schlägt fehl.

CLI

1. ARP auf einem Volume anhalten:

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

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

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

3. **Wenn Sie MAV (verfügbar mit ARP ab ONTAP 9.13.1) zum Schutz Ihrer ARP-Einstellungen verwenden**, fordert Sie der Pausenvorgang auf, die Genehmigung eines oder mehrerer zusätzlicher Administratoren einzuholen. Die Genehmigung muss von allen Administratoren, die mit der MAV-Genehmigungsgruppe verknüpft sind, eingeholt werden. Andernfalls schlägt der Vorgang fehl.

Wenn Sie MAV verwenden und für einen erwarteten Pausenbetrieb zusätzliche Genehmigungen erforderlich sind, führt jeder Genehmiger der MAV-Gruppe Folgendes durch:

- a. Anfrage anzeigen:

```
security multi-admin-verify request show
```

- b. Genehmigen Sie die Anforderung:

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

Die Antwort für den letzten Gruppengenehmiger zeigt an, dass das Volume geändert wurde und der Status von ARP angehalten wurde.

Wenn Sie MAV verwenden und ein Genehmiger der MAV-Gruppe sind, können Sie eine Anforderung für einen Pause-Vorgang ablehnen:

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


Managen Sie die Parameter für die Erkennung von Angriffen gegen autonomen Ransomware-Schutz

Ab ONTAP 9.11.1 können Sie die Parameter für die Ransomware-Erkennung auf einem bestimmten Volume mit aktiviertem Autonomem Ransomware-Schutz ändern und einen bekannten Anstieg als normale Dateiaktivität melden. Durch die Anpassung der Erkennungsparameter wird die Genauigkeit der Berichterstellung auf der Grundlage Ihrer spezifischen Volumenbelastung verbessert.

Wie die Angriffserkennung funktioniert

Wenn sich der Autonomous Ransomware Protection (ARP) im Lernmodus befindet, werden Grundwerte für das Volume-Verhalten entwickelt. Es handelt sich um Entropie, Dateierweiterungen und – seit ONTAP 9.11.1 – IOPS. Diese Baselines dienen zur Bewertung von Ransomware-Bedrohungen. Weitere Informationen zu diesen Kriterien finden Sie unter [Was ARP erkennt](#).

In ONTAP 9.10.1 gibt ARP eine Warnung aus, wenn beide der folgenden Bedingungen erkannt werden:

- Mehr als 20 Dateien mit Dateierweiterungen, die bisher nicht im Volume beobachtet wurden
- Hohe Entropie-Daten

Ab ONTAP 9.11.1 gibt ARP eine Bedrohungswarnung aus, wenn *only* eine Bedingung erfüllt ist. Wenn beispielsweise mehr als 20 Dateien mit Dateierweiterungen, die zuvor nicht im Volume beobachtet wurden, innerhalb eines Zeitraums von 24 Stunden beobachtet werden, kategorisiert ARP diese Datei als Bedrohung *unabhängig* der beobachteten Entropie. (Die Dateiwerte 24 Stunden und 20 Stunden sind Standardwerte, die geändert werden können.)

Ab ONTAP 9.14.1 können Sie Alarmer konfigurieren, wenn ARP eine neue Dateierweiterung beobachtet, und wenn ARP einen Snapshot erstellt. Weitere Informationen finden Sie unter [\[modify-alerts\]](#)

Bestimmte Volumes und Workloads erfordern unterschiedliche Erkennungsparameter. Zum Beispiel kann Ihr ARP-fähiges Volume zahlreiche Arten von Dateierweiterungen hosten. In diesem Fall möchten Sie die Schwellenwertanzahl für nie zuvor gesehene Dateierweiterungen auf eine Zahl ändern, die größer ist als die Standardeinstellung von 20 oder Warnungen deaktivieren, die auf nie zuvor gesehenen Dateierweiterungen basieren. Ab ONTAP 9.11.1 können Sie die Parameter zur Angriffserkennung anpassen, um sie besser auf Ihre spezifischen Workloads anzupassen.

Parameter für die Angriffserkennung ändern

Je nach erwartetem Verhalten des ARP-aktivierten Volumens können Sie die Angriffserkennungsparameter ändern.

Schritte

1. Anzeigen der vorhandenen Angriffserkennungsparameter:

```
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 voll1
```

```

Vserver Name : vs1
Volume Name : voll1
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. Alle angezeigten Felder können mit booleschen oder ganzzahligen Werten geändert werden. Um ein Feld zu ändern, verwenden Sie die `security anti-ransomware volume attack-detection-parameters modify` Befehl.

Eine vollständige Liste der Parameter finden Sie unter "[Befehlsreferenz für ONTAP](#)".

Bekannte Überspannungen melden

ARP ändert auch im aktiven Modus weiterhin Basiswerte für Erkennungsparameter. Wenn Sie von Überspannungen in Ihrer Volumenaktivität wissen - entweder einmal Überspannungen oder eine Überspannung, die für eine neue Normalität charakteristisch ist - sollten Sie sie als sicher melden. Die manuelle Meldung dieser Überspannungen als sicher hilft, die Genauigkeit der ARP-Bedrohungsbewertungen zu verbessern.

Melden Sie eine einmalige Überspannung

1. Wenn ein einmaliger Anstieg unter bekannten Umständen auftritt und Sie möchten, dass ARP in Zukunft einen ähnlichen Anstieg meldet, beheben Sie den Anstieg des Workload-Verhaltens:

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

Änderung des Basisliniensprunges

1. Wenn eine gemeldete Überspannung als normales Anwendungsverhalten betrachtet werden sollte, melden Sie den Überspannungswert als solche, um den Überspannungswert der Basislinie zu ändern.

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

Konfigurieren von ARP-Warnungen

Ab ONTAP 9.14.1 ermöglicht ARP die Angabe von Warnungen für zwei ARP-Ereignisse:

- Beobachtung der neuen Dateierweiterung auf einem Volume
- Erstellung eines ARP-Snapshots

Warnmeldungen für diese beiden Ereignisse können für einzelne Volumes oder für die gesamte SVM festgelegt werden. Wenn Sie Alarmer für die SVM aktivieren, werden die Meldungseinstellungen nur von Volumes übernommen, die nach dem Aktivieren der Warnmeldung erstellt wurden. Standardmäßig sind Warnmeldungen auf keinem Volume aktiviert.


Ereigniswarnungen können durch Verifizierung durch mehrere Administratoren gesteuert werden. Weitere Informationen finden Sie unter [Verifizierung mehrerer Administratoren mit Volumes, die mit ARP gesichert sind](#).

System Manager

Festlegen von Warnmeldungen für ein Volume

1. Navigieren Sie zu **Volumen**. Wählen Sie das einzelne Volume aus, für das Sie die Einstellungen ändern möchten.
2. Wählen Sie die Registerkarte **Sicherheit** und dann **Ereignissicherheitseinstellungen**.
3. Um Warnungen für **Neue Dateierweiterung entdeckt** und **Ransomware Snapshot erstellt** zu erhalten, wählen Sie das Dropdown-Menü unter der Überschrift **Schweregrad**. Ändern Sie die Einstellung von **Ereignis nicht generieren in Hinweis**.
4. Wählen Sie **Speichern**.

Festlegen von Warnmeldungen für eine SVM

1. Navigieren Sie zu **Storage VM**, und wählen Sie dann die SVM aus, für die Sie Einstellungen aktivieren möchten.
2. Suchen Sie unter der Überschrift **Sicherheit** die **Anti-Ransomware**-Karte. Wählen Sie  Dann **Ransomware-Ereignis-Schweregrad bearbeiten**.
3. Um Warnungen für **Neue Dateierweiterung entdeckt** und **Ransomware Snapshot erstellt** zu erhalten, wählen Sie das Dropdown-Menü unter der Überschrift **Schweregrad**. Ändern Sie die Einstellung von **Ereignis nicht generieren in Hinweis**.
4. Wählen Sie **Speichern**.

CLI

Festlegen von Warnmeldungen für ein Volume

- So legen Sie Warnungen für eine neue Dateierweiterung fest:

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

- So legen Sie Warnungen für die Erstellung eines ARP-Snapshots fest:

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

- Bestätigen Sie Ihre Einstellungen mit dem `anti-ransomware volume event-log show` Befehl.

Festlegen von Warnmeldungen für eine SVM

- So legen Sie Warnungen für eine neue Dateierweiterung fest:

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

- So legen Sie Warnungen für die Erstellung eines ARP-Snapshots fest:

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

- Bestätigen Sie Ihre Einstellungen mit dem `security anti-ransomware vserver event-log show` Befehl.

Weitere Informationen

- ["Autonome Ransomware-Schutzangriffe und den Überblick über den autonomen Ransomware-Schutz"](#)

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 akzeptabel ist (falsch positiv) oder ob ein Angriff schädlich erscheint.

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.

- **Potenzieller Ransomware-Angriff**

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

In beiden Fällen wird die normale Überwachung nach der Aktualisierung und dem Löschen der Benachrichtigungen fortgesetzt. ARP zeichnet Ihre Bewertung im Bedrohungsprofil auf und verwendet Ihre Wahl zur Überwachung der nachfolgenden Dateiaktivitäten.

Im Falle eines vermuteten Angriffs müssen Sie feststellen, ob es sich um einen Angriff handelt, darauf reagieren, wenn er der Fall ist, und geschützte Daten wiederherstellen, bevor Sie die Benachrichtigungen löschen. ["Erfahren Sie mehr darüber, wie Sie nach einem Ransomware-Angriff wiederherstellen können"](#).



Wenn Sie ein gesamtes Volume wiederherstellen, müssen keine Hinweise gelöscht werden.

Bevor Sie beginnen

ARP muss im aktiven Modus ausgeführt werden.

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um auf eine anormale Aufgabe zu reagieren.

System Manager


1. Wenn Sie eine Benachrichtigung über „anormale Aktivität“ erhalten, folgen Sie dem Link oder navigieren Sie zur Registerkarte **Sicherheit** in der Übersicht **Volumes**.

Warnungen werden im Fenster **Übersicht** des Menüs **Ereignisse** angezeigt.

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

Wählen Sie auf der Registerkarte **Sicherheit** die Option **vermutete Dateitypen anzeigen** aus.

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	<p>Wählen Sie Update und Suspect File Types löschen, um Ihre Entscheidung zu erfassen und die normale ARP-Überwachung fortzusetzen.</p> <div><p>Wenn Sie ab ONTAP 9.13.1 MAV zum Schutz Ihrer ARP-Einstellungen verwenden, werden Sie durch den Clear-Suspect-Vorgang aufgefordert, die Genehmigung eines oder mehrerer zusätzlicher Administratoren einzuholen. "Die Genehmigung muss von allen Administratoren eingeholt werden" Der MAV-Genehmigungsgruppe zugeordnet oder der Vorgang schlägt fehl.</p></div>
Möglicher Angriff Durch Ransomware	<p>Reagieren Sie auf den Angriff und stellen Sie geschützte Daten wieder her. Wählen Sie dann Update und Suspect File Types löschen, um Ihre Entscheidung aufzuzeichnen und die normale ARP-Überwachung fortzusetzen.</p> <p>Es gibt keine verdächtigen Dateitypen, die gelöscht werden müssen, wenn Sie ein ganzes Volume wiederhergestellt haben.</p>

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 Dateieindungen:

◦ Falsch positiv

Geben Sie den folgenden Befehl ein, um Ihre Entscheidung aufzuzeichnen, die neue Erweiterung zur Liste der zulässigen hinzuzufügen und die normale Anti-Ransomware-Überwachung fortzusetzen:

```
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 ["Wiederherstellen von Daten aus dem ARP-erstellten Backup-Snapshot"](#). Nachdem die Daten wiederhergestellt wurden, geben Sie 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. Der von ARP erstellte Backup-Snapshot wird entfernt und der Angriffsbericht wird gelöscht.

5. Wenn Sie MAV und ein erwartetes verwenden `clear-suspect` Für den Betrieb sind zusätzliche Genehmigungen erforderlich. Jeder Genehmiger der MAV-Gruppe führt die folgenden Schritte aus:

- a. Anfrage anzeigen:

```
security multi-admin-verify request show
```

- b. Genehmigen Sie die Anforderung, das normale Anti-Ransomware-Monitoring fortzusetzen:

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

Die Antwort für den letzten Gruppengenehmiger zeigt an, dass das Volume geändert und ein false positive aufgezeichnet wurde.

6. Wenn Sie MAV verwenden und ein Genehmiger der MAV-Gruppe sind, können Sie auch eine eindeutige Anforderung ablehnen:

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

Weitere Informationen

- ["KB: Snapshots zum autonomen Ransomware-Schutz – Informationen zu Angriffen und dem autonomen Ransomware-Schutz"](#).

Wiederherstellung von Daten nach einem Ransomware-Angriff

Autonomous Ransomware Protection (ARP) erstellt Snapshot-Kopien mit dem Namen `Anti_ransomware_backup` Potenzielle Ransomware-Bedrohungen werden erkannt. Sie können eine dieser ARP Snapshot Kopien oder eine andere Snapshot Kopie Ihres Volumes zum Wiederherstellen von Daten verwenden.

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.

Zum Wiederherstellen aus einem anderen Snapshot als dem `Anti_ransomware_backup` Snapshot Nachdem ein Systemangriff erkannt wurde, müssen Sie den ARP-Snapshot zuerst freigeben.

Wenn kein Systemangriff gemeldet wurde, müssen Sie zuerst vom wiederherstellen `Anti_ransomware_backup` Snapshot-Kopie dann eine nachfolgende Wiederherstellung des Volume von der Snapshot-Kopie Ihrer Wahl abschließen.


Schritte

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

System Manager


Wiederherstellung nach einem Systemangriff

1. fahren Sie mit Schritt 2 fort, um die Wiederherstellung aus dem ARP-Snapshot durchzuführen. Um Restores aus einer früheren Snapshot Kopie durchzuführen, müssen Sie zuerst die Sperre des ARP Snapshot freigeben.
 - a. Wählen Sie **Storage > Volumes**.
 - b. Wählen Sie **Sicherheit** und dann **vermutete Dateitypen anzeigen**
 - c. Markieren Sie die Dateien als "falsch positiv" .
 - d. Wählen Sie **Update** und **Verdächtige Dateitypen löschen**
2. Anzeige der Snapshot Kopien in Volumes:

Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies** aus.
3. Wählen Sie  Neben der Snapshot Kopie, die Sie wiederherstellen möchten, dann **Wiederherstellen**.

Wiederherstellung, wenn ein Systemangriff nicht erkannt wurde

1. Anzeige der Snapshot Kopien in Volumes:

Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies** aus.
2. Wählen Sie  Sie wählen die aus `Anti_ransomware_backup` Snapshot:
3. Wählen Sie **Wiederherstellen**.
4. Kehren Sie zum Menü **Snapshot Kopien** zurück und wählen Sie dann die Snapshot Kopie aus, die Sie verwenden möchten. Wählen Sie **Wiederherstellen**.

CLI

Wiederherstellung nach einem Systemangriff

1. fahren Sie mit Schritt zwei fort, um die Wiederherstellung aus der ARP Snapshot Kopie durchzuführen. Um Daten aus früheren Snapshot Kopien wiederherzustellen, müssen Sie die Sperre des ARP Snapshot freigeben.



Die Anti-Ransomware-SnapLock muss nur freigegeben werden, wenn Sie die verwenden, bevor die Daten aus früheren Snapshot Kopien wiederhergestellt werden `volume snap restore` Wie unten beschrieben. Wenn Sie Daten mit Flex Clone, Single File Snap Restore oder anderen Methoden wiederherstellen, ist dies nicht erforderlich.

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“.

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 voll1:

```
clus1::> volume snapshot show -vserver vs1 -volume voll1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
-----	-----	-----	-----	-----	-----	-----
vs1	voll1	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 voll1:

```
cluster1::> volume snapshot restore -vserver vs0 -volume voll1  
-snapshot daily.2013-01-25_0010
```

Wiederherstellung, wenn ein Systemangriff nicht erkannt wurde

1. 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 voll1:

```
clus1::> volume snapshot show -vserver vs1 -volume voll
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	voll	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. 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 voll:

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

3. Wiederholen Sie die Schritte 1 und 2, um das Volume mithilfe der Desire Snapshot-Kopie wiederherzustellen.

Weitere Informationen

- ["KB: Schutz vor Ransomware und Recovery in ONTAP"](#)

Optionen für automatische Snapshot-Kopien ändern

Ab ONTAP 9.11.1 können Sie die CLI verwenden, um die Aufbewahrungseinstellungen für ARP-Snapshot Kopien (Autonomous Ransomware Protection) zu steuern, die als Reaktion auf vermutete Ransomware-Angriffe automatisch generiert werden.

Bevor Sie beginnen

Sie können nur ARP-Snapshot-Optionen auf einer Node-SVM ändern.

Schritte

1. Um alle aktuellen Einstellungen von ARP Snapshot Kopien anzuzeigen, geben Sie Folgendes ein:

```
vserver options -vserver svm_name arw*
```



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


2. Um die ausgewählten aktuellen Einstellungen von ARP Snapshot Kopien anzuzeigen, geben Sie Folgendes ein:

```
vserver options -vserver svm_name -option-name arw_setting_name
```

3. 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
```

Die folgenden Einstellungen können geändert werden:

ARW-Einstellung	Beschreibung
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 <i>in Stunden</i> zwischen ARP Snapshot Kopien an. Bei Verdacht eines Angriffs wird eine neue Snapshot Kopie erstellt, und die zuvor erstellte Kopie ist älter als dieses angegebene Intervall.
arw.snap.normal.retain.interval.hours	Gibt die Dauer <i>in Stunden</i> 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	<p>Gibt die maximale Dauer <i>in Tagen</i> 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.</p> <p>+</p> <div>  <p>Das maximale Aufbewahrungsintervall für ARP Snapshot Kopien wird ignoriert, wenn eine mäßige Bedrohung erkannt wird. Die als Antwort auf die Bedrohung erstellte ARP Snapshot-Kopie wird beibehalten, bis Sie auf die Bedrohung reagiert haben. Wenn eine Bedrohung als falsch positiv markiert wird, löschen Sie die ARP Snapshot Kopien auf dem Volume.</p> </div>
arw.snap.create.interval.hours.post.max.count	Gibt das Intervall <i>in Stunden</i> zwischen ARP Snapshot Kopien an, wenn das Volume bereits die maximale Anzahl an 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 <i>in Tagen</i> zwischen ARP-Überspannungs-Snapshot-Kopien an. ONTAP erzeugt eine ARP Snapshot Überspannungskopie, wenn ein Anstieg des IO-Verkehrs auftritt, und die letzte erstellte ARP Snapshot-Kopie ist älter als dieses angegebene Intervall. Mit dieser Option wird auch die Aufbewahrungsfrist <i>in Tag</i> für einen ARP-Überspannungsabgleich festgelegt.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.