ARP 9.10.1 bis 9.15.1

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/anti-ransomware/learn-about-arp.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

ARP 9.10.1 bis 9.15.1 . . . 1
Informationen zu ONTAP ARP (ONTAP 9.10.1 bis 9.15.1) . . . 1
Was ARP erkennt . . . 1
Aktivierungsoptionen für ARP . . . 1
ARP-Schutzmodi . . . 1
Gefährdungsanalyse . . . 2
ARP Snapshots . . . 3
Auf einen Angriff reagieren und ihn bewerten . . . 3
Daten nach einem Angriff wiederherstellen . . . 4
Multi-Admin-Verifizierung . . . 4
ONTAP ARP unterstützte Konfigurationen . . . 4
Geeignete Workloads . . . 4
Ungeeignete Workloads . . . 5
Unterstützte Konfigurationen . . . 5
SnapMirror und ARP Interoperabilität . . . 6
Nicht unterstützte Konfigurationen . . . 6
Leistungs- und Volumengrenzen . . . 7
Multi-Admin-Verifizierung mit ARP-geschützten Volumes . . . 7
ARP aktivieren . . . 7
ONTAP ARP auf einem Volume aktivieren . . . 7
ONTAP ARP ist in neuen Volumes standardmäßig aktiviert . . . 11
Nach einer Lernphase in den aktiven Modus von ONTAP ARP in ONTAP wechseln . . . 13
Nach einer Lernphase manuell in den aktiven Modus wechseln . . . 13
Automatische Umschaltung vom Lernmodus in den aktiven Modus . . . 14
ONTAP ARP-Angriffserkennungsparameter verwalten . . . 14
Wie die Erkennung von ARP-Angriffen funktioniert . . . 15
Parameter zur Erkennung von ARP-Angriffen anpassen . . . 15
Bekannte Anstiege melden . . . 16
ARP-Warnmeldungen konfigurieren . . . 17
Auf von ONTAP ARP erkannte abnormale Aktivitäten reagieren . . . 18
Details zu abnormalen Aktivitäten prüfen . . . 19
Snapshot-Verhalten beim Löschen eines vermuteten Ereignisses . . . 20
Als falsch positiv einstufen und Überwachung fortsetzen . . . 21
Als potenziellen Ransomware-Angriff einstufen und Daten wiederherstellen . . . 21
Daten nach einem Ransomware-Angriff mit ONTAP ARP wiederherstellen . . . 22
Wählen Sie eine Wiederherstellungsmethode . . . 23
Einschränkungen und Überlegungen zur Wiederherstellung . . . 23
Wiederherstellung nach einem Systemangriff . . . 24
Wiederherstellung, wenn kein Angriff erkannt wird . . . 26
Einstellungen für automatisch generierte ONTAP ARP Snapshots anpassen . . . 27

ARP 9.10.1 bis 9.15.1

Informationen zu ONTAP ARP (ONTAP 9.10.1 bis 9.15.1)

Für ONTAP 9.10.1 bis 9.15.1 überwacht der Autonomous Ransomware Protection (ARP) NAS-Umgebungen mithilfe einer Lernphase, um Verhaltensbaselines zu erstellen, bevor auf die aktive Ransomware-Erkennung umgeschaltet wird. ARP analysiert Datenentropie, Änderungen der Dateierweiterungen und Datei-IOPS-Muster, um potenzielle Ransomware-Angriffe zu erkennen. Für FlexGroup Volumes gilt das ursprüngliche ARP-Modell ebenfalls bis ONTAP 9.17.1.

> Das ursprüngliche ARP-Modell erhielt nach ONTAP 9.14.1 keine neuen funktionalen Verbesserungen. Bei Verwendung von ONTAP 9.16.1 oder höher auf FlexVol Volumes siehe "Informationen zu ARP/KI". FlexGroup Volumes verwenden das ursprüngliche ARP-Modell bis einschließlich ONTAP 9.17.1 und werden ab ONTAP 9.18.1 von ARP/AI unterstützt.

Was ARP erkennt

ARP identifiziert eingehende Daten als entweder verschlüsselt oder Klartext und verwendet die folgenden diskreten Signale, um Ransomware-Aktivität zu erkennen:

- **Entropie**: Eine Bewertung der Zufälligkeit von Daten in einer Datei (nur NAS)
- **Dateierweiterungstypen**: Eine Dateierweiterung, die nicht den erwarteten Erweiterungstypen entspricht (nur NAS)
- **Datei-IOPS**: Ein Anstieg der ungewöhnlichen Volumenaktivität mit Datenverschlüsselung (nur NAS; ONTAP 9.11.1 und später)

ARP erkennt die Ausbreitung der meisten Ransomware-Angriffe bereits nach der Verschlüsselung einer geringen Anzahl von Dateien, reagiert automatisch zum Schutz der Daten und benachrichtigt Sie, dass ein vermuteter Angriff stattfindet.

> Kein Ransomware-Erkennungssystem kann vollständige Sicherheit garantieren. ARP bietet eine zusätzliche Schutzebene, falls die Antivirensoftware einen Eindringling nicht erkennt.

Aktivierungsoptionen für ARP

ARP wird manuell pro Volume aktiviert oder standardmäßig auf SVM-Ebene für neue Volumes konfiguriert.

- Um ARP standardmäßig auf allen neuen Volumes für eine SVM zu aktivieren, siehe "ARP standardmäßig in neuen Volumes aktivieren".
- Zur Aktivierung von ARP auf einem bestimmten Volume siehe "ARP auf einem Volume aktivieren".

ARP-Schutzmodi

ARP beginnt im Lernmodus, um eine Verhaltensbasislinie zu etablieren, bevor auf aktive Erkennung umgeschaltet wird.

NAS-Volumes

Die folgende Tabelle fasst die ARP-Modi für NAS-Umgebungen zusammen.

Modus	Beschreibung	Volume-Typen und Versionen
Lernen	Wenn ARP aktiviert wird, wird es automatisch in den Lernmodus versetzt. Im Lernmodus entwickelt das ONTAP-System ein Warnprofil basierend auf den Analysebereichen: Entropie, Dateierweiterungstypen und Datei-IOPS. Es wird empfohlen, ARP 30 Tage lang im Lernmodus zu belassen. Ab ONTAP 9.13.1 ermittelt ARP automatisch das optimale Lernintervall und automatisiert die Umstellung, die auch vor Ablauf der 30 Tage erfolgen kann. Bei Versionen vor ONTAP 9.13.1 kann die Umstellung manuell vorgenommen werden. "Weitere Informationen zum Wechsel vom Lern- in den Aktivmodus". Der Befehl `security anti-ransomware volume workload-behavior show` zeigt die im Volume erkannten Dateierweiterungen an. Wenn dieser Befehl früh im Lernmodus ausgeführt wird und eine korrekte Darstellung der Dateitypen liefert, sollten diese Daten nicht als Grundlage für den Wechsel in den aktiven Modus verwendet werden, da ONTAP noch weitere Metriken erfasst. Weitere Informationen zu `security anti-ransomware volume workload-behavior show` finden sich in der "ONTAP-Befehlsreferenz".	• FlexVol Volumes mit ONTAP 9.10.1 bis 9.15.1 • FlexGroup Volumes mit ONTAP 9.13.1 bis 9.17.1
Aktiv	Nach der Lernphase überwacht ARP die Arbeitslastaktivität und reagiert automatisch, wenn ungewöhnliches Verhalten erkannt wird. Wird eine Dateierweiterung als ungewöhnlich markiert, sollte die Warnung bewertet werden. Es besteht die Möglichkeit, auf die Warnung zu reagieren, um die Daten zu schützen, oder die Warnung als Fehlalarm zu kennzeichnen. Das Kennzeichnen einer Warnung als Fehlalarm aktualisiert das Warnungsprofil. Wird die Warnung beispielsweise durch eine neue Dateierweiterung ausgelöst und als Fehlalarm markiert, erfolgt beim nächsten Auftreten dieser Dateierweiterung keine Warnung mehr.	• FlexVol Volumes mit ONTAP 9.10.1 bis 9.15.1 • FlexGroup Volumes mit ONTAP 9.13.1 bis 9.17.1

Gefährdungsanalyse

ARP bewertet die Bedrohungswahrscheinlichkeit anhand zweier Ebenen:

- **Niedrig**: Die früheste Erkennung einer Anomalie im Volume (zum Beispiel wird eine neue Dateierweiterung im Volume festgestellt). Diese Erkennungsstufe ist nur im ursprünglichen ARP-Modell verfügbar.
  - Ab ONTAP 9.11.1 können Sie "die Erkennungsparameter für ARP anpassen".
- **Mittel**: Es wird eine hohe Entropie erkannt oder es werden mehrere Dateien mit derselben, bisher nie gesehenen Dateiendung beobachtet. Die Bedrohung eskaliert auf mittel, nachdem ONTAP einen Analysebericht ausgeführt hat, um festzustellen, ob die Anomalie einem Ransomware-Profil entspricht. Bei mittlerer Angriffswahrscheinlichkeit generiert ONTAP eine EMS-Benachrichtigung, die Sie zur Bewertung

der Bedrohung auffordert.

ONTAP sendet keine Warnungen bei niedrigen Bedrohungen; ab ONTAP 9.14.1 können Sie jedoch "Standard-Benachrichtigungseinstellungen ändern". Weitere Informationen finden Sie unter "Auf abnormale Aktivität reagieren".

Informationen zu Bedrohungen mittlerer Intensität sind im Abschnitt **Ereignisse** des System Manager oder mit dem `security anti-ransomware volume show` Befehl verfügbar. Ereignisse mit geringer Bedrohung können ebenfalls mit dem `security anti-ransomware volume show` Befehl angezeigt werden. Weitere Informationen zu `security anti-ransomware volume show` finden sich in der "ONTAP-Befehlsreferenz".

ARP Snapshots

ARP erstellt einen Snapshot, sobald erste Anzeichen eines Angriffs erkannt werden. Anschließend erfolgt eine detaillierte Analyse, um den potenziellen Angriff zu bestätigen oder auszuschließen. Da ARP Snapshots proaktiv erstellt werden, noch bevor ein Angriff vollständig bestätigt ist, sollte deren Vorhandensein nicht als Anomalie betrachtet werden. Wenn ein wahrscheinlicher Angriff bestätigt wird, wird die Angriffswahrscheinlichkeit auf `Moderate` eskaliert und eine Angriffsbenachrichtigung generiert.

Ab ONTAP 9.11.1 können Sie "Aufbewahrungseinstellungen für Snapshots ändern".

Die folgende Tabelle fasst das Verhalten von ARP Snapshots zusammen.

Funktion	Originales ARP Modell (ONTAP 9.15.1 und früher)
Auslöser für die Erstellung	• Hohe Entropie wird erkannt • Eine neue Dateierweiterung wird erkannt • Ein Anstieg der Dateivorgänge wird erkannt (ONTAP 9.11.1 und höher) Das Snapshot-Erstellungsintervall basiert auf dem Auslösertyp.
Konvention für vorangestellte Namen	"Anti_ransomware_backup"
Löschverhalten	Der ARP Snapshot ist gesperrt und kann vom Administrator nicht gelöscht werden.
Maximale Snapshot-Anzahl	"Konfigurierbares Limit für sechs Snapshots"
Aufbewahrungsfrist	• Wird anhand von Auslösebedingungen bestimmt (nicht festgelegt) • Vor dem Angriff erstellte Snapshots werden aufbewahrt, bis der Administrator den Angriff als echt oder als Fehlalarm (clear-suspect) markiert.
Clear-suspect-Aktion	Administratoren können eine „clear-suspect“-Aktion durchführen, um die Warnung zu beseitigen und gesperrte Snapshots freizugeben.
Ablaufzeit	Keine

Auf einen Angriff reagieren und ihn bewerten

ARP erstellt gesperrte Snapshots, sobald erste Anzeichen eines Angriffs erkannt werden. Es muss bestätigt werden, ob es sich um einen tatsächlichen Angriff oder einen Fehlalarm handelt. Gesperrte Snapshots können nicht auf normalem Wege gelöscht werden. Wird der Angriff später als Fehlalarm eingestuft, löscht ONTAP die

gesperrte Kopie.

- "Auf abnormale Aktivität reagieren: ARP"
- "Feststellen, ob ein Ransomware-Angriff tatsächlich vorliegt"

Daten nach einem Angriff wiederherstellen

Wird der Angriff bestätigt, kann das Volume mithilfe des ARP Snapshots wiederhergestellt werden. Sie können betroffene Dateien aus ausgewählten Snapshots wiederherstellen, anstatt das gesamte Volume zurückzusetzen.

- "Daten aus ARP Snapshots wiederherstellen"
- "Wiederherstellung aus ONTAP Snapshots"
- "Intelligente Ransomware-Wiederherstellung"

Multi-Admin-Verifizierung

Ab ONTAP 9.13.1 wird empfohlen, die Multi-Admin-Verifizierung (MAV) zu aktivieren, sodass für die ARP-Konfiguration zwei oder mehr authentifizierte Benutzeradministratoren erforderlich sind. Weitere Informationen finden sich unter "Multi-Admin-Verifizierung aktivieren".

Verwandte Informationen

- "ARP unterstützte Konfigurationen"
- "ONTAP-Befehlsreferenz"

ONTAP ARP unterstützte Konfigurationen

Autonomous Ransomware Protection (ARP) ist für NAS-Workloads ab ONTAP 9.10.1 bis ONTAP 9.15.1 verfügbar. Vor der Bereitstellung von ARP sind die empfohlenen Anwendungsfälle, unterstützten Konfigurationen sowie die Auswirkungen auf die Leistung zu beachten.

ARP/AI ist das aktuelle ONTAP Ransomware-Schutzmodell für ONTAP 9.16.1 und höher. Bei Verwendung von ONTAP 9.16.1 oder höher siehe "Unterstützte Konfigurationen für ARP/AI".

Geeignete Workloads

ARP eignet sich für folgende Arten von Arbeitslasten:

- Datenbanken auf NFS-Speicher
- Windows oder Linux Home-Verzeichnisse

  Benutzer können Dateien mit Erweiterungen erstellen, die während der Lernphase nicht erkannt werden, daher besteht bei dieser Arbeitslast eine größere Wahrscheinlichkeit für falsch positive Ergebnisse.

- Bilder und Videos

  Zum Beispiel Gesundheitsdatensätze und Electronic Design Automation (EDA)-Daten

Ungeeignete Workloads

ARP ist für diese Arten von Arbeitslasten nicht geeignet:

- Arbeitslasten mit einer hohen Frequenz von Datei-Erstellungs- oder -Löschvorgängen (Hunderttausende von Dateien in wenigen Sekunden, zum Beispiel Test-/Entwicklungsarbeitslasten).

  Die Bedrohungserkennung von ARP beruht auf der Fähigkeit, einen ungewöhnlichen Anstieg von Datei-Erstellungs-, Umbenennungs- oder Löschvorgängen zu erkennen. Wenn die Anwendung selbst die Quelle der Dateiaktivität ist, kann sie nicht effektiv von Ransomware-Aktivität unterschieden werden.

- Workloads auf Volumes mit mehr als 4.000 einzigartigen Dateierweiterungen.

  ARP (ONTAP 9.10.1 bis 9.15.1) kann bis zu 4.000 Dateierweiterungen pro Volume analysieren. Wenn die Anzahl der eindeutigen Dateierweiterungen auf einem Volume dieses Limit überschreitet, kann ARP Ransomware-Aktivitäten nicht effizient erkennen und die Arbeitslast gilt als ungeeignet.

- Workloads, bei denen die Anwendung oder der Host Daten verschlüsselt.

  ARP basiert auf der Unterscheidung eingehender Daten als verschlüsselt oder unverschlüsselt. Wenn die Anwendung die Daten selbst verschlüsselt, ist die Effektivität der Funktion reduziert. ARP kann jedoch weiterhin anhand von Dateiaktivitäten (Löschen, Überschreiben oder Erstellen oder Erstellen oder Umbenennen mit neuer Dateiendung) und Dateityp arbeiten.

- SAN Workloads.

  ARP (9.10.1 bis 9.15.1) unterstützt keine SAN Volumes. SAN-Unterstützung wurde mit ARP/AI in ONTAP 9.17.1 eingeführt. "Weitere Informationen zu SAN sind in der ARP/AI-Dokumentation verfügbar."

Unterstützte Konfigurationen

ARP (9.10.1 bis 9.15.1) unterstützt NAS-Workloads über NFS- und SMB-Protokolle auf FlexVol Volumes und, beginnend mit ONTAP 9.13.1, auf FlexGroup Volumes.

Konfiguration	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
FlexVol Volumes (NAS)	✓	✓	✓	✓	✓	✓
FlexGroup Volumes (NAS)	✓	✓	✓			
Volumes mit SnapMirror asynchron	✓	✓	✓	✓		
SVMs mit SnapMirror asynchron (SVM-Notfallwiederherstellung)	✓	✓	✓	✓		

Konfiguration	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
SVM Datenmobilität (`vserver migrate`)	✓	✓	✓	✓		
Multi-Admin-Verifizierung (MAV)	✓	✓	✓			
MetroCluster Konfigurationen	✓	✓	✓	✓	✓	✓

SnapMirror und ARP Interoperabilität

Ab ONTAP 9.12.1 wird ARP auf SnapMirror asynchronen Ziel-Volumes unterstützt. SnapMirror synchron und SnapMirror active sync werden erst ab ONTAP 9.19.1 mit ARP/AI unterstützt.

Wenn ein SnapMirror Quellvolume ARP-fähig ist, übernimmt das SnapMirror Zielvolume automatisch den ARP-Konfigurationsstatus (wie `dry-run` oder `enabled`), die ARP-Trainingsdaten und den von ARP erstellten Snapshot des Quellvolumes. Für das Zielvolume ist keine separate Aktivierung für ARP erforderlich.

Solange ein Zielvolume aus schreibgeschützten (RO) Snapshots besteht, findet keine ARP-Verarbeitung der Daten statt. Wenn jedoch ein SnapMirror Zielvolume in ein schreibbares (RW) Volume umgewandelt wird, ist ARP auf dem RW-konvertierten Zielvolume automatisch aktiviert.

In ONTAP 9.10.1 und 9.11.1 werden bei SnapMirror der ARP-Konfigurationsstatus, die Trainingsdaten und die Snapshots nicht von Quell- auf Zielvolumes übertragen. Wenn das SnapMirror Zielvolume in den Lese-/Schreib-Modus umgewandelt wird, muss ARP auf dem Zielvolume nach der Umwandlung explizit im Lernmodus aktiviert werden.

Nicht unterstützte Konfigurationen

ARP unterstützt die folgenden Volumenkonfigurationen nicht:

- FlexCache Volumes (ARP wird auf Ursprungs FlexVol Volumes, aber nicht auf Cache Volumes unterstützt)
- Offline Volumes
- SnapLock Volumes
- SnapMirror synchron
- SnapMirror Active Sync
- SnapMirror asynchrone Ziel-Volumes in ONTAP 9.10.1 und 9.11.1 (unterstützt ab ONTAP 9.12.1)
- Eingeschränkte Volumes
- Root Volumes von Storage-VMs
- Volumes gestoppter Storage-VMs
- FlexVol zu FlexGroup Konvertierung (ARP muss vor der Konvertierung deaktiviert werden)

Leistungs- und Volumengrenzen

ARP hat nur minimale Auswirkungen auf die Systemleistung, gemessen an Durchsatz und maximalen IOPS. Die Auswirkungen der ARP-Funktion hängen von der jeweiligen Volume-Arbeitslast ab. Für gängige Arbeitslasten werden die folgenden Konfigurationsgrenzen empfohlen:

Arbeitsbelastungsmerkmale	Empfohlenes Volumenlimit pro Knoten	Leistungsverschlechterung bei Überschreitung des Volumenlimits pro Knoten [1]
Leseintensive oder die Daten können komprimiert werden	150	4 % der maximalen IOPS
Schreibintensiv und die Daten können nicht komprimiert werden	60	10 % der maximalen IOPS

[1] Die Systemleistung wird unabhängig von der Anzahl der über die empfohlenen Grenzwerte hinaus hinzugefügten Volumes nicht über diese Prozentsätze hinaus beeinträchtigt.

Da die ARP-Analysen in einer priorisierten Reihenfolge ausgeführt werden, werden die Analysen auf jedem Volume seltener ausgeführt, je mehr geschützte Volumes vorhanden sind.

> Die standardmäßige Aktivierung von ARP auf einer großen Anzahl neuer Volumes kann die Systemressourcennutzung erhöhen. Berücksichtigen Sie den Speicherplatzbedarf konkurrierender Prozesse wie Snapshots, wenn Sie ARP auf Volumes aktivieren.

Multi-Admin-Verifizierung mit ARP-geschützten Volumes

Ab ONTAP 9.13.1 kann die Multi-Admin-Verifizierung (MAV) für zusätzliche Sicherheit mit ARP aktiviert werden. MAV stellt sicher, dass mindestens zwei oder mehr authentifizierte Administratoren erforderlich sind, um ARP zu deaktivieren, ARP anzuhalten oder einen vermuteten Angriff auf einem geschützten Volume als Fehlalarm zu kennzeichnen. Informationen dazu, wie "MAV für ARP-geschützte Volumes aktivieren".

Sie müssen Administratoren für eine MAV-Gruppe definieren und MAV-Regeln für die `security anti-ransomware volume disable`, `security anti-ransomware volume pause` und `security anti-ransomware volume attack clear-suspect` Befehle erstellen, die Sie schützen möchten.

Weitere Informationen zu `security anti-ransomware volume disable`, `security anti-ransomware volume pause` und `security anti-ransomware volume attack clear-suspect` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "ARP auf einem Volume aktivieren"
- "ARP standardmäßig in neuen Volumes aktivieren"

ARP aktivieren

ONTAP ARP auf einem Volume aktivieren

Ab ONTAP 9.10.1 ist es möglich, den autonomen Ransomware-Schutz (ARP) auf bestehenden NAS-Volumes zu aktivieren oder neue Volumes mit aktiviertem ARP zu erstellen.

Wenn Sie ONTAP 9.16.1 oder höher verwenden, siehe "ARP/AI auf einem Volume aktivieren".

Über diese Aufgabe

ARP für NAS-Workloads (ONTAP 9.10.1 bis 9.15.1) startet im "Lernmodus" (`dry-run` Zustand). Das System analysiert die Workload, um normales Verhalten zu charakterisieren, bevor in den aktiven Modus zur Bedrohungserkennung gewechselt wird. Ein Beginn im aktiven Modus vor Abschluss der Lernphase kann zu einer übermäßigen Anzahl von Fehlalarmen führen.

Für ONTAP 9.10.1 bis 9.12.1 wird empfohlen, ARP mindestens 30 Tage lang im Lernmodus laufen zu lassen. Ab ONTAP 9.13.1 ermittelt ARP automatisch das optimale Lernintervall und automatisiert den Wechsel, der auch vor Ablauf der 30 Tage erfolgen kann.

ARP wird auf SAN-Volumes in ONTAP 9.10.1 bis 9.15.1 nicht unterstützt. Siehe "ARP unterstützte Konfigurationen".

In bestehenden Volumes gelten Lern- und Aktivmodus nur für neu geschriebene Daten, nicht für bereits vorhandene Daten im Volume. Die vorhandenen Daten werden nicht gescannt und analysiert, da die Eigenschaften des vorherigen normalen Datenverkehrs anhand der neuen Daten nach der Aktivierung des Volumes für ARP angenommen werden.

Nach der Aktivierung des autonomen Ransomware-Schutzes kann es je nach Umgebung und ONTAP Version zu einer Übergangsphase kommen:

Volumentyp	ONTAP Version	Verhalten nach der Aktivierung
NAS FlexGroup	ONTAP 9.18.1 und höher	ARP/KI ist sofort ohne Lernphase aktiv
	ONTAP 9.13.1 bis 9.17.1	ARP startet im Lernmodus für 30 Tage
NAS FlexVol	ONTAP 9.16.1 und höher	ARP/KI ist sofort ohne Lernphase aktiv
	ONTAP 9.10.1 bis 9.15.1	ARP startet im Lernmodus für 30 Tage
SAN-Volumes	ONTAP 9.17.1 und höher	ARP/AI wird sofort aktiv und leitet eine Evaluierungsphase ein, um einen geeigneten Alarmschwellenwert festzulegen, bevor von einem anfänglich konservativen Schwellenwert umgeschaltet wird.

Bevor Sie beginnen

- Eine Storage-VM (SVM) mit aktiviertem NFS- oder SMB-Protokoll (oder beiden).
- NAS-Workload mit konfigurierten Clients.
- Ein aktives "Verbindungspfad" für das Volume.
- Die "korrekte Lizenz" für Ihre ONTAP Version.
- (Empfohlen) Multi-Admin-Verifizierung (MAV) aktiviert (ONTAP 9.13.1 und höher). Siehe "Multi-Admin-Verifizierung aktivieren".

ARP auf NAS FlexVol Volumes aktivieren

ARP kann auf NAS FlexVol Volumes mithilfe von System Manager oder der ONTAP CLI aktiviert werden.

System Manager

1. **Storage > Volumes** auswählen und dann das Volume auswählen, das geschützt werden soll.
2. Im Tab **Sicherheit** der **Volumes**-Übersicht **Status** auswählen, um von Deaktiviert auf Aktiviert zu wechseln.
3. Im Feld **Anti-ransomware** ist **Enabled in learning-mode** auszuwählen.

> Sie können "Automatische Übergänge vom Lernmodus in den aktiven Modus auf der zugehörigen Storage-VM deaktivieren" verwenden, wenn der Übergang vom Lernmodus in den aktiven Modus manuell gesteuert werden soll.

> In bestehenden Volumes gelten Lern- und Aktivmodus nur für neu geschriebene Daten, nicht für bereits vorhandene Daten im Volume. Die vorhandenen Daten werden nicht gescannt und analysiert, da die Eigenschaften des vorherigen normalen Datenverkehrs anhand der neuen Daten nach der Aktivierung des Volumes für ARP angenommen werden.

4. Der ARP-Status des Volumes im **Anti-ransomware**-Feld kann überprüft werden.

   Zum Anzeigen des ARP-Status für alle Volumes im Bereich **Volumes** die Option **Anzeigen/Ausblenden** auswählen und sicherstellen, dass der **Anti-ransomware**-Status aktiviert ist.

CLI

ARP auf einem vorhandenen Volume aktivieren (im Lernmodus):

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

Weitere Informationen zu `security anti-ransomware volume dry-run` finden sich in der "ONTAP-Befehlsreferenz".

Ein neues Volume mit aktiviertem ARP (im Lernmodus) erstellen:

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

Automatische Umschaltung vom Lern- in den Aktivmodus deaktivieren (optional):

Wenn Sie ONTAP 9.13.1 bis 9.15.1 verwenden und den Wechsel vom Lernmodus in den Aktivmodus für alle mit einer SVM verbundenen Volumes manuell steuern möchten:

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

ARP-Status überprüfen:

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

ARP auf NAS FlexGroup Volumes aktivieren

ARP-Unterstützung für NAS FlexGroup Volumes ist ab ONTAP 9.13.1 verfügbar.

FlexGroup Volumes in ONTAP 9.13.1 bis 9.17.1 verwenden das ursprüngliche ARP-Modell mit Lernmodus, nicht ARP/AI. ARP/AI mit sofortigem Aktivmodus für FlexGroup Volumes erfordert ONTAP 9.18.1. Siehe "ARP/AI auf einem Volume aktivieren".

System Manager

1. **Speicher > Volumes** auswählen und dann das FlexGroup Volume auswählen, das geschützt werden soll.
2. Im Tab **Sicherheit** der **Volumes**-Übersicht **Status** auswählen, um von Deaktiviert auf Aktiviert zu wechseln.
3. Im Feld **Anti-ransomware** ist **Enabled in learning-mode** auszuwählen.

   Sie können "Automatische Übergänge vom Lernmodus in den aktiven Modus deaktivieren" verwenden, wenn der Übergang vom Lernmodus in den aktiven Modus manuell gesteuert werden soll.

4. Der ARP-Status des Volumes im **Anti-ransomware**-Feld kann überprüft werden.

CLI

ARP auf einem vorhandenen FlexGroup Volume aktivieren (im Lernmodus):

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

Ein neues FlexGroup Volume mit aktiviertem ARP (im Lernmodus) erstellen:

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state dry-run -junction-path </path_name>
```

ARP-Status überprüfen:

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

Verwandte Informationen

- "Vom Lernmodus in den aktiven Modus wechseln"

- "ARP standardmäßig in neuen Volumes aktivieren"

ONTAP ARP ist in neuen Volumes standardmäßig aktiviert

Ab ONTAP 9.10.1 können Storage-VMs (SVMs) so konfiguriert werden, dass neue NAS-Volumes standardmäßig mit Autonomous Ransomware Protection (ARP) im Lernmodus aktiviert sind. Diese Einstellung lässt sich über System Manager oder die ONTAP CLI ändern.

Wenn Sie ONTAP 9.16.1 oder höher verwenden, siehe "ARP/AI ist in neuen Volumes standardmäßig aktiviert".

Für ONTAP 9.13.1 bis 9.17.1 verwenden FlexGroup Volumes das frühere ARP-Modell und benötigen eine Lernphase. Dieses Verfahren gilt für FlexGroup Volumes mit ONTAP 9.17.1 und älteren Versionen.

Über diese Aufgabe

Standardmäßig werden neue Volumes mit deaktiviertem ARP erstellt. Wenn ARP standardmäßig auf einer SVM aktiviert ist, starten neue Volumes, die in dieser SVM erstellt werden, automatisch im ARP-Lernmodus (`dry-run` (Status). Bestehende Volumes ohne aktiviertes ARP ändern ihren ARP-Aktivierungsstatus nicht, wenn die SVM-Standardeinstellung geändert wird.

Ab ONTAP 9.13.1 ist adaptives Lernen standardmäßig aktiviert, was bedeutet, dass ARP automatisch vom Lernmodus in den aktiven Modus wechselt, nachdem festgestellt wurde, dass die Lernphase ausreichend ist. Es besteht die Möglichkeit, diesen automatischen Wechsel zu deaktivieren, um den Übergang manuell zu steuern.

Nach der Aktivierung des autonomen Ransomware-Schutzes kann es je nach Umgebung und ONTAP Version zu einer Übergangsphase kommen:

Volumentyp	ONTAP Version	Verhalten nach der Aktivierung
NAS FlexGroup	ONTAP 9.18.1 und höher	ARP/KI ist sofort ohne Lernphase aktiv
	ONTAP 9.13.1 bis 9.17.1	ARP startet im Lernmodus für 30 Tage
NAS FlexVol	ONTAP 9.16.1 und höher	ARP/KI ist sofort ohne Lernphase aktiv
	ONTAP 9.10.1 bis 9.15.1	ARP startet im Lernmodus für 30 Tage
SAN-Volumes	ONTAP 9.17.1 und höher	ARP/AI wird sofort aktiv und leitet eine Evaluierungsphase ein, um einen geeigneten Alarmschwellenwert festzulegen, bevor von einem anfänglich konservativen Schwellenwert umgeschaltet wird.

Bevor Sie beginnen

- Eine Storage-VM (SVM) mit aktiviertem NFS- oder SMB-Protokoll (oder beiden).
- Ein aktives "Verbindungspfad" für das Volume.
- Die "korrekte Lizenz" für Ihre ONTAP Version.
- (Empfohlen) Multi-Admin-Verifizierung (MAV) aktiviert (ONTAP 9.13.1 und höher). Siehe "Multi-Admin-Verifizierung aktivieren".

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um ARP standardmäßig für neue Volumes auf SVM-Ebene zu aktivieren.

System Manager

1. **Speicher-VMs** auswählen und dann die Speicher-VM auswählen, die die Volumes enthält, die mit ARP geschützt werden sollen.
2. Navigieren Sie zum Tab **Einstellungen**. Unter **Sicherheit** die Kachel **Anti-ransomware** suchen und dann auswählen.
3. Aktivieren Sie das Kontrollkästchen, um Anti-Ransomware (ARP) zu aktivieren. Aktivieren Sie das zusätzliche Kontrollkästchen, um ARP auf allen geeigneten Volumes in der Storage-VM zu aktivieren.
4. **Automatisch vom Lernmodus in den aktiven Modus wechseln nach ausreichendem Lernvorgang** ermöglicht es ARP, die optimale Lernperiode zu bestimmen und den Wechsel in den aktiven Modus zu automatisieren (ONTAP 9.13.1 und höher).

CLI

Eine vorhandene SVM so anpassen, dass ARP im Lernmodus für neue Volumes standardmäßig aktiviert ist:

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume
-state dry-run
```

Eine neue SVM mit standardmäßig aktiviertem ARP (im Lernmodus) für neue Volumes erstellen:

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume
-state dry-run
```

Automatischen Übergang vom Lern- in den aktiven Modus deaktivieren (optional):

Wenn Sie ONTAP 9.13.1 bis 9.15.1 verwenden und den Wechsel vom Lern- in den Aktivmodus für alle mit der SVM verbundenen Volumes manuell steuern möchten:

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

ARP-Status überprüfen:

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

Verwandte Informationen

- "Vom Lernmodus in den aktiven Modus wechseln"
- "security anti-ransomware volume show"

Nach einer Lernphase in den aktiven Modus von ONTAP ARP in ONTAP wechseln

In NAS-Umgebungen kann ein ARP-fähiges Volume manuell oder automatisch vom Lernmodus in den aktiven Modus gewechselt werden. Ein Moduswechsel ist erforderlich, wenn ARP mit ONTAP 9.10.1 bis 9.15.1 verwendet wird oder wenn ARP auf FlexGroup Volumes in ONTAP 9.13.1 bis 9.17.1 läuft.

ARP/AI (ONTAP 9.16.1 und höher) benötigt keine Lernphase. Der ARP/AI-Schutz wird auf FlexVol Volumes sofort aktiv. Für FlexGroup Volumes ist ARP/AI ab ONTAP 9.18.1 erforderlich. Es gibt kein entsprechendes Switch-Mode-Verfahren für ARP/AI. Bei Verwendung von ONTAP 9.16.1 oder höher siehe "Informationen zum autonomen Ransomware-Schutz".

Nachdem ARP einen empfohlenen Lernmoduslauf von mindestens 30 Tagen abgeschlossen hat, kann der Wechsel in den aktiven Modus manuell erfolgen. Ab ONTAP 9.13.1 ermittelt ARP automatisch das optimale Lernintervall und automatisiert den Wechsel, der möglicherweise bereits vor Ablauf der 30 Tage erfolgt.

In bestehenden Volumes gelten Lern- und Aktivmodus nur für neu geschriebene Daten, nicht für bereits vorhandene Daten im Volume. Die vorhandenen Daten werden nicht gescannt und analysiert, da die Eigenschaften des vorherigen normalen Datenverkehrs anhand der neuen Daten nach der Aktivierung des Volumes für ARP angenommen werden.

Nach einer Lernphase manuell in den aktiven Modus wechseln

Für ONTAP 9.10.1 bis 9.15.1 (und FlexGroup Volumes in ONTAP 9.13.1 bis 9.17.1) ist nach Abschluss der Lernphase ein manueller Wechsel vom ARP-Lernmodus in den aktiven Modus über den System Manager oder die ONTAP CLI möglich.

Beispiel 1. Schritte

System Manager

1. **Speicher > Volumes** auswählen und dann das Volume auswählen, das für den aktiven Modus bereit ist.
2. Auf der Registerkarte **Sicherheit** der **Volumes**-Übersicht im Feld Anti-Ransomware ist **In den aktiven Modus wechseln** auszuwählen.
3. Der ARP-Status des Volumes im **Anti-ransomware**-Feld kann überprüft werden.

CLI

1. Das geschützte Volume in den aktiven Modus wechseln:

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

Sie können auch mit dem `volume modify` Befehl in den aktiven Modus wechseln:

```
volume modify -volume <vol_name> -vserver <svm_name> -anti
```

```
-ransomware-state enabled
```

2. Der ARP-Status des Volumes kann überprüft werden:

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

Automatische Umschaltung vom Lernmodus in den aktiven Modus

Ab ONTAP 9.13.1 wurde adaptives Lernen in die ARP-Analyse integriert, und 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
```

Wenn die automatische Umschaltung aktiviert ist, wechselt das Volume nach maximal 30 Tagen automatisch in den aktiven Modus, selbst wenn nicht alle Bedingungen erfüllt sind. Diese 30-Tage-Grenze ist fest und kann nicht geändert werden.

Sie können die automatische Umschaltung vom Lern- in den Aktivmodus für alle Volumes in einer SVM deaktivieren, wenn der Übergang lieber manuell gesteuert werden soll:

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

Weitere Informationen zu den ARP-Konfigurationsoptionen, einschließlich Standardwerten, sind unter "ONTAP-Befehlsreferenz" zu finden.

Verwandte Informationen

- "Security Anti-Ransomware Volume"

ONTAP ARP-Angriffserkennungsparameter verwalten

Ab ONTAP 9.11.1 können die Parameter für die Ransomware-Erkennung auf einem bestimmten ARP-fähigen NAS-Volume angepasst und ein bekannter Anstieg als normale Dateiaktivität gemeldet werden. Die Anpassung der Erkennungsparameter trägt dazu bei, die Genauigkeit der Berichterstattung basierend auf der spezifischen Volume-Auslastung zu verbessern.

Wenn Sie ONTAP 9.16.1 oder höher verwenden, siehe "ARP/AI-Angriffserkennungsparameter verwalten".

Wie die Erkennung von ARP-Angriffen funktioniert

Im Lernmodus entwickelt der autonome Ransomware-Schutz (ARP) Basiswerte für das Volume-Verhalten. Dazu gehören Entropie, Dateierweiterungen und ab ONTAP 9.11.1 IOPS. Diese Basiswerte werden zur Bewertung von Ransomware-Bedrohungen verwendet. Weitere Informationen zu diesen Kriterien sind unter "was ARP erkennt" zu finden.

In ONTAP 9.10.1 gibt ARP eine Warnung aus, wenn **beide** der folgenden Bedingungen erfüllt sind:

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

In ONTAP 9.10.1 wird eine Warnung vor geringer Bedrohung zu einer Warnung vor mittlerer Bedrohung hochgestuft, wenn 100 oder mehr Dateien betroffen sind.

Ab ONTAP 9.11.1 gibt ARP eine Bedrohungswarnung aus, wenn **eine** der beiden Bedingungen erfüllt ist. Wenn beispielsweise innerhalb eines Zeitraums von 24 Stunden mehr als 20 Dateien mit zuvor im Volume nicht beobachteten Dateierweiterungen erkannt werden, kategorisiert ARP dies als Bedrohung, unabhängig von der beobachteten Entropie. Die Werte von 24 Stunden und 20 Dateien sind Standardwerte, die geändert werden können.

> Zur Reduzierung einer hohen Anzahl falsch positiver Warnmeldungen zu **Storage > Volumes > Security > Configure workload characteristics** wechseln und **Monitor new file types** deaktivieren. Diese Einstellung ist in ONTAP 9.14.1 P7 und 9.15.1 P1 standardmäßig deaktiviert.

ARP wertet SAN-Volumes in ONTAP 9.10.1 bis 9.15.1 nicht aus. Ab ONTAP 9.17.1 werden SAN-Volumes ausschließlich von ARP/AI unterstützt.

Ab ONTAP 9.14.1 ist es möglich, Benachrichtigungen zu konfigurieren, wenn ARP eine neue Dateierweiterung erkennt oder wenn ARP einen Snapshot erstellt. Weitere Informationen finden sich unter ARP-Warnmeldungen konfigurieren.

Parameter zur Erkennung von ARP-Angriffen anpassen

Je nach dem zu erwartenden Verhalten des ARP-fähigen NAS-Volumes kann es sinnvoll sein, die Parameter für die Angriffserkennung zu ändern.

Schritte

1. Vorhandene Parameter zur Angriffserkennung werden angezeigt:

```
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. Alle angezeigten Felder sind mit booleschen oder ganzzahligen Werten änderbar. Zum Ändern eines Feldes wird der `security anti-ransomware volume attack-detection-parameters modify` Befehl verwendet.

   Weitere Informationen zu `security anti-ransomware volume attack-detection-parameters modify` finden sich in der "ONTAP-Befehlsreferenz".

Bekannte Anstiege melden

ARP passt die Basiswerte für die Erkennungsparameter auch im aktiven Zustand kontinuierlich an. Wenn Anstiege in Ihrer Volumenaktivität bekannt sind, entweder einmalige Anstiege oder ein Anstieg, der für eine neue Normalität charakteristisch ist, sollten diese als unbedenklich gemeldet werden. Das manuelle Melden dieser Anstiege als unbedenklich trägt zur Verbesserung der Genauigkeit der Bedrohungsbewertungen von ARP bei.

Ein einmaliger Anstieg kann gemeldet werden

1. Wenn unter bekannten Umständen eine einmalige Lastspitze auftritt und Sie möchten, dass ARP eine ähnliche Lastspitze auch in Zukunft meldet, entfernen Sie die Lastspitze aus dem Workload-Verhalten:

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

   Weitere Informationen zu `security anti-ransomware volume workload-behavior clear-surge` finden sich in der "ONTAP-Befehlsreferenz".

Basislinienanstieg ändern

1. Wenn ein gemeldeter Anstieg als normales Anwendungsverhalten betrachtet werden sollte, ist der Anstieg entsprechend zu melden, um den Basiswert für den Anstieg zu ändern:

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

   Weitere Informationen zu `security anti-ransomware volume workload-behavior update-baseline-from-surge` finden sich in der "ONTAP-Befehlsreferenz".

ARP-Warnmeldungen konfigurieren

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

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

Warnungen für diese beiden Ereignisse können für einzelne Volumes oder für die gesamte SVM eingerichtet werden. Wenn Warnungen für die SVM aktiviert werden, werden die Warnungseinstellungen nur von Volumes übernommen, die nach der Aktivierung der Warnung erstellt werden. Standardmäßig sind Warnungen für kein Volume aktiviert.

Ereignisbenachrichtigungen können mit Multi-Admin-Verifizierung gesteuert werden. Weitere Informationen finden Sie unter "Multi-Admin-Verifizierung mit ARP-geschützten Volumes".

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um Warnmeldungen für ARP-Ereignisse festzulegen.

System Manager

Alarme für ein Volume festlegen

1. Navigieren Sie zu **Volumes**. Wählen Sie das einzelne Volume aus, für das Sie die Einstellungen ändern möchten.
2. Die Registerkarte **Sicherheit** und dann **Ereignis-Schweregrad-Einstellungen** auswählen.
3. Um Benachrichtigungen für **Neue Dateierweiterung erkannt** und **Ransomware-Snapshot erstellt** zu erhalten, das Dropdown-Menü unter der Überschrift **Schweregrad** auswählen. Die Einstellung von **Kein Ereignis generieren** auf **Benachrichtigung** ändern.
4. **Speichern** auswählen.

Alarme für eine SVM festlegen

1. Zu **Storage VM** navigieren und dann die SVM auswählen, für die Einstellungen aktiviert werden sollen.
2. Unter der Überschrift **Sicherheit** die Karte **Anti-ransomware** suchen. ⋮ dann **Schweregrad von Ransomware-Ereignissen bearbeiten** auswählen.
3. Um Benachrichtigungen für **Neue Dateierweiterung erkannt** und **Ransomware-Snapshot erstellt** zu erhalten, das Dropdown-Menü unter der Überschrift **Schweregrad** auswählen. Die Einstellung von **Kein Ereignis generieren** auf **Benachrichtigung** ändern.
4. **Speichern** auswählen.

CLI

Alarme für ein Volume festlegen

- Benachrichtigungen für eine neue Dateierweiterung einrichten:

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

- Zum Einrichten von Benachrichtigungen für die Erstellung eines ARP Snapshot:

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

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

Alarme für eine SVM festlegen

- Benachrichtigungen für eine neue Dateierweiterung einrichten:

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

- Zum Einrichten von Benachrichtigungen für die Erstellung eines ARP Snapshot:

```
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 zu `security anti-ransomware vserver event-log`Befehlen finden Sie in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Informationen zu ARP-Angriffen und dem ARP-Snapshot"
- "ONTAP-Befehlsreferenz"

Auf von ONTAP ARP erkannte abnormale Aktivitäten reagieren

Wenn der autonome Ransomware Protection (ARP) ungewöhnliche Aktivitäten in einem geschützten NAS-Volume erkennt, wird eine Warnung ausgegeben. Die Benachrichtigung sollte geprüft werden, um festzustellen, ob die Aktivität akzeptabel ist (Fehlalarm) oder ob ein Angriff als bösartig erscheint. Nach der Kategorisierung des Angriffs kann die Warnung entfernt und die normale Überwachung fortgesetzt werden.

Wenn Sie ONTAP 9.16.1 oder höher verwenden, siehe "Auf von ARP/AI erkannte anomale Aktivitäten reagieren".

Wenn ein Angriff kategorisiert wird, werden ARP-Snapshots in ONTAP 9.15.1 und früher sofort gelöscht, wenn das verdächtige Ereignis gelöscht wird. Wenn `volume snapshot restore` zur Wiederherstellung von Daten verwendet wird, muss die Wiederherstellung **vor** dem Löschen des verdächtigen Ereignisses erfolgen.

Ab ONTAP 9.11.1 ist es möglich, die "Aufbewahrungseinstellungen" für ARP-Snapshots zu

ändern.

Über diese Aufgabe

Bei NAS-Volumes zeigt ARP eine Liste verdächtiger Dateien an, wenn eine Kombination aus hoher Datenentropie, ungewöhnlicher Volume-Aktivität mit Datenverschlüsselung und ungewöhnlichen Dateierweiterungen erkannt wird. ARP (9.10.1 bis 9.15.1) unterstützt keine SAN-Volumes.

Obwohl der autonome Ransomware-Schutz die Erkennung und Erstellung von Snapshots automatisiert, erfordert die endgültige Feststellung, ob eine Datei oder ein Ereignis tatsächlich schädlich ist, eine manuelle Untersuchung. Der autonome Ransomware-Schutz kann nicht mit Sicherheit feststellen, ob es sich bei einem Ereignis um einen echten Ransomware-Angriff handelt. Verdächtige Aktivitäten werden gekennzeichnet, jedoch ist eine Untersuchung und Bestätigung erforderlich, ob es sich tatsächlich um Ransomware oder einen Fehlalarm (harmlose Aktivität) handelt.

"Es wird festgestellt, ob eine Datei oder ein Ereignis tatsächlich schädlich ist.".

Wenn eine ARP-Warnmeldung ausgegeben wird, kann die Aktivität auf eine von zwei Arten gekennzeichnet werden:

- **Falsch positiv**: Der identifizierte Dateityp wird in Ihrer Arbeitslast erwartet und kann ignoriert werden.
- **Potenzieller Ransomware-Angriff**: Der identifizierte Dateityp ist in Ihrer Arbeitslast unerwartet und sollte als potenzieller Angriff behandelt werden.

Die normale Überwachung wird wieder aufgenommen, nachdem Sie Ihre Entscheidung aktualisiert und die ARP-Benachrichtigungen gelöscht haben. ARP speichert Ihre Bewertung im Bedrohungsanalyseprofil und verwendet Ihre Auswahl zur Überwachung nachfolgender Dateiaktivitäten.

Im Falle eines vermuteten Angriffs ist festzustellen, ob es sich tatsächlich um einen Angriff handelt, gegebenenfalls darauf zu reagieren und anschließend Benachrichtigungen zu löschen sowie Daten wiederherzustellen. "Weitere Informationen zur Wiederherstellung nach einem Ransomware-Angriff".

Bevor Sie beginnen

ARP muss ein Volume aktiv schützen (nicht im Lernmodus oder pausiert).

Schritte

Gehen Sie wie folgt vor, wenn Sie abnormale Aktivitäten klassifizieren müssen:

1. Details zu abnormalen Aktivitäten prüfen
2. Snapshot-Verhalten beim Löschen eines vermuteten Ereignisses
3. Führen Sie einen der folgenden Schritte aus:
    - Als falsch positiv einstufen und Überwachung fortsetzen
    - Als potenziellen Ransomware-Angriff einstufen, Daten wiederherstellen und abschließen

Falls eine Wiederherstellung von Daten erforderlich ist, sind die Schritte in "Daten nach einem Ransomware-Angriff mit ARP wiederherstellen" zu beachten.

Details zu abnormalen Aktivitäten prüfen

Sie können den System Manager oder die ONTAP CLI verwenden, um die ARP-Warnungsdetails zu überprüfen, bevor Sie einen Antwortablauf auswählen.

System Manager

1. Wenn Sie eine Benachrichtigung über „ungewöhnliche Aktivitäten“ erhalten, folgen Sie dem Link. Alternativ navigieren Sie zu **Speicher > Volumes**, suchen ein betroffenes Volume und wählen die Registerkarte **Sicherheit** aus.

   Warnungen werden im System Manager-Dashboard im Bereich **Übersicht** des Menüs **Ereignisse** angezeigt.

2. Im Tab **Sicherheit** wird der Bericht **Verdächtige Dateitypen** angezeigt. Ein Dialogfeld **Verdächtige Dateitypen** zeigt die von ARP identifizierten Dateierweiterungen und Dateianzahlen an.

CLI

1. Wenn eine Benachrichtigung über einen vermuteten Ransomware-Angriff eingeht, sollten Zeitpunkt und Schweregrad des Angriffs überprüft werden:

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

   Beispielausgabe:

   ```
   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
   ```

Snapshot-Verhalten beim Löschen eines vermuteten Ereignisses

Bei ONTAP 9.15.1 und älteren Versionen werden ARP-Snapshots **sofort gelöscht**, wenn das verdächtige Ereignis gelöscht wird. Das bedeutet, dass **die Daten vor dem Löschen wiederhergestellt werden müssen**, wenn eine Nutzung von `volume snapshot restore` geplant ist. Nach dem Löschen ist der Snapshot nicht mehr vorhanden und kann nicht mehr für eine Wiederherstellung verwendet werden.

Wenn andere Wiederherstellungsmethoden (FlexClone, Einzeldatei SnapRestore, Datenkopie) verwendet werden, kann die Wiederherstellung entweder vor oder nach dem Löschen des vermuteten Ereignisses erfolgen; diese Methoden löschen den Snapshot nicht.

Ab ONTAP 9.13.1, wenn Sie MAV zum Schutz von ARP-Einstellungen verwenden, kann der `clear-suspect` -Vorgang zusätzliche Genehmigungen erfordern. "Die Zustimmung aller Administratoren muss eingeholt werden." der MAV-Genehmigungsgruppe oder der Vorgang schlägt fehl.

Als falsch positiv einstufen und Überwachung fortsetzen

Dieser Ablauf kommt zum Einsatz, wenn der identifizierte Dateityp für die Arbeitslast *erwartet* ist.

System Manager

1. Wählen Sie die betroffenen Dateien aus, **Als falsch positiv markieren** auswählen und dann **Verdächtige Dateitypen aktualisieren und löschen** wählen.

Diese Aktion beseitigt die Warnmeldung. Anschließend setzt ARP die normale Überwachung des Volumens fort.

CLI

1. Führen Sie den folgenden Befehl aus, um Ihre Entscheidung zu speichern und die normale ARP-Überwachung fortzusetzen:

   ```
   security anti-ransomware volume attack clear-suspect -vserver
   <svm_name> -volume <vol_name> [<extension_identifiers>] -false
   -positive true
   ```

   Verwenden Sie den folgenden optionalen Parameter, um nur bestimmte Erweiterungen als falsch positive Ergebnisse zu kennzeichnen: `[-extension <text>, … ]`

Als potenziellen Ransomware-Angriff einstufen und Daten wiederherstellen

Dieser Ablauf kommt zum Einsatz, wenn der ermittelte Dateityp für die Arbeitslast *unerwartet* ist.

System Manager

1. Ausgewählte Dateien als **Potenzieller Ransomware-Angriff** markieren.
2. Bevor Sie Daten wiederherstellen, sollten Sie Ihre "Optionen für Wiederherstellungsmethoden" Sicherheitsvorkehrungen beachten. Anschließend ist eine der folgenden Optionen möglich:
   - **Wenn Sie planen, ein Volume wiederherzustellen**: Die Datenwiederherstellung sollte **vor** dem Löschen der Benachrichtigungen abgeschlossen werden:
     i. "Daten aus dem aktuellsten ARP-Snapshot oder einem früheren Snapshot wiederherstellen".
     ii. Nach Abschluss der Datenwiederherstellung erfolgt der Abschluss durch das Löschen des vermuteten Ereignisses:
     - Bei NAS-Dateitypwarnungen wählen Sie **Aktualisieren und Verdächtige Dateitypen löschen**.

       Durch das Speichern Ihrer Entscheidung werden der Angriffsbericht gelöscht und der ARP-Snapshot entfernt. Die Datenwiederherstellung sollte vor diesem Schritt abgeschlossen sein.

   - **Falls eine andere Wiederherstellungsmethode (FlexClone oder Einzeldatei SnapRestore) verwendet werden soll: Zuerst die Daten wiederherstellen, dann die Hinweise löschen:**
     i. "Stellen Sie Daten mithilfe von FlexClone oder Einzeldatei-SnapRestore wieder her".

ii. Nach Abschluss der Datenwiederherstellung die Kategorisierung abschließend vornehmen:

- Wählen Sie **Aktualisieren und Verdächtige Dateitypen löschen**.

CLI

1. (Optional) Einen Angriffsbericht generieren und angeben, wo dieser gespeichert werden soll:

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

2. Für ONTAP 9.15.1 und frühere Versionen mit `volume snapshot restore`: Daten **vor** dem Löschen des vermuteten Ereignisses wiederherstellen. Siehe "Daten nach einem Angriff mit ARP wiederherstellen".
3. Nachdem die Daten wiederhergestellt wurden (oder falls eine alternative Wiederherstellungsmethode verwendet wird), sollte das verdächtige Ereignis gelöscht und der Angriff als potenzielle Ransomware (`-false-positive false` markiert werden:

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> [<extension_identifiers>] -false
-positive false
```

In ONTAP 9.15.1 und früher führt das Ausführen von `clear-suspect`**sofortigen Löschens** von ARP-Snapshots. Dieser Befehl sollte erst nach Abschluss der Datenwiederherstellung ausgeführt werden.

Daten nach einem Ransomware-Angriff mit ONTAP ARP wiederherstellen

Autonomous Ransomware Protection (ARP) erstellt Snapshots, um NAS-Volumes vor Ransomware-Bedrohungen zu schützen. Mit ARP-Snapshots oder einem anderen Snapshot Ihres Volumes lässt sich die Wiederherstellung von Daten durchführen.

Wenn Sie ONTAP 9.16.1 oder höher verwenden, siehe "Daten nach einem Ransomware-Angriff mit ARP/AI wiederherstellen".

Über diese Aufgabe

Je nach potenzieller Angriffssituation stellen Sie die Daten auf eine der folgenden Arten wieder her:

- **Wiederherstellung vom aktuellsten ARP-Snapshot**: Der aktuellste verfügbare ARP-Snapshot kann verwendet werden, wenn dessen Integrität sichergestellt ist.
- **Wiederherstellung aus einem früheren Snapshot**: Die Sperre des zuletzt gespeicherten ARP-Snapshots aufheben und anschließend einen früheren Snapshot wiederherstellen.
- **Wiederherstellung, wenn kein Angriff gemeldet wird**: Zuerst wird die Wiederherstellung aus dem aktuellsten ARP-Snapshot durchgeführt, anschließend erfolgt eine weitere Wiederherstellung aus dem von

Ihnen gewählten Snapshot.

ARP erstellt Snapshots mit dem vorangestellten Namen `Anti_ransomware_backup`. Zum Beispiel `Anti_ransomware_backup.2022-12-20_1248`.

Bevor Sie beginnen

- Wenn Sie auf eine Warnung wegen ungewöhnlicher Aktivitäten reagieren, "Es ist als potenzieller Ransomware-Angriff zu kategorisieren." bevor Sie mit der Datenwiederherstellung fortfahren.
- Wählen Sie eine Wiederherstellungsmethode und überprüfen Sie Wiederherstellungsbeschränkungen bevor der Wiederherstellungsvorgang abgeschlossen wird.

Wählen Sie eine Wiederherstellungsmethode

Je nach Ausmaß der Datenbeschädigung und Ihren betrieblichen Anforderungen wählen Sie eine oder mehrere dieser Wiederherstellungsmethoden.

- **Wiederherstellung eines Volume-Snapshots**: Setzt das gesamte Volume auf einen ausgewählten Snapshot (ARP oder geplant) zurück. Dies ist die schnellste Methode, entfernt jedoch alle Snapshots, die nach dem Wiederherstellungspunkt erstellt wurden.

> Für ONTAP 9.15.1 und frühere Versionen: ARP Snapshots werden **sofort gelöscht**, wenn `clear-suspect` ausgeführt wird. Die Wiederherstellung des Volume Snapshots muss **vor** dem Löschen abgeschlossen sein. Weitere Informationen unter "Snapshot-Verhalten beim Löschen eines vermuteten Ereignisses".

- **FlexClone von einem sauberen Snapshot**: Erstellt ein Klon-Volume aus dem ausgewählten Snapshot, wobei das Original-Volume und alle seine Snapshots für forensische Analysen oder zusätzliche Wiederherstellung erhalten bleiben. Es wird empfohlen, den Klon vom übergeordneten Volume zu trennen, um das infizierte übergeordnete Volume vom sauberen Klon zu isolieren.

  Weitere Informationen zu "Erstellen eines FlexClone Volume aus einem Snapshot" und "Abspaltung eines FlexClone von seinem Elternteil".

- **Einzeldatei SnapRestore**: Stellt einzelne Dateien aus Snapshots wieder her. Jede Datei kann aus einem anderen Snapshot stammen. Dies ist sinnvoll, wenn die Anzahl der betroffenen Dateien relativ gering ist.

  Weitere Informationen zu "Wiederherstellen einer einzelnen Datei aus einem Snapshot".

- **Datenkopie aus dem `.snapshot` Verzeichnis**: Kopiert Daten vom Snapshot-Mountpunkt mithilfe standardmäßiger Dateikopiervorgänge auf ein neues Volume. Bei dieser Methode bleiben das Original-Volume und die Snapshots für die Analyse erhalten.
- **Hybridansatz**: Das Volume wird zuerst mithilfe von SnapRestore auf den nächstgelegenen sauberen Snapshot zurückgesetzt, dann werden alle verbleibenden beschädigten Dateien einzeln aus einem anderen Snapshot oder externem Backup wiederhergestellt.

Einschränkungen und Überlegungen zur Wiederherstellung

- In ONTAP 9.15.1 und früher werden ARP-Snapshots **sofort** gelöscht, wenn Sie `clear-suspect` ausführen. Dies gilt unabhängig davon, ob die Aktivität als Fehlalarm oder als tatsächlicher Angriff markiert wird. Wenn `volume snapshot restore` verwendet werden soll, muss die Wiederherstellung **vor** dem Löschen verdächtiger Ereignisse abgeschlossen werden.
- Das Freigeben der ARP-Snapshot-Sperre ist nur erforderlich, wenn `volume snapshot restore` zur

Wiederherstellung aus einem früheren Snapshot verwendet wird. Dies ist nicht erforderlich für FlexClone, Einzeldatei SnapRestore, Datenkopiervorgänge oder ähnliche Methoden.

- Wenn Sie ein ARP-geschütztes Volume aus einem Snapshot wiederherstellen, während es an einer SnapMirror asynchronen Beziehung teilnimmt, sollten nach der Wiederherstellung alle Spiegelkopien manuell aktualisiert werden. Andernfalls können Spiegelkopien unbrauchbar werden und müssen möglicherweise gelöscht und neu erstellt werden.
- ARP (9.10.1 bis 9.15.1) unterstützt weder SnapMirror synchron noch SnapMirror active sync. Dies sind ausschließlich ARP/AI-Funktionen (ONTAP 9.19.1 und später).

Wiederherstellung nach einem Systemangriff

Für die Wiederherstellung von Volume-Snapshots wählen Sie je nach Snapshot-Quelle und Situation einen dieser Abläufe:

- Wiederherstellung vom aktuellsten ARP-Snapshot
- Wiederherstellung aus einem früheren Snapshot
- Wiederherstellung, wenn kein Angriff erkannt wird

Wiederherstellung vom aktuellsten ARP-Snapshot

Wählen Sie diesen Ablauf, wenn Sie die Wiederherstellung sicher vom aktuellsten ARP-Snapshot durchführen können, da dies der aktuellste für die Wiederherstellung verfügbare Snapshot ist.

System Manager

1. Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies**.
2. Wählen Sie ⋮ neben dem zuletzt gespeicherten ARP-Snapshot (`Anti_ransomware_backup` aus, den Sie wiederherstellen möchten, und wählen Sie dann **Wiederherstellen**.
3. Nach Abschluss der Wiederherstellung "Zurück zum Antwortablauf" können verdächtige Dateien gelöscht werden.

CLI

1. Snapshots in einem Volume auflisten:

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

2. Den Inhalt eines Volumes aus einem Snapshot wiederherstellen:

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

3. Nach Abschluss der Wiederherstellung "Zurück zum Antwortablauf" können verdächtige Dateien gelöscht werden.

Wiederherstellung aus einem früheren Snapshot

Wählen Sie diesen Ablauf, wenn Sie einen früheren Snapshot wiederherstellen möchten. Die Sperre des aktuellsten ARP-Snapshots ist aufzuheben, bevor eine Wiederherstellung aus dem früheren Snapshot erfolgt.

> In ONTAP 9.15.1 und früheren Versionen führt das Löschen des vermuteten Ereignisses dazu, dass **ARP-Snapshots sofort gelöscht werden**. In diesem Ablauf erfolgt die Wiederherstellung absichtlich aus einem früheren Snapshot (nicht dem ARP-Snapshot), daher ist das vorherige Löschen erforderlich, um die Sperre aufzuheben. Wenn Daten aus dem ARP-Snapshot benötigt werden, sollte stattdessen der Wiederherstellung vom aktuellsten ARP-Snapshot Ablauf verwendet werden.

System Manager

1. Die Sperre für den aktuellsten ARP-Snapshot aufheben:
   a. **Speicher > Volumes** auswählen.
   b. **Sicherheit** und dann **Verdächtige Dateitypen anzeigen** auswählen.
   c. Die Dateien werden als „Potenzieller Ransomware-Angriff“ markiert.
   d. Wählen Sie **Aktualisieren und Verdächtige Dateitypen löschen**.
2. Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies**.
3. Wählen Sie ⋮ neben dem früheren Snapshot, den Sie wiederherstellen möchten, und wählen Sie dann **Wiederherstellen**.

CLI

1. Den Angriff als potenzielle Ransomware (`-false-positive false` markieren und verdächtige Dateien löschen, um die Sperre aufzuheben:

   > Dadurch werden ARP Snapshots in ONTAP 9.15.1 und früher sofort gelöscht. Dieser Befehl sollte nur ausgeführt werden, wenn eine Wiederherstellung von einem früheren (nicht-ARP) Snapshot beabsichtigt ist und der ARP Snapshot nicht benötigt wird.

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

2. Snapshots in einem Volume auflisten:

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

   Das folgende Beispiel zeigt die Momentaufnahme 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. Den Inhalt eines Volumes aus einem Snapshot wiederherstellen:

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

Das folgende Beispiel stellt den Inhalt von `vol1` wieder her:

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

Wiederherstellung, wenn kein Angriff erkannt wird

Wenn kein Angriff festgestellt wird, wird zuerst der aktuellste ARP-Snapshot und anschließend ein früherer Snapshot wiederhergestellt.

System Manager

1. Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies**.
2. Wählen Sie ⋮ und wählen Sie dann den aktuellsten `Anti_ransomware_backup` Snapshot aus.
3. **Wiederherstellen** auswählen.
4. Kehren Sie zum Menü **Snapshot Copies** zurück und wählen Sie dann den früheren Snapshot aus, den Sie verwenden möchten.
5. **Wiederherstellen** auswählen.

CLI

1. Zuerst vom aktuellsten ARP-Snapshot wiederherstellen:
   a. Snapshots in einem Volume auflisten:

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

   b. Den Inhalt eines Volumes aus einem Snapshot wiederherstellen:

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

2. Wählen Sie den früheren Snapshot aus, den Sie verwenden möchten, und wiederholen Sie die Wiederherstellung.

Weitere Informationen zu `volume snapshot` finden sich in der "ONTAP-Befehlsreferenz".

Einstellungen für automatisch generierte ONTAP ARP Snapshots anpassen

Ab ONTAP 9.11.1 kann über die CLI die Aufbewahrungseinstellungen für Autonomous Ransomware Protection (ARP) Snapshots gesteuert werden, die automatisch als Reaktion auf vermutete Ransomware-Angriffe generiert werden.

Wenn Sie ONTAP 9.16.1 oder höher verwenden, siehe "Einstellungen für automatisch generierte ARP/AI Snapshots anpassen".

Bevor Sie beginnen

Die ARP-Snapshot-Optionen können nur auf einer "Node SVM" und nicht auf anderen SVM-Typen geändert werden.

Die in diesem Abschnitt aufgeführten Einstellungen gelten für ONTAP 9.11.1 bis 9.15.1. Wenn Sie auf ONTAP 9.16.1 oder höher aktualisiert haben, verwenden Sie die "ARP/AI Snapshot-Einstellungen".

Schritte

1. Alle aktuellen ARP Snapshot-Einstellungen:

```
options -option-name arw*
```

2. Ausgewählte aktuelle ARP-Snapshot-Einstellungen:

```
options -option-name <arw_setting_name>
```

3. ARP Snapshot-Einstellungen anpassen:

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

Sie können die folgenden Einstellungen ändern (ONTAP 9.11.1 bis 9.15.1):

Einstellung	Beschreibung	Unterstützte Versionen mit ARP
`arw.snap.max.count`	Legt die maximale Anzahl von ARP-Snapshots fest, die zu einem bestimmten Zeitpunkt auf einem Volume vorhanden sein können. Ältere Kopien werden gelöscht, um sicherzustellen, dass die Gesamtzahl der ARP-Snapshots innerhalb dieses Grenzwerts bleibt.	ONTAP 9.11.1 bis 9.15.1
`arw.snap.create.interval.hours`	Gibt das Intervall *in Stunden* zwischen ARP-Snapshots an. Ein neuer ARP-Snapshot wird erstellt, wenn ein Angriff auf Basis der Datenentropie vermutet wird und der zuletzt erstellte Snapshot älter als das angegebene Intervall ist.	ONTAP 9.11.1 bis 9.15.1
`arw.snap.normal.retain.interval.hours`	Gibt die Dauer *in Stunden* an, für die ein ARP-Snapshot aufbewahrt wird. Wenn ein ARP-Snapshot den Aufbewahrungsschwellenwert erreicht, wird er gelöscht.	ONTAP 9.11.1 bis 9.15.1 (veraltet in 9.17.1 und später)
`arw.snap.max.retain.interval.days`	Gibt die maximale Dauer *in Tagen* an, für die ein ARP Snapshot aufbewahrt werden kann. Jeder ARP Snapshot, der älter als diese Dauer ist, wird gelöscht, wenn kein Angriff auf dem Volume gemeldet wird. Das maximale Aufbewahrungsintervall wird ignoriert, wenn eine Bedrohung mittlerer Stärke erkannt wird. Der als Reaktion auf die Bedrohung erstellte ARP-Snapshot wird aufbewahrt, bis Sie auf die Bedrohung reagieren. Wenn Sie eine Bedrohung als Fehlalarm markieren, löscht ONTAP die ARP-Snapshots für das Volume.	ONTAP 9.11.1 bis 9.15.1 (veraltet in 9.17.1 und später)
`arw.snap.create.interval.hours.post.max.count`	Legt das Intervall *in Stunden* zwischen ARP-Snapshots fest, wenn das Volume bereits die maximale Anzahl an ARP-Snapshots enthält. Wenn die maximale Anzahl erreicht ist, wird ein ARP-Snapshot gelöscht, um Platz für eine neue Kopie zu schaffen. Mit dieser Option lässt sich die Erstellungsgeschwindigkeit reduzieren, sodass ältere Kopien erhalten bleiben.	ONTAP 9.11.1 bis 9.15.1 (veraltet in 9.17.1 und später)
`arw.snap.new.extns.interval.hours`	Gibt das Intervall *in Stunden* zwischen ARP-Snapshots an, die bei Erkennung einer neuen Dateierweiterung erstellt werden. Ein neuer ARP-Snapshot wird erstellt, wenn eine neue Dateierweiterung erkannt wird und der vorherige entsprechende Snapshot älter als das angegebene Intervall ist. Diese Option besteht unabhängig von `arw.snap.create.interval.hours`, die das Intervall für entropiebasierte Snapshots festlegt.	ONTAP 9.11.1 bis 9.15.1 (veraltet in 9.17.1 und später)
`arw.snap.surge.interval.days`	Legt das Intervall *in Tagen* zwischen ARP-Snapshots fest, die als Reaktion auf IO-Spitzen erstellt werden. Diese Option legt außerdem die Aufbewahrungsdauer *in Tagen* für einen ARP-Surge-Snapshot fest.	ONTAP 9.11.1 bis 9.15.1

Verwandte Informationen

- "Bedrohungsanalyse und ARP-Snapshots"

- "Einstellungen für ARP/AI Snapshots anpassen (ONTAP 9.16.1 und höher)"

Copyright-Informationen

Copyright © 2026 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 IRGENDEINER 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.