ARP/AI 9.16.1 und höher

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/anti-ransomware/learn-about-arpai.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

ARP/AI 9.16.1 und höher . . . 1
Informationen zu ONTAP ARP/AI (ONTAP 9.16.1 und höher) . . . 1
Funktionsweise von ARP/KI . . . 1
Was ARP/AI erkennt . . . 1
Aktivierungsoptionen für ARP/AI . . . 2
ARP/AI-Schutzmodi . . . 2
Gefährdungsanalyse . . . 4
ARP/AI Snapshots . . . 4
Auf einen Angriff reagieren und ihn bewerten . . . 6
Daten nach einem Angriff wiederherstellen . . . 6
Multi-Admin-Verifizierung . . . 6
Unterstützte Konfigurationen für ONTAP ARP/AI . . . 6
Geeignete Workloads . . . 6
Ungeeignete Workloads . . . 7
Unterstützte Konfigurationen . . . 7
SnapMirror und ARP/AI Interoperabilität . . . 8
ARP/AI und virtuelle Maschinen . . . 9
Nicht unterstützte Konfigurationen . . . 10
ARP/AI-Leistung und Frequenzüberlegungen . . . 10
Upgrade-Überlegungen für bestehende Cluster . . . 11
Multi-Admin-Verifizierung mit ARP/AI-geschützten Volumes . . . 11
ARP/AI aktivieren . . . 11
ONTAP ARP/AI auf einem Volume aktivieren . . . 11
ONTAP ARP/AI ist in neuen Volumes standardmäßig aktiviert . . . 15
Automatische Aktivierung von ONTAP ARP/AI während Upgrades verwalten . . . 17
Informationen zur Entropieauswertung von ONTAP ARP/AI für Blockgeräte-Workloads . . . 18
Unterstützte Workloads und Anwendbarkeit der Evaluierung . . . 19
Entropiebewertung . . . 19
Geeignete Arbeitslasten und adaptive Schwellenwerte . . . 20
ONTAP ARP/AI-Angriffserkennungsparameter verwalten . . . 21
Funktionsweise der Erkennung von ARP/AI-Angriffen . . . 21
Ändern der ARP/AI Angriffserkennungsparameter . . . 22
Bekannte Anstiege melden . . . 23
ARP/AI-Warnungen konfigurieren . . . 23
Auf von ONTAP ARP/AI erkannte abnormale Aktivitäten reagieren . . . 25
Details zu abnormalen Aktivitäten prüfen . . . 26
Snapshot-Verhalten beim Löschen eines vermuteten Ereignisses . . . 28
Als falsch positiv einstufen und Überwachung fortsetzen . . . 28
Als potenziellen Ransomware-Angriff einstufen und Daten wiederherstellen . . . 29
Daten nach einem Ransomware-Angriff mit ONTAP ARP/AI wiederherstellen . . . 31
Wählen Sie eine Wiederherstellungsmethode . . . 31
Einschränkungen und Überlegungen zur Wiederherstellung . . . 32
Wiederherstellung nach einem Systemangriff . . . 33

Wiederherstellung, wenn kein Angriff erkannt wird . . . 35
Konfiguration von ONTAP ARP/AI Snapshot-Antwortrichtlinien und -Einstellungen . . . 36
Konfiguration einer Snapshot-Antwortrichtlinie . . . 36
Anpassung der Einstellungen für die Erstellung und Aufbewahrung von Snapshots . . . 38
Aktualisierung von ONTAP Autonomous Ransomware Protection with AI . . . 41
Eine Aktualisierungseinstellung für ARP/AI auswählen . . . 41
ARP/AI manuell mit dem neuesten Sicherheitspaket aktualisieren . . . 42
ARP/AI-Updates überprüfen . . . 43

ARP/AI 9.16.1 und höher

Informationen zu ONTAP ARP/AI (ONTAP 9.16.1 und höher)

Ab ONTAP 9.16.1 nutzt der autonome Ransomware-Schutz ein vortrainiertes Machine-Learning-Modell (ARP/AI), um sich ständig weiterentwickelnde Formen von Ransomware in NAS- und SAN-Umgebungen zu erkennen. ARP/AI bietet sofortigen aktiven Schutz ohne Lernphase und unterstützt automatische Sicherheitsupdates unabhängig von ONTAP Releases.

ARP/AI ist vom früheren ARP-Modell zu unterscheiden, das in ONTAP 9.10.1 bis 9.15.1 verwendet wurde und vor dem aktiven Schutz eine Lernphase erforderte. Ein Vergleich der Funktionen nebeneinander findet sich unter "Vergleich der Funktionen von ARP/AI und dem herkömmlichen ARP".

Funktionsweise von ARP/KI

Das Machine-Learning-Modell von ARP/AI wurde anhand eines umfangreichen Datensatzes von Dateien vor und nach einem simulierten Ransomware-Angriff vortrainiert. Dieses ressourcenintensive Training erfolgt außerhalb ONTAP mithilfe von Open-Source-Datensätzen aus der forensischen Forschung. Kundendaten werden im gesamten Modellierungsprozess nicht verwendet. Das vortrainierte Modell ist in ONTAP enthalten und kann weder über die ONTAP CLI noch über die ONTAP API aufgerufen oder geändert werden.

Sofortiger Schutz auf unterstützten Volumes

ARP/AI bietet sofortigen aktiven Schutz für die folgenden unterstützten Volume-Typen:

- NAS FlexVol Volumes mit ONTAP 9.16.1 und höher
- NAS FlexGroup Volumes mit ONTAP 9.18.1 und höher
- SAN FlexVol Volumes mit ONTAP 9.17.1 und höher (sofort aktiv, auch während der "Bewertungszeitraum")

> Für upgradespezifisches Verhalten, wie Übergänge von früheren ARP-Funktionen, siehe "Upgrade-Überlegungen für bestehende Cluster".

Automatische Sicherheitsupdates

Um stets vor den neuesten Ransomware-Bedrohungen geschützt zu sein, bietet ARP/AI regelmäßige automatische Updates, die außerhalb der regulären ONTAP-Upgrade- und Release-Zyklen erfolgen. Wenn Sie "Automatische Updates aktiviert" haben, können Sie nach Auswahl automatischer Updates für Sicherheitsdateien auch automatische Sicherheitsupdates für ARP/AI erhalten. Sie können außerdem "Diese Aktualisierungen manuell durchführen" steuern, wann diese erfolgen.

Ab ONTAP 9.16.1 sind Sicherheitsupdates für ARP/AI über System Manager zusätzlich zu System- und Firmware-Updates verfügbar.

"Weitere Informationen zu ARP/AI Updates"

Was ARP/AI erkennt

ARP/AI identifiziert eingehende Daten als entweder verschlüsselt oder Klartext und verwendet ein vortrainiertes Machine-Learning-Modell, das mehrere entropiebasierte Signale und Dateiverhaltensmuster gleichzeitig auswertet, um Ransomware-Aktivitäten in Echtzeit zu erkennen.

ARP/AI 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/AI bietet eine zusätzliche Verteidigungsebene, falls Antivirensoftware einen Eindringling nicht erkennt.

Aktivierungsoptionen für ARP/AI

ARP/AI bietet flexible Aktivierungsoptionen auf Cluster-, SVM- und Volume-Ebene.

Automatische Standardaktivierung auf neuen Volumes

Ab ONTAP 9.18.1 ist ARP/AI auf allen neuen Volumes für AFF A-Series, AFF C-Series, ASA und ASA r2 Systeme standardmäßig aktiviert. Diese automatische Standardaktivierung gilt nicht für "Nicht unterstützte Volumes oder Konfigurationen". Es ist möglich, "ARP/AI auf bestehenden Volumes manuell aktivieren".

Sie können "Standardmäßige Aktivierung ein- oder ausschalten" jederzeit nach der Bereitstellung durchführen.

Für das upgrade-spezifische Aktivierungsverhalten, einschließlich Kulanzfrist und SnapMirror Versionsanforderungen, siehe "Upgrade-Überlegungen für bestehende Cluster".

Manuelle Standardaktivierung auf neuen Volumes

Wenn Sie die automatische Standardaktivierung auf Clusterebene deaktiviert haben, besteht auch die Möglichkeit, "ARP/AI ist standardmäßig auf allen neuen Volumes manuell aktiviert" auf SVM-Ebene auszuwählen. Für ONTAP 9.17.1 und frühere Versionen ist dies die einzige Möglichkeit, ARP/AI standardmäßig auf neuen Volumes zu aktivieren.

Aktivierung auf allen oder bestimmten bestehenden Volumes

Ab ONTAP 9.18.1 ist es möglich, ARP/AI manuell auf allen vorhandenen Volumes auf Clusterebene zu aktivieren (unter **Cluster > Sicherheit** und ⋮ im Abschnitt **Anti-ransomware** dann **Auf allen vorhandenen Volumes aktivieren** auswählen).

Zur Aktivierung von ARP/AI auf einem bestimmten Volume siehe "ARP/AI auf einem Volume aktivieren".

ARP/AI-Schutzmodi

ARP/AI schützt Volumes sofort ohne Lernphase. Die folgenden Tabellen beschreiben das Schutzverhalten je nach Volume-Typ.

NAS-Volumes

Modus	Beschreibung	Volume-Typen und Versionen
Auswertung	Zur Ermittlung des grundlegenden Verschlüsselungsverhaltens wird eine zwei- bis vierwöchige Evaluierungsphase durchgeführt, während ARP/AI während der Evaluierungsphase sofortigen aktiven Schutz bietet. Erkennungen und Warnmeldungen können auftreten, während die Basisschwellenwerte festgelegt werden. Ob die Evaluierungsphase abgeschlossen ist, lässt sich durch Ausführen des `security anti-ransomware volume show` Befehls und Überprüfen von `Block device detection status` feststellen. "Informationen zum ARP/AI-Evaluierungszeitraum für Block-Device-Workloads".	NAS FlexVol Volumes mit von ONTAP erkannten Hypervisor-virtuellen Festplatten mit ONTAP 9.17.1P5 und höher
Aktiv	ARP/AI überwacht die Arbeitslastaktivität und reagiert automatisch, wenn ungewöhnliches Verhalten erkannt wird, das auf einen Ransomware-Angriff hindeutet. Auf eine Warnung kann reagiert werden, um Daten zu schützen, oder die Warnung kann als Fehlalarm markiert werden. Die Markierung einer Warnung als Fehlalarm aktualisiert das Erkennungsmodell. Wenn die Warnung durch ungewöhnliches Dateiverhalten ausgelöst wird und sie als Fehlalarm markiert wird, erfolgt beim nächsten Auftreten dieses Musters keine Warnung mehr.	• NAS FlexVol Volumes mit ONTAP 9.16.1 und höher • NAS FlexGroup Volumes mit ONTAP 9.18.1 und höher

SAN-Volumes

Modus	Beschreibung	Volume-Typen und Versionen
Auswertung	Zur Ermittlung des Verschlüsselungsverhaltens im Normalbetrieb wird eine zwei- bis vierwöchige Evaluierungsphase durchgeführt, während ARP/AI während der Evaluierungsphase sofortigen aktiven Schutz für SAN-Volumes bietet. Erkennungen und Warnmeldungen können auftreten, während die Schwellenwerte festgelegt werden. Ob die Evaluierungsphase abgeschlossen ist, lässt sich durch Ausführen des `security anti-ransomware volume show` Befehls und Überprüfung von `Block device detection status` feststellen. "Informationen zum ARP/AI-Evaluierungszeitraum für Block-Device-Workloads".	SAN FlexVol Volumes mit ONTAP 9.17.1 und höher

Modus	Beschreibung	Volume-Typen und Versionen
Aktiv	Nach Ablauf der Testphase lässt sich feststellen, ob der ARP/AI SAN-Schutz aktiv ist, indem der `security anti-ransomware volume show` Befehl ausgeführt und `Block device detection status` überprüft wird. Ein Status von `Active_suitable_workload` zeigt an, dass die bewertete Entropiemenge erfolgreich überwacht werden kann. ARP/AI passt den adaptiven Schwellenwert automatisch entsprechend den während der Auswertung geprüften Daten an.	SAN FlexVol Volumes mit ONTAP 9.17.1 und höher

Gefährdungsanalyse

ARP/AI bewertet die Bedrohungswahrscheinlichkeit kontinuierlich, während Daten auf den Speicher geschrieben werden. Wenn das Machine-Learning-Modell feststellt, dass eine Aktivität einem Ransomware-Profil entspricht, generiert ONTAP eine EMS-Benachrichtigung mit der **mittleren** Bedrohungsstufe, die eine Bewertung der Bedrohung nahelegt. ARP/AI verwendet keine niedrige Bedrohungsstufe; alle Erkennungen werden mit der mittleren Stufe gemeldet.

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

Weitere Informationen finden Sie unter "Auf abnormale Aktivität reagieren".

ARP/AI Snapshots

ARP/AI erstellt einen Snapshot, sobald erste Anzeichen eines Angriffs erkannt werden. Anschließend wird eine Analyse durchgeführt, um den potenziellen Angriff zu bestätigen oder auszuschließen. Ab ONTAP 9.17.1 generiert ARP/AI Snapshots zudem regelmäßig alle 4 Stunden; das Vorhandensein dieser Snapshots ist nicht als Anomalie zu werten. Wird ein Angriff bestätigt, wird die Angriffswahrscheinlichkeit auf `Moderate` gesetzt und eine Angriffsbenachrichtigung generiert.

Die folgende Tabelle fasst das Verhalten von ARP/AI Snapshots zusammen.

Funktion	ARP/AI Modell (ONTAP 9.16.1 und höher)
Auslöser für die Erstellung	**ONTAP 9.16.1:** • Bestätigung eines Angriffs **ONTAP 9.17.1 und höher:** • Snapshots werden in festen 4-Stunden-Intervallen erstellt, unabhängig von einem bestimmten Auslöser • Bestätigung eines Angriffs Ein „periodischer“ oder „Angriffs“-Snapshot wird abhängig vom Auslösertyp erstellt.

Funktion	ARP/AI Modell (ONTAP 9.16.1 und höher)
Konvention für vorangestellte Namen	**ONTAP 9.16.1:** "Anti_ransomware_backup" **ONTAP 9.17.1 und höher:** "Anti_ransomware_periodic_backup" "Anti_ransomware_attack_backup"
Löschverhalten	Der ARP/AI Snapshot ist gesperrt und kann vom Administrator nicht gelöscht werden.
Maximale Snapshot-Anzahl	"Konfigurierbares Snapshot-Limit"; Standardwert ab ONTAP 9.20.1 von 6 auf 2 reduziert, sofern der Standardwert nicht zuvor geändert wurde
Aufbewahrungsfrist	Snapshots werden normalerweise 12 Stunden lang aufbewahrt (ab ONTAP 9.20.1 standardmäßig 7 Stunden, sofern die Standardeinstellung nicht zuvor geändert wurde). • NAS Volumes: Wenn ein Angriff durch eine Dateianalyse bestätigt wird, werden Snapshots, die vor dem Angriff erstellt wurden, so lange aufbewahrt, bis der Administrator den Angriff als echt oder als Fehlalarm (clear-suspect) kennzeichnet. • SAN Volume oder VM-Datenspeicher: Wenn ein Angriff durch eine Blockentropieanalyse bestätigt wird, werden Snapshots, die vor dem Angriff erstellt wurden, für 10 Tage (konfigurierbar) aufbewahrt.
Clear-suspect-Aktion	Administratoren können eine „Verdacht klären“-Aktion durchführen, die die Aufbewahrung auf Basis einer Bestätigung festlegt: • 24 Stunden für falsch-positive Aufbewahrung • 7 Tage für die True-Positive-Retention
Ablaufzeit	Für alle Snapshots ist eine Ablaufzeit festgelegt.

SnapMirror synchron und aktive Synchronisierung

Ab ONTAP 9.19.1 gelten für ARP/AI-Snapshots, die für Volumes erstellt werden, die an SnapMirror synchronen oder SnapMirror active sync Beziehungen teilnehmen, folgende zusätzliche Regeln:

- ARP/AI-Snapshots werden auf dem primären Volume erstellt und beibehalten.
- ARP/AI-Snapshots werden nicht als Teil von SnapMirror synchron oder SnapMirror active sync auf den sekundären Server repliziert. Nach dem Failover ist "ARP/AI wieder aktivieren" auf dem Wiederherstellungsvolume erforderlich.

> Die Wiederherstellung auf Volume-Ebene (`volume snapshot restore` bei SnapMirror synchron oder SnapMirror active sync SAN-Volumes kann es erforderlich machen, die SnapMirror synchron oder SnapMirror active sync Beziehung vorübergehend zu quiescieren oder zu unterbrechen. In vielen Fällen lässt sich das Unterbrechen von SnapMirror synchron oder SnapMirror active sync vermeiden, indem FlexClone oder Wiederherstellungsvorgänge auf Dateiebene aus ARP/AI- oder anderen Snapshots des primären Volumes verwendet werden.

"Erfahren Sie mehr über die Unterstützung für SnapMirror synchron und SnapMirror active sync".

Auf einen Angriff reagieren und ihn bewerten

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

- "Reaktion auf abnormale Aktivität: ARP/AI"
- "Feststellen, ob ein Ransomware-Angriff tatsächlich vorliegt"

Daten nach einem Angriff wiederherstellen

Wenn der Angriff bestätigt wird, kann das Volume mithilfe des ARP/AI Snapshot wiederhergestellt werden. Betroffene Dateien lassen sich aus ausgewählten Snapshots wiederherstellen, ohne das gesamte Volume zurückzusetzen.

- "Daten aus ARP/AI 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/AI-Konfiguration zwei oder mehr authentifizierte Benutzeradministratoren erforderlich sind. Weitere Informationen finden sich unter "Multi-Admin-Verifizierung aktivieren".

Verwandte Informationen

- "ARP/AI unterstützte Konfigurationen"
- "ONTAP-Befehlsreferenz"

Unterstützte Konfigurationen für ONTAP ARP/AI

Autonomous Ransomware Protection mit KI (ARP/AI) ist für NAS (ab ONTAP 9.16.1) und SAN (ab ONTAP 9.17.1) Workloads verfügbar. Vor der Bereitstellung von ARP/AI sollten die unterstützten Konfigurationen und Anwendungsfälle geprüft und bestätigt werden, dass die Umgebung die Anforderungen erfüllt.

Wenn Sie ONTAP 9.15.1 oder eine frühere Version verwenden, siehe "Unterstützte Konfigurationen für ARP".

Geeignete Workloads

ARP/AI eignet sich für folgende Arten von Arbeitslasten:

- Datenbanken auf NFS oder SAN-Speicher
- Windows oder Linux Home-Verzeichnisse
- Bilder und Videos (zum Beispiel Krankenakten und Electronic Design Automation (EDA)-Daten)
- SAN-Workloads auf Volumes mit LUNs oder NVMe Namespaces (ONTAP 9.17.1 und höher)

- Workloads virtueller Maschinen auf VMware, Hyper-V, KVM und OpenStack (ONTAP 9.17.1 und höher)

Ungeeignete Workloads

ARP/AI ist für diese Art 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/AI hängt von der Fähigkeit ab, einen ungewöhnlichen Anstieg bei Datei-Erstellungs-, Umbenennungs- oder Löschvorgängen zu erkennen. Wenn die Anwendung selbst die Quelle der Dateiaktivität ist, kann sie nicht wirksam von Ransomware-Aktivität unterschieden werden.

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

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

- Workloads innerhalb von VMs, die eine große Anzahl hochkomprimierter oder verschlüsselter Dateien beinhalten (wie 7z, ZIP oder passwortgeschützte PDF oder DOC Dateien).

Unterstützte Konfigurationen

ARP/AI unterstützt NAS- und SAN-Workloads über verschiedene ONTAP Versionen und Umgebungen hinweg. Die unterstützten Funktionen sollten überprüft werden, um zu bestätigen, dass Ihre Umgebung vor der Bereitstellung von ARP/AI unterstützt wird.

Basisunterstützung

Die ARP/AI-Unterstützung beginnt in ONTAP 9.16.1 und umfasst NAS-Workloads (NFS und SMB) auf FlexVol Volumes und MetroCluster Konfigurationen, ohne dass eine Lernphase erforderlich ist.

Protokoll- und Hypervisor-Unterstützung nach ONTAP Version

- ONTAP 9.17.1 und höher: SAN Block-Device-Workloads (Volumes mit LUNs oder NVMe-Namespaces) und NAS-Volumes mit VMware Virtual Disks.
- ONTAP 9.17.1P5 und höher: NAS-Volumes mit Hyper-V, KVM und OpenStack Hypervisoren.

Matrix für Funktions- und Konfigurationsunterstützung

Unterstützung für zusätzliche Konfigurationen und Volumentypen ist in den folgenden ONTAP Versionen verfügbar:

	ONTAP 9.20.1	ONTAP 9.19.1	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1
Volumes, die mit SnapMirror asynchron geschützt sind	✓	✓	✓	✓	✓

	ONTAP 9.20.1	ONTAP 9.19.1	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1
Mit SnapMirror synchron[1] geschützte Volumes	✓	✓			
Mit SnapMirror active sync geschützte Volumes [1]	✓	✓			
SVMs, die mit SnapMirror asynchron (SVM-Notfallwiederherstellung) geschützt sind	✓	✓	✓	✓	✓
SVM Datenmobilität (`vserver migrate`)	✓	✓	✓	✓	✓
FlexGroup Volumes	✓	✓	✓	✓ [2]	✓ [2]
Multi-Admin-Verifizierung	✓	✓	✓	✓	✓
Standardmäßige Aktivierung von ARP/AI	✓	✓	✓		
Konfigurierbare Snapshot-Reaktionsrichtlinie	✓				

[1] Ab ONTAP 9.19.1 unterstützt ARP/AI primäre Volumes in SnapMirror synchronen Beziehungen für NAS und SAN auf FAS, AFF A-Series, AFF C-Series und AFX Systemen sowie primäre Volumes in SnapMirror active sync SAN Beziehungen auf AFF A-Series, AFF C-Series und ASA r2 Systemen. Weitere Informationen sind unter [SnapMirror] zu finden.

[2] ONTAP 9.16.1 und 9.17.1 FlexGroup Volumes verwenden das ARP-Modell vor ARP/AI, vollständige ARP/AI-Unterstützung für FlexGroup Volumes beginnt in ONTAP 9.18.1.

SnapMirror und ARP/AI Interoperabilität

Ab ONTAP 9.12.1 wird ARP auf SnapMirror asynchronen Ziel-Volumes unterstützt.

Ab ONTAP 9.19.1 unterstützt ARP/AI primäre Volumes, die an SnapMirror synchronen und SnapMirror active sync SAN-Beziehungen teilnehmen, mit folgendem Verhalten:

- ARP/AI wird auf *primären* Volumes in SnapMirror synchronen Beziehungen für NAS und SAN auf FAS, AFF A-Series, AFF C-Series und AFX-Systemen unterstützt.

- ARP/AI wird auf *primären* Volumes in SnapMirror active sync SAN-Beziehungen auf AFF A-series, AFF C-series und ASA r2-Systemen unterstützt.
- ARP/AI-Analysen laufen nur auf dem aktiven, schreib- und lesefähigen primären Volume in SnapMirror synchron und SnapMirror active sync SAN-Beziehungen.
- ARP/AI-Snapshots werden nicht auf das sekundäre Volume in SnapMirror synchronen oder SnapMirror active sync-Beziehungen repliziert. Nach einem Failover ist "ARP/AI wieder aktivieren" auf dem Wiederherstellungsvolume erforderlich.

> Da jeder Schreibvorgang auf beide Volumes in einer synchronen Spiegelbeziehung geschrieben wird, reicht es aus, ARP/AI nur auf dem primären Volume zu aktivieren, um Anomalien zu erkennen. Die von der ARP/AI-Analyse auf dem primären Volume generierten internen Metadaten werden auf das sekundäre Volume repliziert. Aus diesem Grund sind die erforderlichen Metadaten bereits vorhanden, wenn ARP/AI nach einem Failover auf dem sekundären Volume aktiviert wird.

Wenn ein SnapMirror asynchrones Quellvolume ARP/AI-fähig ist, übernimmt das SnapMirror Zielvolume automatisch den ARP/AI-Konfigurationsstatus (wie `enabled`), die ARP/AI-Sicherheitsdaten und die von ARP/AI erstellten Snapshots des Quellvolumes. Eine explizite Aktivierung ist nicht erforderlich.

Obwohl das asynchrone Zielvolume aus schreibgeschützten (RO) Snapshots besteht, findet keine ARP/AI-Verarbeitung der Daten statt. Wird das SnapMirror asynchrone Zielvolume jedoch in ein Lese-/Schreibvolume (RW) umgewandelt, ist ARP/AI auf dem RW-konvertierten Zielvolume automatisch aktiviert.

ARP/AI und virtuelle Maschinen

ARP/AI unterstützt virtuelle Maschinen (VMs) auf VMware, Hyper-V, KVM und OpenStack. VMware-Unterstützung beginnt mit ONTAP 9.17.1; Hyper-V-, KVM- und OpenStack-Unterstützung beginnt mit ONTAP 9.17.1P5. Die ARP/AI-Erkennung verhält sich unterschiedlich bei Änderungen innerhalb und außerhalb der VM. ARP/AI wird nicht für Workloads empfohlen, die eine große Anzahl stark komprimierter Dateien (wie 7z und ZIP) oder verschlüsselter Dateien (wie passwortgeschützte PDF-, DOC- oder ZIP-Dateien) innerhalb der VM umfassen.

Änderungen außerhalb der VM

ARP/AI kann Dateierweiterungsänderungen auf einem NFS-Volume außerhalb der VM erkennen, wenn eine neue Erweiterung im verschlüsselten Zustand auf das Volume gelangt oder wenn sich eine Dateierweiterung ändert.

Änderungen innerhalb der VM

Wenn ein Ransomware-Angriff Dateien innerhalb der VM verändert, ohne Änderungen außerhalb der VM vorzunehmen, erkennt ARP/AI die Bedrohung, falls die Standardentropie der VM niedrig ist (z. B. .txt, .docx oder .mp4 Dateien). Ab ONTAP 9.17.1 mit SAN-Unterstützung generiert ARP/AI zusätzlich eine Bedrohungswarnung, wenn eine Entropieanomalie innerhalb der VM erkannt wird.

Wenn die Dateien standardmäßig eine hohe Entropie aufweisen (z. B. .gzip-Dateien oder passwortgeschützte Dateien), sind die Erkennungsfähigkeiten von ARP/AI eingeschränkt. ARP/AI kann in diesem Fall weiterhin proaktiv Snapshots erstellen; es werden jedoch keine Warnungen ausgelöst, wenn die Dateierweiterungen nicht extern manipuliert wurden.

> Die Erkennung von Angriffen innerhalb einer VM ist nur für FlexVol Volumes verfügbar und nicht verfügbar, wenn der VM-Datenspeicher auf einem FlexGroup Volume in ONTAP 9.18.1 und später konfiguriert ist.

Nicht unterstützte Konfigurationen

ARP/AI wird in ONTAP S3 Umgebungen nicht unterstützt.

ARP/AI unterstützt die folgenden Volumenkonfigurationen nicht:

- FlexGroup Volumes mit ONTAP 9.16.1 und 9.17.1 (FlexGroup Volumes verwenden in diesen Versionen das ältere ARP-Modell; ARP/AI-Unterstützung für FlexGroup Volumes beginnt in ONTAP 9.18.1)
- FlexCache Volumes (ARP/AI wird auf Ursprungs-FlexVol Volumes, aber nicht auf Cache Volumes unterstützt)
- Offline Volumes
- SnapLock Volumes
- SnapMirror active sync in ONTAP 9.18.1 und früher
- SnapMirror synchron in ONTAP 9.18.1 und früher
- Kaskadierte Konfigurationen von einem SnapMirror synchronen Zielvolume
- Eingeschränkte Volumes
- Root Volumes von Storage-VMs
- Volumes gestoppter Storage-VMs
- FlexVol zu FlexGroup Konvertierung (ARP/AI muss vor der Konvertierung deaktiviert werden)

ARP/AI-Leistung und Frequenzüberlegungen

ARP/AI hat nur minimale Auswirkungen auf die Systemleistung, gemessen an Durchsatz und maximaler IOPS. Die Auswirkungen 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	• NAS: 4% der maximalen IOPS für ONTAP 9.16.1 und höher • SAN: 5 % der maximalen IOPS für ONTAP 9.17.1 und höher

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

Die standardmäßige Aktivierung von ARP/AI auf einer großen Anzahl neuer Volumes kann die Systemressourcennutzung erhöhen. Beim Aktivieren von ARP/AI auf Volumes sind die Speicherplatzanforderungen konkurrierender Prozesse wie Snapshots zu berücksichtigen.

Ab ONTAP 9.18.1 unterstützt ARP/AI erhöhte Volumenbegrenzungen basierend auf Plattformtyp und CPU-Kernanzahl:

Plattformtyp	Maximale Anzahl ARP/AI-fähiger Volumes pro Knoten
Low-end (Systeme mit bis zu 20 CPU-Kernen)	250
Mittel (Systeme mit bis zu 64 CPU-Kernen)	750
High-end (Systeme mit mehr als 64 CPU-Kernen)	1000

Die Angabe zur Anzahl der CPU-Kerne bezieht sich auf jeden einzelnen Knoten in einem 2-Node-HA-Paar.

Upgrade-Überlegungen für bestehende Cluster

Wenn ein neues ONTAP 9.18.1 oder neuer Cluster bereitgestellt wird, ist ARP/AI auf neuen Volumes standardmäßig automatisch aktiviert. Siehe "Informationen zu ARP/KI".

Beim Upgrade auf ONTAP 9.18.1 oder höher auf AFF A-Series, AFF C-Series, ASA oder ASA r2 Systemen wird ARP/AI nach einer 12-stündigen Übergangsphase standardmäßig automatisch für neue Volumes aktiviert. Während der Übergangsphase ist es möglich, "Automatische Aktivierung ablehnen". Bestehende Volumes bleiben unverändert; "ARP/AI manuell aktivieren" muss für bestehende Volumes durchgeführt werden.

Für FlexGroup Volumes, die von ONTAP 9.17.1 oder früher auf ONTAP 9.18.1 aktualisiert wurden, wird ARP/AI automatisch verfügbar und Volumes im Lernmodus werden in den aktiven Modus überführt.

Multi-Admin-Verifizierung mit ARP/AI-geschützten Volumes

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

ARP/AI aktivieren

ONTAP ARP/AI auf einem Volume aktivieren

Ab ONTAP 9.16.1 ist es möglich, den autonomen Ransomware-Schutz mit KI (ARP/AI) auf einem bestehenden Volume zu aktivieren oder ein neues Volume mit aktiviertem ARP/AI zu erstellen. ARP/AI ist sofort aktiv, eine Lernphase ist nicht erforderlich.

Wenn Sie ONTAP 9.15.1 oder eine frühere Version verwenden, siehe "ARP auf einem Volume aktivieren".

Über diese Aufgabe

ARP/AI ist das aktuelle Ransomware-Schutzmodell für ONTAP 9.16.1 und höher. Die Aktivierung von ARP/AI erfolgt entsprechend der für Ihre Umgebung passenden Vorgehensweise, nachdem sichergestellt wurde, dass Ihre Umgebung die Anforderungen erfüllt.

- NAS mit FlexVol Volumes (ONTAP 9.16.1 und höher)
- NAS mit FlexGroup Volumes (ONTAP 9.18.1 und höher)
- SAN-Volumes (ONTAP 9.17.1 und höher)

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

Vor der Aktivierung von ARP/AI muss sichergestellt sein, dass Ihre Umgebung Folgendes aufweist:

NAS-spezifische Anforderungen

- Eine Storage-VM (SVM) mit aktiviertem NFS- oder SMB-Protokoll (oder beiden).
- NAS-Workload mit konfigurierten Clients.
- Ein aktives "Verbindungspfad" für das Volume.

SAN-spezifische Anforderungen

- Eine Storage VM (SVM) mit aktiviertem iSCSI, FC oder NVMe Protokoll.
- SAN-Workload mit konfigurierten Clients.

Allgemeine Anforderungen

- 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/AI auf NAS FlexVol Volumes aktivieren

Ab ONTAP 9.16.1 ist ARP/AI für NAS FlexVol Volumes sofort nach der Aktivierung aktiv.

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

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

CLI

ARP/AI auf einem vorhandenen Volume aktivieren:

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

Neues Volume mit aktiviertem ARP/AI erstellen:

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

Den ARP/AI-Status überprüfen:

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

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

ARP/AI auf NAS FlexGroup Volumes aktivieren

Ab ONTAP 9.18.1 ist ARP/AI für FlexGroup Volumes sofort nach der Aktivierung aktiv.

Für ONTAP 9.13.1 bis 9.17.1 verwenden FlexGroup Volumes das frühere ARP-Modell und benötigen eine Lernphase. Siehe "ARP auf NAS FlexGroup Volumes 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. Der ARP/AI-Status des Volumes im **Anti-ransomware**-Feld kann überprüft werden.

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

CLI

ARP/AI auf einem vorhandenen FlexGroup Volume aktivieren:

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

Ein neues FlexGroup Volume mit aktiviertem ARP/AI erstellen:

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

Den ARP/AI-Status überprüfen:

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

ARP/AI auf SAN Volumes aktivieren

Ab ONTAP 9.17.1 kann ARP/AI auf SAN-Volumes aktiviert werden. ARP/AI ist unmittelbar nach der Aktivierung automatisch aktiv und beginnt, die SAN-Volumes während der "Entropiebewertungszeitraum"Laufzeit zu überwachen und zu schützen, während gleichzeitig ermittelt wird, ob Workloads für ARP/AI geeignet sind, und ein optimaler Verschlüsselungsschwellenwert für die Erkennung festgelegt wird.

System Manager

1. **Speicher > Volumes** auswählen und dann das SAN-Volume auswählen, das geschützt werden soll.
2. Im Tab **Sicherheit** der **Volumes**-Übersicht **Status** auswählen, um von Deaktiviert auf Aktiviert zu wechseln.
3. ARP/AI wechselt automatisch in die Evaluierungsphase.
4. Der ARP/AI-Status und der Auswertungsstatus im **Anti-ransomware**-Feld können überprüft werden.

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

CLI

ARP/AI auf einem vorhandenen SAN Volume aktivieren:

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

Ein neues SAN-Volume mit aktiviertem ARP/AI erstellen:

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
```

```
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

Den ARP/AI-Status und den Auswertungsstatus überprüfen:

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

Das `Block device detection status` Feld kann zur Überwachung des Fortschritts des Evaluierungszeitraums herangezogen werden. Weitere Informationen zu `security anti-ransomware volume show` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "ARP/AI Entropieauswertungszeitraum für SAN Volumes"

ONTAP ARP/AI ist in neuen Volumes standardmäßig aktiviert

Ab ONTAP 9.16.1 können Storage-VMs (SVMs) so konfiguriert werden, dass neue Volumes standardmäßig mit Autonomous Ransomware Protection with AI (ARP/AI) aktiviert sind. Ab ONTAP 9.18.1 wird ARP/AI "Unterstützte Systeme" nach einer 12-stündigen Kulanzfrist automatisch auf Clusterebene aktiviert. Dieses Verfahren ist anzuwenden, wenn ARP/AI standardmäßig für neue Volumes auf SVM-Ebene statt auf Clusterebene aktiviert werden soll.

Für ONTAP 9.17.1 und früher ist die Konfiguration auf SVM-Ebene die einzige Möglichkeit, ARP standardmäßig auf neuen Volumes zu aktivieren.

Wenn Sie ONTAP 9.15.1 oder eine frühere Version verwenden, siehe "ARP standardmäßig in neuen Volumes aktivieren".

Für ONTAP 9.13.1 bis 9.17.1 verwenden FlexGroup Volumes das frühere ARP-Modell und benötigen eine Lernphase. Siehe "ARP standardmäßig in neuen Volumes aktivieren".

Über diese Aufgabe

Auf Systemen, auf denen ARP/AI nicht automatisch auf Clusterebene aktiviert ist, werden neue Volumes standardmäßig mit deaktivierter ARP/AI-Funktionalität erstellt. ARP/AI muss aktiviert und so konfiguriert werden, dass es für neue in der SVM erstellte Volumes standardmäßig aktiviert ist.

Vorhandene Volumes ohne aktiviertes ARP/AI ändern ihren ARP/AI-Aktivierungsstatus nicht automatisch, wenn die SVM-Standardeinstellung geändert wird. Die in diesem Verfahren beschriebene SVM-Einstellung betrifft nur neue Volumes. Informationen dazu, wie "ARP/AI für bestehende Volumes aktivieren".

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

Bevor ARP/AI standardmäßig aktiviert wird, muss sichergestellt sein, dass Ihre Umgebung Folgendes aufweist:

NAS-spezifische Anforderungen

- Eine Storage-VM (SVM) mit aktiviertem NFS- oder SMB-Protokoll (oder beiden).
- Ein aktives "Verbindungspfad" für das Volume.

SAN-spezifische Anforderungen

- Eine Storage VM (SVM) mit aktiviertem iSCSI, FC oder NVMe Protokoll.

Allgemeine Anforderungen

- 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/AI standardmäßig für neue Volumes auf SVM-Ebene zu aktivieren.

System Manager

1. **Speicher** oder **Cluster** (je nach Umgebung) auswählen, **Speicher-VMs** auswählen und die Speicher-VM auswählen, die die Volumes enthält, die mit ARP/AI 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/AI) zu aktivieren. Aktivieren Sie das zusätzliche Kontrollkästchen, um ARP/AI auf allen geeigneten Volumes in der Storage-VM zu aktivieren.

ARP/AI wechselt sofort in den aktiven Modus; eine Lernphase ist nicht erforderlich.

CLI

Eine bestehende SVM so modifizieren, dass ARP/AI in neuen Volumes standardmäßig aktiviert ist

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume
```

```
-state enabled
```

Eine neue SVM mit standardmäßig aktiviertem ARP/AI für neue Volumes erstellen

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

Den ARP/AI-Status überprüfen

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

Verwandte Informationen

- "Von der automatischen ARP/AI-Aktivierung abmelden"
- "security anti-ransomware volume show"

Automatische Aktivierung von ONTAP ARP/AI während Upgrades verwalten

Beim Upgrade auf ONTAP 9.18.1 oder höher wird der Autonomous Ransomware Protection mit AI (ARP/AI) nach einer 12-stündigen Karenzzeit standardmäßig auf allen neuen Volumes für AFF A-Serie, AFF C-Serie, ASA und ASA r2 Systeme aktiviert, sofern eine Anti-Ransomware-Lizenz installiert ist. Dieses Verfahren ermöglicht es, die automatische Standardaktivierung während oder nach der Karenzzeit abzuwählen oder die Einstellung jederzeit nach dem Upgrade zu ändern.

Wenn Sie ONTAP 9.15.1 oder eine frühere Version verwenden, siehe "Informationen zum autonomen Ransomware-Schutz".

Wenn Sie ONTAP 9.17.1 oder eine frühere Version verwenden, gilt die automatische Standardaktivierung auf Clusterebene nicht. Die Standardaktivierung auf SVM-Ebene kann mit "ARP/AI ist in neuen Volumes standardmäßig aktiviert" konfiguriert werden.

Vorhandene Volumes müssen "manuell aktiviert"für ARP/AI sein.

Ab ONTAP 9.19.1 gilt die standardmäßige ARP/AI-Aktivierung für Cluster, die SnapMirror synchron und SnapMirror active sync SAN-Beziehungen enthalten. In ONTAP 9.18.1 war die Standardaktivierung für diese Konfigurationen unterdrückt. Für clusterübergreifende SnapMirror synchron Beziehungen erfolgt die Standardaktivierung, nachdem sowohl der Quell- als auch der Ziel-Cluster auf ONTAP 9.19.1 aktualisiert wurden.

Über diese Aufgabe

Die von Ihnen gewählte Einstellung kann später geändert werden. Nach Ablauf der Testphase besteht jederzeit die Flexibilität, die automatische Standardaktivierung ein- oder auszuschalten:

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
```

```
false|true
```

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um die automatische Standardaktivierung von ARP/AI zu verwalten.

System Manager

1. **Cluster > Einstellungen** auswählen.
2. Führen Sie einen der folgenden Schritte aus:
   - Während der aktiven Kulanzfrist deaktivieren:
     i. Im Abschnitt **Anti-ransomware** wird eine Meldung angezeigt, die die verbleibenden Stunden bis zur Aktivierung von ARP/AI angibt. **Nicht aktivieren** auswählen.
     ii. Im nächsten Dialogfeld **Deaktivieren** auswählen, um zu bestätigen, dass die standardmäßige ARP/AI-Aktivierung für neue Volumes deaktiviert ist.
   - Nach Ablauf der Kulanzfrist deaktivieren:
     i. Im Abschnitt **Anti-ransomware** wählen Sie .
     ii. Das Kontrollkästchen auswählen und anschließend **Speichern** wählen, um die automatische Standardaktivierung von ARP/AI für neue Volumes zu deaktivieren.

CLI

1. Status der automatischen Aktivierung prüfen:

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

2. Automatische Standardaktivierung für neue Volumes deaktivieren:

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false
```

Verwandte Informationen

- "ARP/AI auf einem einzelnen Volume aktivieren"

Informationen zur Entropieauswertung von ONTAP ARP/AI für Blockgeräte-Workloads

Ab ONTAP 9.17.1 benötigt ARP/AI eine Evaluierungsphase, um festzustellen, ob die Entropiewerte für Blockgeräte-Workloads für den Schutz vor Ransomware geeignet sind. Zu diesen Workloads gehören SAN LUNs und virtuelle Hypervisor-Festplatten (zum Beispiel VMware-Festplatten in NFS-Datenspeichern und ab ONTAP 9.17.1P5 Hyper-V, KVM und OpenStack virtuelle Festplatten), die in ONTAP Volumes gespeichert sind. Nach der Aktivierung von ARP/AI auf einem geeigneten Volume überwacht und schützt

es dieses während der Evaluierungsphase aktiv und ermittelt gleichzeitig einen optimalen Verschlüsselungsschwellenwert.

Diese Seite gilt für ARP/AI (ONTAP 9.17.1 und höher). ARP unterstützt SAN-Volumes in früheren Versionen von ONTAP nicht.

Unterstützte Workloads und Anwendbarkeit der Evaluierung

Die Evaluierungsfrist für Blockgeräte gilt in den folgenden Szenarien:

- **SAN Volumes**: LUN-basierte Workloads, die Hosts oder Hypervisoren als Blockgeräte bereitgestellt werden.
- **NAS-Volumes, die Hypervisor-Virtual-Disks enthalten und von ONTAP automatisch erkannt werden**: Unterstützte Hypervisoren sind VMware, Hyper-V, KVM und OpenStack Virtual Disks, die in NFS- oder SMB-Datenspeichern gespeichert sind.

Innerhalb dieser Volumes:

- Der Auswertungszeitraum *ist* anwendbar auf Angriffe, die anhand von Entropieänderungen innerhalb des Gastdateisystems der virtuellen Festplatte erkannt werden (zum Beispiel Ransomware, die auf Dateien innerhalb des Gastbetriebssystems operiert, die einer LUN oder virtuellen Festplatte zugeordnet sind).
- Der Auswertungszeitraum gilt nicht für Angriffe, die anhand von Entropie- und Dateierweiterungsänderungen erkannt werden, die direkt an den virtuellen Festplattendateien vom Hypervisor-Host aus vorgenommen werden (zum Beispiel Ransomware, die direkt auf .vmdk-Dateien von einem ESXi NFS-Datenspeicher-Mountpunkt zugreift). Diese Direct-to-Disk-Angriffe verwenden einen anderen Erkennungspfad.

Entropiebewertung

Die Auswertungsphase dauert mindestens zwei Wochen und maximal vier Wochen. Werden in den ersten zwei Wochen mehr als 10 GB Daten geschrieben, ist die Auswertung nach Ablauf dieses zweiwöchigen Zeitraums abgeschlossen. Wird die 10-GB-Grenze innerhalb von zwei Wochen nicht erreicht, läuft die Auswertung weiter, bis 10 GB Daten geschrieben wurden, jedoch höchstens vier Wochen lang.

Während der Evaluierungsphase sammelt das System kontinuierlich Verschlüsselungsstatistiken in 10-Minuten-Intervallen von unterstützten Blockgeräte- und Hypervisor-Workloads. Auch werden periodische ARP/AI-Snapshots weiterhin alle vier Stunden erstellt. Überschreitet der Verschlüsselungsprozentsatz innerhalb eines Intervalls den für dieses Volume identifizierten optimalen Verschlüsselungsschwellenwert, wird eine Warnung ausgelöst, ein `Anti_ransomware_attack_backup`Snapshot erstellt und die Aufbewahrungszeit für alle periodischen ARP/AI-Snapshots erhöht.

Bestätigen, dass der Bewertungszeitraum aktiv ist

Sie können bestätigen, dass die Evaluierung aktiv ist, indem Sie den folgenden Befehl ausführen und auf einen Status von `evaluation_period` achten. Wenn ein Volume nicht für die Evaluierung geeignet ist, wird der Evaluierungsstatus nicht angezeigt.

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

Beispielantwort:

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Evaluation_period
```

Datenerfassung im Überwachungszeitraum überwachen

Sie können die Verschlüsselungserkennung in Echtzeit überwachen. Dieser Befehl gibt ein Histogramm zurück, das die Datenmenge in jedem Verschlüsselungsprozentbereich anzeigt. Das Histogramm wird alle 10 Minuten aktualisiert.

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -volume <vol_name> -duration real_time
```

Geeignete Arbeitslasten und adaptive Schwellenwerte

Die Auswertung endet mit einem der folgenden Ergebnisse:

- Die Arbeitslast eignet sich für ARP/AI. ARP/AI setzt den adaptiven Schwellenwert automatisch auf mehr als 10 % des maximalen Verschlüsselungsprozentsatzes, der während des Evaluierungszeitraums festgestellt wurde. ARP/AI setzt außerdem die Erfassung von Statistiken fort und erstellt regelmäßig ARP/AI Snapshots.
- Die Arbeitslast ist für ARP/AI ungeeignet. ARP/AI setzt den adaptiven Schwellenwert automatisch auf den maximalen Verschlüsselungsprozentsatz, der während des Evaluierungszeitraums festgestellt wurde. ARP/AI setzt außerdem die Erfassung von Statistiken fort und erstellt regelmäßig ARP/AI-Snapshots, jedoch empfiehlt das System letztlich, ARP/AI auf dem Volume zu deaktivieren.

Ermittlung der Auswertungsergebnisse

Nach Ablauf des Evaluierungszeitraums legt ARP/AI den adaptiven Schwellenwert automatisch anhand der Evaluierungsergebnisse fest. Die Evaluierungsergebnisse lassen sich mit dem folgenden Befehl ermitteln. Die Eignung des Volumens wird im `Block device detection status` Feld angezeigt:

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

Beispielantwort:

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
```

```
Number of Attacks                          : -
Attack Detected By                         : -
Block device detection status              : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

Sie können auch den im Rahmen der Auswertung festgelegten Schwellenwert anzeigen:

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

Verwandte Informationen

- "Snapshot-Optionen für ARP/AI ändern"
- "ARP/AI-Angriffserkennungsparameter verwalten"
- "Auf von ARP/AI erkannte anomale Aktivitäten reagieren"

ONTAP ARP/AI-Angriffserkennungsparameter verwalten

Ab ONTAP 9.16.1 können die Parameter für die Ransomware-Erkennung auf einem bestimmten ARP/AI-fähigen 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-Workload zu verbessern.

Wenn Sie ONTAP 9.15.1 oder eine frühere Version verwenden, siehe "Verwaltung der ARP-Angriffserkennungsparameter".

Funktionsweise der Erkennung von ARP/AI-Angriffen

ARP/AI nutzt ein Machine-Learning-Modell zur Erkennung von Ransomware-Aktivitäten. Wenn ARP/AI sich im aktiven Modus befindet (oder im Evaluierungsmodus für SAN-Volumes), werden die Volume-Verhaltensweisen kontinuierlich überwacht. Dazu gehören Entropie, Dateierweiterungen und Datei-IOPS (NAS) oder Verschlüsselungsraten auf Volume-Ebene (SAN). Weitere Informationen zu den Erkennungskriterien finden sich unter "was ARP/AI erkennt".

Bestimmte Volumes und Workloads erfordern unterschiedliche Erkennungsparameter. Beispielsweise kann ein ARP/AI-fähiges Volume zahlreiche Arten von Dateierweiterungen enthalten, in diesem Fall kann es sinnvoll sein, die Schwellenwertanzahl für bisher unbekannte Dateierweiterungen anzupassen oder diese Warnungen vollständig zu deaktivieren.

Ab ONTAP 9.14.1 ist die Konfiguration von Benachrichtigungen möglich, wenn ARP/AI eine neue Dateierweiterung erkennt oder wenn ARP/AI einen Snapshot erstellt. Weitere Informationen finden sich unter ARP/AI-Warnungen konfigurieren.

Angriffserkennung in NAS-Umgebungen

ARP/AI gibt eine Bedrohungswarnung aus, wenn eine der folgenden Bedingungen erkannt wird:

- Daten mit hoher Entropie
- Mehrere Dateien mit derselben noch nie zuvor gesehenen Dateiendung (innerhalb eines Zeitraums von 48 Stunden beobachtet)

> Um die Anzahl falsch positiver Warnmeldungen zu reduzieren, zu **Speicher > Volumes > Sicherheit > Workload-Merkmale konfigurieren** wechseln und **Neue Dateitypen überwachen** deaktivieren. Ab ONTAP 9.18.1 P2 zeigt System Manager keine ARP/AI Workload-Merkmale mehr an, einschließlich Basis- und Spitzen-Statistiken. Spitzen-Statistiken sind weiterhin über ONTAP CLI und REST API Optionen für erweiterte Analysen verfügbar.

Angriffserkennung in SAN-Umgebungen

Ab ONTAP 9.17.1 gibt ARP/AI eine Warnung aus, wenn hohe Verschlüsselungsraten erkannt werden, die einen automatisch erlernten Schwellenwert überschreiten. Dieser Schwellenwert wird nach einem "Bewertungszeitraum" festgelegt, kann aber angepasst werden.

Ändern der ARP/AI Angriffserkennungsparameter

Je nach dem zu erwartenden Verhalten des ARP/AI-fähigen Volumes kann eine Anpassung der Parameter für die Angriffserkennung sinnvoll sein.

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
          Block Device Auto Learned Encryption Threshold : 10
           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 : 5
       Never Seen before File Extensions Duration in Hour : 48
```

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/AI passt die Basiswerte für die Erkennungsparameter auch im aktiven Modus 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 solcher Anstiege als unbedenklich trägt zur Verbesserung der Genauigkeit der Bedrohungsbewertungen von ARP/AI bei.

Ein einmaliger Anstieg kann gemeldet werden

1. Wenn unter bekannten Umständen eine einmalige Lastspitze auftritt und ARP/AI eine ähnliche Lastspitze auch in Zukunft melden soll, kann die Lastspitze aus dem Workload-Verhalten entfernt werden:

```
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/AI-Warnungen konfigurieren

Ab ONTAP 9.14.1 können Benachrichtigungen für zwei Ereignisse festgelegt werden:

- Beobachtung einer neuen Dateierweiterung auf einem Volume
- Erstellung eines ARP/AI 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/AI-geschützten Volumes".

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um Warnmeldungen für ARP/AI-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/AI Snapshots:

```
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/AI Snapshots:

```
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/AI-Angriffen und dem ARP/AI-Snapshot"
- "ONTAP-Befehlsreferenz"

Auf von ONTAP ARP/AI erkannte abnormale Aktivitäten reagieren

Wenn der autonome Ransomware-Schutz mit KI (ARP/AI) ungewöhnliche Aktivitäten in einem geschützten Volume erkennt (ONTAP 9.16.1 und höher), wird eine Warnung ausgegeben. Die Benachrichtigung sollte bewertet und entweder als Fehlalarm oder als potenzieller Ransomware-Angriff eingestuft werden. Nachdem die Aktivität kategorisiert wurde, speichert ARP/AI die Bewertung, passt das Bedrohungsprofil an und setzt die normale Überwachung fort.

Wenn Sie ONTAP 9.15.1 oder eine frühere Version verwenden, siehe "Auf von ARP erkannte abnormale Aktivität reagieren".

Wenn ein Angriff kategorisiert wird, werden ARP/AI Snapshots für einen durch den Kategorisierungsvorgang initiierten verkürzten Zeitraum aufbewahrt:

- ONTAP 9.17.1 und höher: 7 Tage bei bestätigten Angriffen, 24 Stunden bei Fehlalarmen.
- ONTAP 9.16.1 und früher: 5 Tage für bestätigte Angriffe, 48 Stunden für Fehlalarme.

Sie können diese "Aufbewahrungseinstellungen" für ARP/AI Snapshots anpassen.

Über diese Aufgabe

Bei NAS-Volumes zeigt ARP/AI eine Liste verdächtiger Dateien an, wenn eine Kombination aus hoher Datenentropie, ungewöhnlicher Volume-Aktivität mit Datenverschlüsselung und ungewöhnlichen Dateierweiterungen erkannt wird.

Ab ONTAP 9.17.1:

- **Für NAS-Volumes**: ARP/AI stellt weiterhin verdächtige Dateien und Dateitypen bereit.
- **Für SAN Volumes** (Volumes, die LUNs oder NVMe Namespaces enthalten): ARP/AI bewertet die Entropie nur auf Volume-Ebene. ONTAP sieht keine einzelnen Dateien innerhalb der LUN oder des Namespace,

daher sind Listen verdächtiger Dateien und Dateitypen **nicht** verfügbar. Stattdessen meldet ARP/AI Volumenebene-Spitzen im Verschlüsselungsprozentsatz (Entropiespitzen).

Einzelheiten zu Entropiespitzen sowohl für NAS- als auch für SAN-Volumes werden auf der Anti-Ransomware-Seite im System Manager angezeigt.

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

- **Falsch positiv**: Der identifizierte Dateityp oder der Entropieanstieg ist in Ihrer Arbeitslast zu erwarten und kann ignoriert werden.
- **Potenzieller Ransomware-Angriff**: Der identifizierte Dateityp oder der Entropieanstieg 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/AI-Benachrichtigungen gelöscht haben. ARP/AI 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/AI muss ein Volume aktiv schützen und darf sich bei SAN-Volumes nicht im Auswertungsmodus befinden.

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 wiederherstellen" zu beachten.

Details zu abnormalen Aktivitäten prüfen

Sie können den System Manager oder die ONTAP CLI verwenden, um die ARP/AI-Warnungsdetails zu überprüfen, bevor ein Antwortablauf ausgewählt wird.

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. Überprüfen Sie im Tab **Sicherheit** die Details zu den ungewöhnlichen Aktivitäten:
   - Für NAS-Volumes steht der Bericht **Verdächtige Dateitypen** zur Verfügung. Ein Dialogfeld **Verdächtige Dateitypen** zeigt die von ARP/AI identifizierten Dateierweiterungen und Dateianzahlen an.
   - Prüfen Sie für NAS- und SAN-Volumes den Entropiespitzenbericht, der das Zeitfenster, die Dauer, die Menge der geschriebenen Daten und die Entropiewerte anzeigt.

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: 5/12/2025 01:03:23
   Number of Attacks: 1
   Attack Detected By: encryption_percentage_analysis
   ```

   Sie können auch EMS-Nachrichten überprüfen:

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

2. (Optional, NAS und SAN) Kürzlich erkannte Entropiespitzen auf dem Volume anzeigen:

   ```
   security anti-ransomware volume entropy-stat show-recent-high-
   encryption-stat -vserver <svm_name> -volume <vol_name>
   ```

3. (Optional) Histogramm des Verschlüsselungsprozentsatzes im Zeitverlauf anzeigen:

```
security anti-ransomware volume entropy-stat show-encryption-
percentage-histogram -vserver <svm_name> -volume <vol_name>
```

Snapshot-Verhalten beim Löschen eines vermuteten Ereignisses

- Für `volume snapshot restore` ONTAP 9.16.1 und höher sollte **zuerst das verdächtige Ereignis gelöscht** und anschließend die Wiederherstellung durchgeführt werden. Nach dem Löschen verdächtiger Dateien bleiben ARP/AI-Snapshots entsprechend der Kategorisierung der Aktivität erhalten: 7 Tage (standardmäßig), wenn die Aktivität als potenzieller Ransomware-Angriff markiert wird, oder 24 Stunden, wenn sie als Fehlalarm markiert wird. Das vorherige Löschen entfernt das Wiederherstellungsziel nicht. Zudem ist die Option clear-suspect nach einer Volume-Wiederherstellung nicht mehr verfügbar, daher muss das Löschen vor der Wiederherstellung erfolgen.
- Bei Wiederherstellungsmethoden außer `volume snapshot restore` (zum Beispiel FlexClone oder Einzeldatei SnapRestore), führen Sie zuerst die Datenwiederherstellung durch und löschen Sie anschließend das verdächtige Ereignis. Diese Methoden beeinträchtigen die Verfügbarkeit der Option „Verdächtiges Ereignis löschen“ nicht.
- Ab ONTAP 9.13.1 kann bei Verwendung von MAV zum Schutz der ARP/AI-Einstellungen der `clear-suspect`-Vorgang zusätzliche Genehmigungen erfordern. "Die Zustimmung aller Administratoren muss eingeholt werden." müssen der MAV-Genehmigungsgruppe zugeordnet sein, sonst schlägt der Vorgang fehl.

Als falsch positiv einstufen und Überwachung fortsetzen

Verwenden Sie diesen Ablauf, wenn der identifizierte Dateityp oder der Entropieanstieg für die Arbeitslast *erwartet* wird.

System Manager

1. Notieren Sie Ihre Antwort:
   - Bei NAS-Dateitypwarnungen wählen Sie die betroffenen Dateien aus, wählen Sie **Als falsch positiv markieren** und dann **Verdächtige Dateitypen aktualisieren und löschen**.
   - Bei Entropiespitzen (NAS und SAN) wählen Sie **Als falsch positiv markieren** und dann **Speichern und verwerfen**.

Diese Maßnahmen beseitigen Warnmeldungen zu verdächtigen Dateien (NAS) oder ungewöhnlicher Aktivität (NAS und SAN). Anschließend setzt ARP/AI die normale Überwachung des Volumes fort.

CLI

1. Führen Sie einen der folgenden Befehle aus, um Ihre Entscheidung zu protokollieren und die normale ARP/AI-Überwachung fortzusetzen:
   - Für NAS-Dateierweiterungen:

```
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>, … ]`

- Bei Entropiespitzen (NAS und SAN):

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY HH:MM:SS>
-end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
```

Für SAN-Volumes ist dies die einzige unterstützte Methode zur Kategorisierung abnormaler Aktivitäten; es gibt keine Listen verdächtiger Dateien oder Dateierweiterungen.

2. Ab ONTAP 9.18.1 können Sie den Status des `clear-suspect` Vorgangs ermitteln:

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

Als potenziellen Ransomware-Angriff einstufen und Daten wiederherstellen

Verwenden Sie diesen Ablauf, wenn der ermittelte Dateityp oder der Entropieanstieg für die Arbeitslast *unerwartet* ist.

System Manager

1. Klassifizieren Sie die Aktivität:
   - Bei Warnungen zu NAS-Dateitypen markiere ausgewählte Dateien als **Potenzieller Ransomware-Angriff**.
   - Bei Entropiespitzen (NAS und SAN) wählen Sie **Als potenziellen Ransomware-Angriff markieren**.
2. Bevor Sie Daten wiederherstellen, sollten Sie Ihre "Optionen für Wiederherstellungsmethoden" Sicherheitsvorkehrungen beachten. Anschließend ist eine der folgenden Optionen möglich:
   - **Zum Wiederherstellen eines Volumes**: Zuerst die Benachrichtigungen löschen, dann das Volume wiederherstellen:
     i. Klare Hinweise auf den potenziellen Angriff:
        - Bei NAS-Dateitypwarnungen wählen Sie **Aktualisieren und Verdächtige Dateitypen löschen**.
        - Bei Entropiespitzen (NAS und SAN) wählen Sie **Speichern und schließen**.

> Nachdem Sie verdächtige Dateien gelöscht haben, wird der ARP/AI Snapshot standardmäßig 7 Tage lang aufbewahrt. Wenn mehr Zeit für die Datenwiederherstellung benötigt wird, "ARP/AI Snapshot-Einstellungen anpassen" kann die Aufbewahrungsdauer des Snapshots verlängert werden. Nachdem die Datenwiederherstellung abgeschlossen ist, kann die Aufbewahrungsdauer wieder verkürzt werden.

ii. Daten mit "der aktuellste ARP/AI Snapshot oder ein früherer Snapshot" wiederherstellen.

- **Falls Sie eine andere Wiederherstellungsmethode verwenden möchten**: Stellen Sie zuerst die Daten wieder her und löschen Sie dann die Benachrichtigungen:

  i. "Stellen Sie Daten mithilfe von FlexClone oder Einzeldatei-SnapRestore wieder her".

  ii. Die Kategorisierung nach der Datenwiederherstellung abschließen, damit die normale ARP/AI-Überwachung fortgesetzt werden kann:

  - Bei NAS-Dateitypwarnungen wählen Sie **Aktualisieren und Verdächtige Dateitypen löschen**.
  - Bei Entropiespitzen (NAS und SAN) wählen Sie **Speichern und schließen**.

  ⓘ Durch das Protokollieren Ihrer Entscheidung wird der Angriffsbericht gelöscht.

CLI

1. (Nur NAS-Volumes) Erstellen Sie einen Angriffsbericht:

   a. Generieren Sie einen Angriffsbericht und geben Sie an, 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. Das verdächtige Ereignis vor der Wiederherstellung (für `volume snapshot restore`) beseitigen. Den Angriff als potenzielle Ransomware (`-false-positive false` markieren und verdächtige Dateien löschen, um die Sperre aufzuheben:

   - Für NAS-Dateierweiterungen:

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

   - Bei Entropiespitzen (NAS und SAN):

   ```
   security anti-ransomware volume attack clear-suspect -vserver
   <svm_name> -volume <vol_name> -start-time <MM/DD/YYYY HH:MM:SS>
   -end-time <MM/DD/YYYY HH:MM:SS> -false-positive false
   ```

3. Weiter zu "Daten wiederherstellen".

Daten nach einem Ransomware-Angriff mit ONTAP ARP/AI wiederherstellen

Autonomer Ransomware-Schutz mit KI (ARP/AI) erstellt Snapshots, um vor Ransomware-Bedrohungen zu schützen. Es können ARP/AI-Snapshots oder ein anderer Snapshot Ihres Volumes zur Wiederherstellung von Daten verwendet werden.

Wenn Sie ONTAP 9.15.1 oder eine frühere Version verwenden, siehe "Daten nach einem Ransomware-Angriff mit ARP wiederherstellen".

Über diese Aufgabe

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

- **Wiederherstellung aus dem aktuellsten ARP/AI Snapshot**: Der aktuellste verfügbare ARP/AI-Snapshot kann verwendet werden, sofern dessen Integrität sichergestellt ist.
- **Wiederherstellung aus einem früheren Snapshot**: Die Sperre des zuletzt gespeicherten ARP/AI-Snapshots wird aufgehoben und anschließend ein älterer Snapshot wiederhergestellt.
- **Wiederherstellung, wenn kein Angriff gemeldet wird**: Zuerst wird aus dem aktuellsten ARP/AI Snapshot wiederhergestellt, anschließend erfolgt eine Wiederherstellung aus dem gewünschten Snapshot.

ARP/AI erstellt Snapshots mit einem der folgenden vorangestellten Namen:

- `Anti_ransomware_periodic_backup`: Wird in ONTAP 9.17.1 und später für Snapshots verwendet, die in regelmäßigen 4-Stunden-Intervallen erstellt werden. Zum Beispiel, `Anti_ransomware_periodic_backup.2025-06-01_1248`.
- `Anti_ransomware_attack_backup`: Wird in ONTAP 9.17.1 und später für Snapshots verwendet, die als Reaktion auf Abnormalitäten erstellt werden. Diese Snapshots haben eine Standardaufbewahrungsdauer von 10 Tagen. Zum Beispiel, `Anti_ransomware_attack_backup.2025-08-25_1248`.
- `Anti_ransomware_backup`: Wurde in ONTAP 9.16.1 und früher für Snapshots verwendet, die als Reaktion auf Anomalien erstellt wurden. Zum Beispiel `Anti_ransomware_backup.2022-12-20_1248`.

Bevor Sie beginnen

- Wenn Sie auf eine Warnung wegen ungewöhnlicher Aktivitäten reagieren, "Sie müssen es zunächst als potenziellen Ransomware-Angriff einstufen" bevor Sie mit der Datenwiederherstellung fortfahren.
- Wählen Sie eine Wiederherstellungsmethode und überprüfen Sie Wiederherstellungsbeschränkungen bevor der Wiederherstellungsvorgang abgeschlossen wird.
- Ab ONTAP 9.20.1 werden keine ARP/AI-Snapshots erstellt, und die Wiederherstellung von ARP/AI-Snapshots ist nicht verfügbar, wenn die ARP/AI-Snapshot-Antwortrichtlinie auf `alert-only` gesetzt ist. Zur Wiederherstellung von Daten kann ein geplanter ONTAP Snapshot oder eine eigene Backup-Lösung verwendet werden.

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/AI oder geplant) zurück. Dies ist die schnellste Methode, entfernt jedoch alle Snapshots,

die nach dem Wiederherstellungspunkt erstellt wurden.

- **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

- Für ONTAP 9.16.1 und höher: Das verdächtige Ereignis **zuerst** (in "Auf abnormale Aktivität reagieren") löschen und anschließend die Wiederherstellung durchführen. Nach dem Löschen werden ARP/AI Snapshots entsprechend der Kategorisierung der Aktivität beibehalten. Ab ONTAP 9.17.1 gelten als Standard 7 Tage (echter Angriff) oder 24 Stunden (falsch positiv). In ONTAP 9.16.1 gelten als Standard 5 Tage (echter Angriff) oder 48 Stunden (falsch positiv). Die Option clear-suspect ist nach einer Volume Restore nicht mehr verfügbar, daher muss das Ereignis vor der Wiederherstellung gelöscht werden.
- Das Freigeben der ARP/AI 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.
- Bei SAN-Volumes, bei denen der Angriff ausschließlich durch eine Entropieanalyse erkannt wird, werden nur der unmittelbar vor dem Angriffszeitpunkt erstellte Snapshot und der Angriffssnapshot für einen längeren Zeitraum (standardmäßig 10 Tage, konfigurierbar) aufbewahrt. Andere periodische Snapshots unterliegen weiterhin den normalen Aufbewahrungsregeln. Dies unterscheidet sich von NAS-Volumes, bei denen alle vor dem Angriffszeitpunkt erstellten Snapshots so lange aufbewahrt werden, bis der Administrator eine Aktion zur Beseitigung des Verdachts durchführt.
- Für ONTAP 9.20.1 und höher: Durch die Wiederherstellung eines Volume-Snapshots kann die ARP/AI-Snapshot-Antwortrichtlinie des Volumes auf die Richtlinie zurückgesetzt werden, die zum Zeitpunkt der Snapshot-Erstellung gültig war. Nach der Wiederherstellung eines Volumes sollte überprüft werden, ob die Snapshot-Antwortrichtlinie noch korrekt ist.

```
security anti-ransomware volume snapshot-settings show -vserver
<svm_name> -volume <volume_name>
```

SnapMirror Überlegungen

- Wenn das Volume Teil einer SnapMirror synchron oder SnapMirror active sync SAN-Beziehung in ONTAP 9.19.1 ist und eine Wiederherstellung auf Volume-Ebene geplant ist, sollte das Volume in den Quiesce-Modus "Die Beziehung vor der Wiederherstellung aufheben" versetzt und der Schutz nach der

Wiederherstellung wiederhergestellt werden.

- Wenn ein ARP/AI-geschütztes Volume aus einem Snapshot wiederhergestellt wird, während es an einer SnapMirror Beziehung beteiligt ist, sollten alle Spiegelkopien nach der Wiederherstellung manuell aktualisiert werden. Andernfalls können Spiegelkopien unbrauchbar werden und müssen möglicherweise gelöscht und neu erstellt werden.

Für das vollständige SnapMirror und ARP/AI Interoperabilitätsverhalten siehe "SnapMirror und ARP/AI Interoperabilität".

Wiederherstellung nach einem Systemangriff

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

- Wiederherstellung aus dem aktuellsten ARP/AI Snapshot
- Wiederherstellung aus einem früheren Snapshot
- Wiederherstellung, wenn kein Angriff erkannt wird

Wiederherstellung aus dem aktuellsten ARP/AI Snapshot

Dieser Ablauf eignet sich, wenn die Wiederherstellung sicher vom aktuellsten ARP/AI-Snapshot erfolgen kann, da dies der aktuellste für die Wiederherstellung verfügbare Snapshot ist.

System Manager

1. Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies**.
2. Bevor Sie eine Volume-Wiederherstellung durchführen, "Verdächtige Dateien löschen".

   Nachdem Sie verdächtige Dateien gelöscht haben, wird der ARP/AI Snapshot standardmäßig 7 Tage lang aufbewahrt. Wenn mehr Zeit für die Datenwiederherstellung benötigt wird, "ARP/AI Snapshot-Einstellungen anpassen" kann die Aufbewahrungsdauer verlängert werden. Nachdem die Datenwiederherstellung abgeschlossen ist, kann die Aufbewahrungsdauer wieder verkürzt werden.

3. Wählen Sie ⋮ neben dem zuletzt verfügbaren ARP/AI Snapshot (`Anti_ransomware` den gewünschten Snapshot aus, der wiederhergestellt werden soll, und wählen Sie anschließend **Wiederherstellen**.

CLI

1. Snapshots in einem Volume auflisten:

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

2. Bevor Sie `volume snapshot restore`, "Verdächtige Dateien löschen" ausführen.
3. Den Inhalt eines Volumes aus einem Snapshot wiederherstellen:

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

```
<snapshot>
```

Wiederherstellung aus einem früheren Snapshot

Diesen Ablauf wählen, wenn eine Wiederherstellung aus einem früheren Snapshot erfolgen soll. Vor der Wiederherstellung aus dem früheren Snapshot ist die Sperre des aktuellsten ARP/AI-Snapshots aufzuheben.

System Manager

1. Die Sperre für den aktuellsten ARP/AI 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:

```
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 erkannt wird, erfolgt zunächst die Wiederherstellung aus dem aktuellsten ARP/AI-Snapshot und anschließend aus einem früheren Snapshot.

System Manager

1. Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies**.
2. Wählen Sie ⋮ und wählen Sie dann den aktuellsten `Anti_ransomware` 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 aus dem aktuellsten ARP/AI 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".

Konfiguration von ONTAP ARP/AI Snapshot-Antwortrichtlinien und -Einstellungen

Ab ONTAP 9.16.1 können Sie die CLI verwenden, um die Erstellungs- und Aufbewahrungseinstellungen für Autonomous Ransomware Protection with AI (ARP/AI) Snapshots zu steuern. Ab ONTAP 9.20.1 können Sie außerdem die Snapshot-Reaktionsrichtlinie für periodische und Angriffs-Snapshots konfigurieren, um festzulegen, ob ARP/AI Snapshots erstellt, wenn ungewöhnliche Aktivitäten erkannt werden.

Wenn Sie ONTAP 9.15.1 oder eine frühere Version verwenden, siehe "Einstellungen für automatisch generierte ARP Snapshots anpassen".

Konfiguration einer Snapshot-Antwortrichtlinie

Ab ONTAP 9.20.1 können Sie die ARP/AI Snapshot-Antwortrichtlinie für periodische und Angriffs-Snapshots konfigurieren, um zu steuern, ob ARP/AI Snapshots erstellt, wenn anormale Aktivitäten erkannt werden. Sie können die Richtlinie auf SVM Level festlegen, wobei alle Volumes auf der SVM die Einstellung übernehmen, oder sie auf Volume Level überschreiben.

Die folgenden Snapshot-Antwortrichtlinien stehen zur Verfügung:

Richtlinie	Verhalten
`alert-with-proactive-and-periodic-snapshot`	(Standard) ARP/AI generiert Warnmeldungen und Ereignisprotokolle, erstellt in regelmäßigen Abständen Snapshots und erstellt zusätzliche Snapshots, wenn ein Angriff erkannt wird.
`alert-with-proactive-snapshot`	ARP/AI generiert Warnmeldungen und Ereignisprotokolle und erstellt Snapshots nur dann, wenn ein Angriff erkannt wird. Es werden keine regelmäßigen Snapshots erstellt.
`alert-only`	ARP/AI generiert ausschließlich Warnmeldungen und Ereignisprotokolle. ARP/AI erstellt keine Snapshots.

Wenn Sie die Richtlinie auf `alert-only` setzen, erstellt ARP/AI keine Snapshots. Wenn ein Ransomware-Angriff bestätigt wird, stehen auch während eines aktiven Angriffs keine ARP/AI-Snapshots für die Datenwiederherstellung zur Verfügung. Vor der Verwendung von `alert-only` muss ein ausreichender externer Datenschutz vorhanden sein, z. B. durch geplante ONTAP Snapshots, SnapCenter Backups oder eine andere Backup-Lösung.

Wenn Sie die Snapshot-Antwortrichtlinie ändern, werden vorhandene ARP/AI-Snapshots nicht sofort gelöscht. Sie werden gelöscht, sobald ihre geplante Ablaufzeit erreicht ist. Nach einer Richtlinienänderung ist keine sofortige Freigabe von Storage-Kapazität zu erwarten.

System Manager

Konfiguration der Snapshot-Antwortrichtlinie auf SVM Level:

1. Die Auswahl der Storage VM erfolgt unter **Cluster** > **Storage VMs**.
2. Zur Registerkarte **Settings** wechseln. Unter **Security** die Kachel **Anti-ransomware** suchen und auswählen.
3. Unter **Schutzstufe** wird der Schutztyp ausgewählt, der auf alle ARP/AI-fähigen Volumes auf der SVM angewendet werden soll.
4. **Speichern** auswählen.

Die Snapshot-Antwortrichtlinie wird auf Volume-Ebene konfiguriert:

1. **Storage** > **Volumes** auswählen und das Volume auswählen.
2. Auf der Registerkarte **Sicherheit** ist im Abschnitt **Anti-Ransomware** auszuwählen.
3. Unter **Schutzstufe** erfolgt die Auswahl der Snapshot-Antwortrichtlinie, die die SVM-Einstellung für dieses Volume überschreibt.
4. **Speichern** auswählen.

CLI

1. Anzeige der aktuellen ARP/AI-Snapshot-Antwortrichtlinie:

   Auf SVM-Ebene:

   ```
   security anti-ransomware vserver snapshot-settings show -vserver
   <svm_name>
   ```

   Auf Volume-Level:

   ```
   security anti-ransomware volume snapshot-settings show -vserver
   <svm_name> -volume <volume_name>
   ```

2. Konfigurieren der ARP/AI-Snapshot-Antwortrichtlinie:

   Auf SVM-Ebene:

   ```
   security anti-ransomware vserver snapshot-settings modify -vserver
   <svm_name> -anti-ransomware-snapshot-policy <policy>
   ```

   Diese Einstellung gilt für Volumes, auf denen ARP/AI aktiviert ist. Sie hat keine rückwirkenden Auswirkungen auf bereits vorhandene Volumes mit aktiviertem ARP/AI.

   Auf Volume-Ebene (überschreibt die SVM-Einstellung):

   ```
   security anti-ransomware volume snapshot-settings modify -vserver
   <svm_name> -volume <volume_name> -anti-ransomware-snapshot-policy
   <policy>
   ```

Anpassung der Einstellungen für die Erstellung und Aufbewahrung von Snapshots

> Ab ONTAP 9.20.1 gelten die folgenden Einstellungen nur, wenn die Snapshot-Antwortrichtlinie `alert-with-proactive-snapshot` oder `alert-with-proactive-and-periodic-snapshot` ist.

Bevor Sie beginnen

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

Schritte

1. Alle aktuellen ARP/AI Snapshot-Einstellungen anzeigen:

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

2. Ausgewählte aktuelle ARP/AI Snapshot-Einstellungen:

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

3. ARP/AI Snapshot-Einstellungen ändern:

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

Die folgenden Einstellungen lassen sich ändern (ONTAP 9.16.1 und höher):

Einstellung	Beschreibung	Unterstützte Versionen mit ARP/AI
`arw.snap.max.count`	Legt die maximale Anzahl von ARP/AI-Snapshots fest, die zu einem bestimmten Zeitpunkt in einem Volume vorhanden sein können. Ältere Kopien werden gelöscht, um sicherzustellen, dass die Gesamtzahl der ARP/AI-Snapshots innerhalb dieses Grenzwerts bleibt. Ab ONTAP 9.20.1 gilt diese Einstellung nur, wenn die Snapshot-Antwortrichtlinie auf `alert-with-proactive-and-periodic-snapshot` gesetzt ist. Wenn die Richtlinie auf `alert-with-proactive-snapshot` oder `alert-only` gesetzt ist, ignoriert ONTAP diese Einstellung.	ONTAP 9.16.1 und höher
`arw.snap.create.interval.hours`	Gibt das Intervall *in Stunden* zwischen ARP/AI Snapshots an. Ein neuer ARP/AI Snapshot wird erstellt, wenn ein datenentropiebasierter Angriff vermutet wird und der zuletzt erstellte Snapshot älter als das angegebene Intervall ist.	ONTAP 9.16.1 und höher

Einstellung	Beschreibung	Unterstützte Versionen mit ARP/AI
`arw.snap.normal.retain.interval.hours`	Gibt die Dauer *in Stunden* an, für die ein ARP/AI Snapshot aufbewahrt wird. Wenn ein ARP/AI Snapshot den Aufbewahrungsschwellenwert erreicht, wird er gelöscht.	ONTAP 9.16.1 (deprecated in 9.17.1 und höher)
`arw.snap.max.retain.interval.days`	Gibt die maximale Aufbewahrungsdauer *in Tagen* eines ARP/AI-Snapshots an. Alle ARP/AI-Snapshots, die älter als diese Dauer sind, werden gelöscht, wenn kein Angriff auf das Volume gemeldet wird. Das maximale Aufbewahrungsintervall wird ignoriert, wenn ARP/AI eine Bedrohung erkennt. Der als Reaktion auf die Bedrohung erstellte ARP/AI-Snapshot wird so lange aufbewahrt, bis Sie auf die Bedrohung reagieren. Wenn Sie eine Bedrohung als Fehlalarm markieren, wird der durch `arw.snap.retain.hours.after.clear.suspect.false.alert` festgelegte Aufbewahrungstimer auf die ARP/AI-Snapshots angewendet. Nach Ablauf dieses Timers gelten wieder die Standardeinstellungen für die Aufbewahrung.	ONTAP 9.16.1 (deprecated in 9.17.1 und höher)
`arw.snap.create.interval.hours.post.max.count`	Legt das Intervall *in Stunden* zwischen ARP/AI-Snapshots fest, wenn das Volume bereits die maximale Anzahl an ARP/AI-Snapshots enthält. Wenn die maximale Anzahl erreicht ist, wird ein ARP/AI-Snapshot gelöscht, um Platz für eine neue Kopie zu schaffen. Mit dieser Option lässt sich die Erstellungsgeschwindigkeit reduzieren, sodass ältere Kopien erhalten bleiben.	ONTAP 9.16.1 (deprecated in 9.17.1 und höher)
`arw.snap.new.extns.interval.hours`	Gibt das Intervall *in Stunden* zwischen ARP/AI-Snapshots an, die erstellt werden, wenn eine neue Dateierweiterung erkannt wird. Ein neuer ARP/AI-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 angibt.	ONTAP 9.16.1 (deprecated in 9.17.1 und höher)
`arw.snap.low.encryption.retain.duration.hours`	Legt die Aufbewahrungsdauer *in Stunden* für ARP/AI Snapshots fest, die während Perioden geringer Verschlüsselungsaktivität erstellt wurden.	ONTAP 9.17.1 und höher
`arw.snap.retain.hours.after.clear.suspect.false.alert`	Gibt das Intervall *in Stunden* an, in dem ein ARP/AI-Snapshot vorsorglich aufbewahrt wird, nachdem ein Angriffsereignis vom Administrator als Fehlalarm markiert wurde.	ONTAP 9.16.1 und höher

Einstellung	Beschreibung	Unterstützte Versionen mit ARP/AI
`arw.snap.retain.hours.after.clear.suspect.real.attack`	Gibt das Intervall *in Stunden* an, in dem ein ARP/AI-Snapshot vorsorglich aufbewahrt wird, nachdem ein Angriffsereignis vom Administrator als echter Angriff markiert wurde.	ONTAP 9.16.1 und höher
`arw.snap.surge.interval.days`	Legt das Intervall *in Tagen* zwischen ARP/AI-Snapshots fest, die als Reaktion auf IO-Spitzen erstellt werden. Diese Option legt außerdem die Aufbewahrungsdauer *in Tagen* für einen ARP/AI-Surge-Snapshot fest.	ONTAP 9.16.1 und höher
`arw.high.encryption.alert.enabled`	Aktiviert Warnmeldungen bei hohem Verschlüsselungsgrad. Wenn auf `on` (Standardeinstellung) gesetzt, sendet ONTAP eine Warnmeldung, wenn der Prozentsatz der Verschlüsselung den in `arw.high.encryption.percentage.threshold` angegebenen Schwellenwert überschreitet.	Nur ONTAP 9.17.1
`arw.high.encryption.percentage.threshold`	Legt den maximalen Prozentsatz der Verschlüsselung für ein Volume fest. Wenn der Prozentsatz der Verschlüsselung diesen Schwellenwert überschreitet, behandelt ONTAP die Erhöhung als Angriff und erstellt einen ARP/AI-Snapshot. `arw.high.encryption.alert.enabled` muss auf `on` gesetzt werden, damit diese Option wirksam wird.	Nur ONTAP 9.17.1
`arw.snap.high.encryption.retain.duration.hours`	Gibt das Aufbewahrungsintervall *in Stunden* für Snapshots an, die während eines Ereignisses mit hohem Verschlüsselungsschwellenwert erstellt wurden.	ONTAP 9.17.1 und höher

4. Wenn Sie ARP/AI in einer SAN-Umgebung verwenden, können Sie auch die folgenden Einstellungen für den Evaluierungszeitraum ändern:

Einstellung	Beschreibung	Unterstützte Versionen
`arw.block_device.auto.learn.threshold.min_value`	Legt den minimalen Verschlüsselungsschwellenwert in Prozent während der automatischen Lernphase der Evaluierung für Blockgeräte fest.	ONTAP 9.17.1 und höher
`arw.block_device.auto.learn.threshold.max_value`	Legt den maximalen Verschlüsselungsschwellenwert in Prozent während der automatischen Lernphase der Evaluierung für Blockgeräte fest.	ONTAP 9.17.1 und höher
`arw.block_device.evaluation.phase.min_hours`	Gibt das Mindestintervall *in Stunden* an, das die Auswertungsphase durchlaufen muss, bevor der Verschlüsselungsschwellenwert festgelegt wird.	ONTAP 9.17.1 und höher
`arw.block_device.evaluation.phase.max_hours`	Gibt das maximale Intervall *in Stunden* an, das die Auswertungsphase durchlaufen muss, bevor der Verschlüsselungsschwellenwert festgelegt wird.	ONTAP 9.17.1 und höher

Einstellung	Beschreibung	Unterstützte Versionen
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	Gibt die Mindestmenge an Daten *in GB* an, die während der Auswertungsphase erfasst werden muss, bevor der Verschlüsselungsschwellenwert festgelegt wird.	ONTAP 9.17.1 und höher
`arw.block_device.evaluation.phase.alert.enabled`	Gibt an, ob Warnmeldungen für die Auswertungsphase von ARP/AI auf Blockgeräten aktiviert sind. Standardwert ist `True`.	ONTAP 9.17.1 und höher
`arw.block_device.evaluation.phase.alert.threshold`	Legt den Schwellenwert in Prozent während der Auswertungsphase von ARP/AI auf Blockgeräten fest. Wenn der Prozentsatz der Verschlüsselung diesen Schwellenwert überschreitet, wird eine Warnung ausgelöst.	ONTAP 9.17.1 und höher

Verwandte Informationen

- "Bedrohungsanalyse und ARP/AI Snapshots"
- "ARP/AI Entropieauswertungszeitraum für SAN Volumes"
- "Daten nach einem Ransomware-Angriff mit ARP/AI wiederherstellen"

Aktualisierung von ONTAP Autonomous Ransomware Protection with AI

Um den Schutz vor den neuesten Ransomware-Bedrohungen auf dem neuesten Stand zu halten, bietet ARP/AI automatische Updates, die außerhalb der regulären ONTAP Releasezyklen erfolgen.

Ab ONTAP 9.16.1 sind Sicherheitsupdates für ARP/AI zusätzlich zu System- und Firmware-Updates auch in den Software-Downloads des System Manager verfügbar. Wenn Ihr ONTAP Cluster bereits in "automatische System- und Firmware-Updates" registriert ist, erfolgt eine automatische Benachrichtigung, sobald ARP/AI-Sicherheitsupdates verfügbar sind. Es besteht außerdem die Möglichkeit, Ihre Aktualisierungseinstellungen so zu ändern, dass ONTAP Sicherheitsupdates automatisch installiert.

ARP (ONTAP 9.10.1 bis 9.15.1) unterstützt keine automatischen Aktualisierungen des Sicherheitsmodells. Die Sicherheitserkennungsfunktionen werden nur mit ONTAP Software-Upgrades aktualisiert. Bei Verwendung von ONTAP 9.15.1 oder einer früheren Version siehe "Informationen zum autonomen Ransomware-Schutz".

Wenn Sie ARP/AI manuell aktualisieren möchten, können Updates von der NetApp Support Site heruntergeladen und mit System Manager installiert werden.

Über diese Aufgabe

ARP/AI kann ausschließlich mit dem System Manager aktualisiert werden.

Eine Aktualisierungseinstellung für ARP/AI auswählen

Im System Manager sind die Einstellungen auf der Seite „Automatische Updates für Sicherheitsdateien aktivieren“ auf `Show notifications` gesetzt, wenn Sie bereits für automatische Firmware- und

Systemupdates registriert sind. Die Update-Einstellungen können auf `Automatically update` geändert werden, wenn ONTAP die neuesten Updates automatisch anwenden soll. Wenn Sie eine Dark-Site-Umgebung nutzen oder Updates lieber manuell durchführen, besteht die Möglichkeit, Benachrichtigungen anzuzeigen oder Sicherheitsupdates automatisch zu verwerfen.

Bevor Sie beginnen

Für automatische Sicherheitsupdates, "AutoSupport und AutoSupport OnDemand sollten aktiviert sein und das Transportprotokoll sollte auf HTTPS eingestellt sein.".

Schritte

1. Im System Manager unter **Cluster > Einstellungen > Software updates** navigieren.
2. Im Abschnitt **Software updates** → auswählen.
3. Auf der Seite **Software updates** die Registerkarte **All other updates** auswählen.
4. Die Registerkarte **Alle anderen Updates** auswählen und auf **Mehr** klicken.
5. **Einstellungen für automatische Updates bearbeiten** auswählen.
6. Auf der Seite „Einstellungen für automatische Updates“ die Option „Sicherheitsdateien“ auswählen.
7. Die auszuführende Aktion für Sicherheitsdateien (ARP/AI-Aktualisierungen) angeben.

   Es besteht die Möglichkeit, Aktualisierungen automatisch durchzuführen, Benachrichtigungen anzuzeigen oder Aktualisierungen automatisch zu verwerfen.

   ⓘ Damit Sicherheitsupdates automatisch installiert werden, sollten AutoSupport und AutoSupport OnDemand aktiviert sein und das Transportprotokoll sollte auf HTTPS eingestellt sein.

8. Die Allgemeinen Geschäftsbedingungen akzeptieren und **Speichern** auswählen.

ARP/AI manuell mit dem neuesten Sicherheitspaket aktualisieren

Das entsprechende Verfahren hängt davon ab, ob Sie bei Active IQ Unified Manager registriert sind.

ⓘ Es sollte nur ein neueres ARP/AI Update als die aktuelle Version installiert werden, um unbeabsichtigte ARP/AI Downgrades zu vermeiden.

ONTAP 9.16.1 und höher mit Digital Advisor

1. Im System Manager zur **Dashboard** wechseln.

   Im Abschnitt **Integrität** wird eine Meldung angezeigt, falls empfohlene Sicherheitsupdates für den Cluster verfügbar sind.

2. Klicken Sie auf die Warnmeldung.
3. Neben den Sicherheitsupdates in der Liste der empfohlenen Updates die Option **Aktionen** auswählen.
4. **Aktualisieren** installiert das Update sofort, **Planen** legt die Installation für einen späteren Zeitpunkt fest.

   Wenn das Update bereits geplant ist, besteht die Möglichkeit, es **zu bearbeiten** oder **zu stornieren**.

ONTAP 9.16.1 und höher ohne Digital Advisor

1. Navigieren Sie zu "NetApp Support Site" und melden Sie sich an.
2. Füllen Sie die Eingabeaufforderungen aus und laden Sie das Sicherheitspaket herunter, das Sie zur Aktualisierung Ihres Cluster-ARP/AI verwenden möchten.
3. Die Dateien werden auf einen HTTP- oder FTP-Server im Netzwerk oder in einen lokalen Ordner kopiert, auf den der Cluster mit ARP/AI zugreifen kann.
4. Im System Manager unter **Cluster > Einstellungen > Software updates** navigieren.
5. In **Softwareaktualisierungen** die Registerkarte **Alle anderen Aktualisierungen** auswählen.
6. Im Bereich **Manuelle Aktualisierungen** auf **Sicherheitsdateien hinzufügen** klicken und die Dateien mit einer der folgenden Einstellungen hinzufügen:
   - **Vom Server herunterladen**: Geben Sie die URL für das Sicherheitsdateipaket ein.
   - **Hochladen vom lokalen Client**: Zur heruntergeladenen TGZ-Datei navigieren.

   > Stellen Sie sicher, dass der Dateiname mit `ontap_security_file_arpai_` beginnt und `.tgz` als Dateiendung hat.

7. **Hinzufügen** auswählen, um die Aktualisierungen anzuwenden.

ARP/AI-Updates überprüfen

Der Verlauf der automatischen Updates, die verworfen wurden oder deren Installation fehlgeschlagen ist, kann wie folgt angezeigt werden:

1. Im System Manager unter **Cluster > Einstellungen > Software updates** navigieren.
2. Im Abschnitt **Software updates** → auswählen.
3. Auf der Seite **Software updates** die Registerkarte **All other updates** auswählen und auf **More** klicken.
4. **Alle automatischen Updates anzeigen** auswählen.

Verwandte Informationen

- "Informationen zu ARP/KI"
- "E-Mail-Abonnements für Softwareupdates"

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.