Autonomer Schutz Durch Ransomware

ONTAP 9

NetApp
February 12, 2026

Inhalt

Autonomer Schutz Durch Ransomware

Informieren Sie sich über den autonomen Ransomware-Schutz von ONTAP

Ab ONTAP 9.10.1 können ONTAP -Administratoren Autonomous Ransomware Protection (ARP) aktivieren, um Workload-Analysen in NAS-Umgebungen (NFS und SMB) durchzuführen und so proaktiv ungewöhnliche Aktivitäten zu erkennen und davor zu warnen, die auf einen Ransomware-Angriff hindeuten könnten. Ab ONTAP 9.17.1 unterstützt ARP auch Blockgeräte-Volumes, einschließlich SAN-Volumes mit LUNs oder NVMe-Namespaces oder NAS-Volumes mit virtuellen Festplatten von Hypervisoren wie VMware.

ARP ist direkt in ONTAP integriert und gewährleistet die integrierte Steuerung und Koordination mit den anderen Funktionen von ONTAP. ARP arbeitet in Echtzeit, verarbeitet Daten beim Schreiben oder Lesen in das Dateisystem und erkennt und reagiert schnell auf potenzielle Ransomware-Angriffe.

ARP erstellt zur zusätzlichen Absicherung in regelmäßigen Abständen gesperrte Snapshots zusätzlich zu den geplanten Snapshots. Es verwaltet intelligent, wie lange Momentaufnahmen aufbewahrt werden. Wenn keine ungewöhnliche Aktivität festgestellt wird, werden die Snapshots schnell wiederverwendet. Wird jedoch ein Angriff erkannt, wird eine vor Beginn des Angriffs erstellte Momentaufnahme für einen längeren Zeitraum aufbewahrt. Weitere Informationen, einschließlich der durch die ONTAP Version hinzugefügten Änderungen, finden Sie unter ARP-SchnappschüsseDie

Lizenzen und Enablement

Sie benötigen eine Lizenz zur Nutzung von ARP. Entscheiden Sie, ob ARP standardmäßig auf neuen Volumes aktiviert oder manuell pro Volume aktiviert werden soll.

Lizenzoptionen für ARP

ARP-Unterstützung ist im Lieferumfang enthalten."ONTAP One-Lizenz" Die Wenn Sie nicht über die ONTAP One-Lizenz verfügen, stehen Ihnen für die ARP-Nutzung andere Lizenzen zur Verfügung, die sich je nach Ihrer ONTAP-Version unterscheiden

ONTAP-Versionen	Lizenz
ONTAP 9.11.1 und höher	`Anti_ransomware`
ONTAP 9.10.1	`MT_EK_MGMT` (Multi-Tenant-Schlüsselverwaltung)

- Wenn Sie von ONTAP 9.10.1 auf ONTAP 9.11.1 oder höher aktualisieren und ARP bereits auf Ihrem System konfiguriert ist, müssen Sie die neue `Anti-ransomware` Lizenz. Für neue ARP-Konfigurationen ist die neue Lizenz erforderlich.
- Wenn Sie von ONTAP 9.11.1 oder höher auf ONTAP 9.10.1 zurückkehren und ARP mit der Anti_ransomware-Lizenz aktiviert haben, wird eine Warnmeldung angezeigt und Sie müssen ARP möglicherweise neu konfigurieren. "Erfahren Sie mehr über das Zurücksetzen von ARP" .

Aktivierungsoptionen für ARP

ARP bietet flexible Aktivierungsoptionen auf Cluster-, SVM- und Volume-Ebene, sodass Sie die automatische Standardaktivierung für neue Volumes konfigurieren oder ARP bei Bedarf manuell auf bestehenden Volumes aktivieren können.

Automatische Standardaktivierung auf neuen Volumes

Ab ONTAP 9.18.1 ist ARP auf allen neuen Volumes der AFF A-Serie und AFF C-Serie, ASA und ASA r2-Systemen standardmäßig automatisch aktiviert. Diese automatische Standard-ARP-Aktivierung gilt nicht für "Nicht unterstützte Volumes oder Konfigurationen".

Die standardmäßige ARP-Aktivierung auf neuen Volumes tritt nach einer 12-stündigen Übergangsfrist nach einem Upgrade oder sofort bei einer neuen ONTAP 9.18.1-Installation in Kraft, sofern in beiden Fällen eine ARP-Lizenz installiert ist. Sie müssen ARP manuell aktivieren auf bestehenden Volumes durchführen.

Während der Testphase können Sie "Deaktivieren Sie die standardmäßige Aktivierung für neue Volumes auf Clusterebene mithilfe von System Manager oder der ONTAP CLI". Wenn Sie nicht widersprechen, wird ARP nach Ablauf der Testphase automatisch für alle neuen Volumes aktiviert. Sollten sich Ihre Anforderungen nach der Testphase ändern, können Sie die Standardaktivierung jederzeit aktivieren oder deaktivieren.

Manuelle Standardaktivierung auf neuen Volumes

Wenn Sie die automatische Standardaktivierung von ARP auf Clusterebene deaktiviert haben, können Sie sich auch dafür entscheiden, "ARP standardmäßig auf allen neuen Volumes manuell aktivieren" auf SVM-Ebene vorzugehen. Für ONTAP 9.17.1 und frühere Versionen ist dies die einzige Möglichkeit, ARP so zu konfigurieren, dass es auf neuen Volumes standardmäßig aktiviert ist.

ARP-Aktivierung auf allen oder bestimmten vorhandenen Volumes

Ab Version 9.18.1 können Sie ARP manuell auf allen vorhandenen Volumes auf Clusterebene aktivieren (wählen Sie **Cluster > Sicherheit** und ⋮ im Abschnitt **Anti-ransomware** dann **Auf allen vorhandenen Volumes aktivieren**).

Falls Sie die ARP-Aktivierung auf ein bestimmtes Volume beschränken möchten, können Sie "ARP auf Basis einzelner Volumes aktivieren".

ONTAP Strategie zum Schutz der Ransomware

Effektiver Ransomware-Schutz erfordert viele Schutzebenen, die zusammenarbeiten.

Während ONTAP Funktionen wie FPolicy, Snapshots, SnapLock und Active IQ Digital Advisor (auch bekannt als Digital Advisor) zum Schutz vor Ransomware bietet, stellt ARP eine zusätzliche Verteidigungsebene dar.

Weitere Informationen zu anderen Funktionen im NetApp Portfolio, die vor Ransomware schützen, finden Sie hier:

- "Ransomware und das Datensicherungsportfolio von NetApp"
- "ONTAP Cyber Vault-Härtung mit PowerShell"

Was ARP erkennt

ONTAP ARP schützt vor Denial-of-Service-Angriffen, bei denen der Angreifer Daten zurückhält, bis ein Lösegeld gezahlt wird. ARP bietet Ransomware-Erkennung in Echtzeit basierend auf folgenden Kriterien:

- Identifizierung eingehender Daten als verschlüsselt oder im Klartext.

- Analysen, die Folgendes erkennen:
  - **Entropie**: (Wird in NAS und SAN verwendet) Eine Bewertung der Zufälligkeit von Daten in einer Datei
  - **Dateierweiterungstypen**: (Nur in NAS verwendet) Eine Dateierweiterung, die nicht den erwarteten Erweiterungstypen entspricht
  - **Datei-IOPS**: (Wird in NAS erst ab ONTAP 9.11.1 verwendet) Ein Anstieg der anormalen Volume-Aktivität mit Datenverschlüsselung

ARP erkennt die Ausbreitung der meisten Ransomware-Angriffe, nachdem nur eine kleine Anzahl von Dateien verschlüsselt wurde, reagiert automatisch, um die Daten zu schützen, und warnt Sie, wenn ein mutmaßlicher Angriff stattfindet.

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

Erfahren Sie mehr über ARP-Modi

Nachdem ARP für ein Volume aktiviert wurde, beginnt eine Lernphase, um eine Basislinie festzulegen. ARP analysiert Systemmetriken, um ein Alarmprofil zu entwickeln, bevor in den aktiven Erkennungsmodus gewechselt wird. Im aktiven Modus überwacht ARP abnormale Aktivitäten, ergreift Schutzmaßnahmen und generiert Warnungen, wenn es abnormales Verhalten erkennt.

Bei ARP unterscheiden sich das Verhalten im Lernmodus und im aktiven Modus je nach ONTAP Version, Volume-Typ und Protokoll (NAS oder SAN).

NAS-Umgebungen und Modustypen

Die folgende Tabelle fasst die Unterschiede zwischen ONTAP 9.10.1 und späteren Versionen für NAS-Umgebungen zusammen.

Bei Versionen mit dem älteren ARP-Modell wird eine Lernphase empfohlen, bevor die aktive Überwachung beginnt. Für NAS-Umgebungen, die Folgendes unterstützenARP/AI Es gibt keine Einarbeitungszeit, die aktive Überwachung beginnt sofort.

Modus	Beschreibung	Datenträgertypen und -versionen
Lernen	Bei bestimmten ONTAP Versionen und bestimmten Volume-Typen wird ARP automatisch in den Lernmodus versetzt, wenn Sie ARP aktivieren. Im Lernmodus entwickelt das ONTAP -System ein Alarmprofil basierend auf den Analysebereichen Entropie, Dateierweiterungstypen und Datei-IOPS. Es wird empfohlen, ARP 30 Tage lang im Lernmodus zu belassen. Ab ONTAP 9.13.1 ermittelt ARP automatisch das optimale Lernintervall und automatisiert den Wechsel, der möglicherweise schon vor 30 Tagen erfolgt. Bei Versionen vor ONTAP 9.13.1 können Sie die Umstellung manuell vornehmen. Ab ONTAP 9.16.1 für FlexVol -Volumes gibt es nur noch den aktiven Modus, und der Lernmodus wird bei jedem FlexVol Volume, das auf diese Version oder höher aktualisiert wird, automatisch in den aktiven Modus überführt. Bei ONTAP 9.16.1 bis 9.17.1 werden FlexGroup Volumes noch nicht von ARP/AI unterstützt und verwenden weiterhin das ältere ARP-Modell. Aus diesem Grund wird für diese Versionen mit FlexGroup -Volumes weiterhin eine Einarbeitungszeit empfohlen. Ab ONTAP 9.18.1 gibt es für FlexVol und FlexGroup -Volumes nur noch den aktiven Modus. Alle aktualisierten Volumes werden automatisch in den aktiven Modus geschaltet. "Erfahren Sie mehr über den Wechsel vom Lern- in den Aktivmodus" . Der Befehl `security anti-ransomware volume workload-behavior show` zeigt Dateierweiterungen an, die im Volume erkannt wurden. Wenn Sie diesen Befehl früh im Lernmodus ausführen und er eine genaue Darstellung der Dateitypen zeigt, sollten Sie diese Daten nicht als Grundlage für den Wechsel in den aktiven Modus verwenden, da ONTAP weiterhin andere Metriken sammelt. Erfahren Sie mehr über `security anti-ransomware volume workload-behavior show` in der "ONTAP-Befehlsreferenz".	• FlexVol -Volumes mit ONTAP 9.10.1 bis 9.15.1 • FlexGroup Volumes mit ONTAP 9.13.1 bis ONTAP 9.17.1
Aktiv	Wenn im aktiven Modus eine Dateierweiterung als ungewöhnlich gekennzeichnet wird, sollten Sie die Warnung auswerten. Sie können auf die Warnung reagieren, um Ihre Daten zu schützen, oder sie als falsch positiv markieren. Durch die Markierung einer Warnung als falsch positiv wird das Warnungsprofil aktualisiert. Wenn die Warnung beispielsweise durch eine neue Dateierweiterung ausgelöst wird und Sie sie als falsch positiv markieren, erhalten Sie beim nächsten Auftreten der Dateierweiterung keine Warnung mehr.	Alle unterstützten ONTAP -Versionen und FlexVol und FlexGroup -Volumes

SAN-Umgebungen und Modustypen

SAN-Umgebungen nutzen Evaluierungsphasen (ähnlich den Lernmodi in NAS-Umgebungen), bevor sie automatisch zur aktiven Erkennung wechseln. Die folgende Tabelle fasst die Evaluierungs- und aktiven Modi zusammen.

Modus	Beschreibung	Datenträgertypen und -versionen
Auswertung	Zur Ermittlung des grundlegenden Verschlüsselungsverhaltens wird eine zwei- bis vierwöchige Evaluierungsphase durchgeführt, während ARP/AI während der Evaluierungsphase einen sofortigen aktiven Schutz für SAN-Volumes gewährleistet. Erkennungen und Warnmeldungen können bereits während der Festlegung von Basisschwellenwerten erfolgen. Sie können feststellen, ob der Evaluierungszeitraum abgeschlossen ist, indem Sie den folgenden Befehl ausführen: `security anti-ransomware volume show` Befehl und Überprüfung `Block device detection status` Die "Erfahren Sie mehr über SAN-Volumes und den Entropie-Evaluierungszeitraum" .	• FlexVol -Volumes mit ONTAP 9.17.1 und höher
Aktiv	Nach dem Testzeitraum können Sie feststellen, ob der ARP-SAN-Schutz aktiv ist, indem Sie den Befehl `security anti-ransomware volume show` ausführen und prüfen, ob `Block device detection status. Active_suitable_workload` zeigt an, dass die ausgewertete Entropiemenge erfolgreich überwacht werden kann. ARP passt den adaptiven Schwellenwert automatisch anhand der während der Auswertung überprüften Daten an.	• FlexVol -Volumes mit ONTAP 9.17.1 und höher

Bedrohungsbewertung und ARP-Snapshots

ARP bewertet die Bedrohungswahrscheinlichkeit anhand eingehender Daten, die mit erlernten Analysen verglichen werden. Wenn ARP eine Anomalie erkennt, wird ein Messwert zugewiesen. ARP kann zum Zeitpunkt der Erkennung oder in regelmäßigen Abständen einen Snapshot zuweisen.

ARP-Schwellenwerte

- **Low**: Früheste Erkennung einer Anomalie im Volume (z.B. wird eine neue Dateierweiterung im Volume beobachtet). Diese Erkennungsstufe ist nur in Versionen vor ONTAP 9.16.1 verfügbar, die nicht über ARP/AI verfügen.
  - Ab ONTAP 9.11.1 können Sie "Passen Sie die Erkennungsparameter für ARP an" .
  - In ONTAP 9.10.1 liegt der Schwellenwert für die Eskalation auf moderat bei 100 oder mehr Dateien.
- **Moderat**: Es wird eine hohe Entropie erkannt oder es werden mehrere Dateien mit derselben noch nie dagewesenen Dateierweiterung beobachtet. Dies ist die Basiserkennungsstufe in ONTAP 9.16.1 und höher mit ARP/AI.

Die Bedrohung wird auf mittel eingestuft, nachdem ONTAP einen Analysebericht erstellt hat, der feststellt, ob die Anomalie mit einem Ransomware-Profil übereinstimmt. Bei mittlerer Angriffswahrscheinlichkeit generiert ONTAP eine EMS-Benachrichtigung mit der Aufforderung, die Bedrohung zu bewerten. ONTAP sendet keine Warnungen über geringe Bedrohungen; ab ONTAP 9.14.1 können Sie jedoch "Standard-Alarmeinstellungen ändern". Weitere Informationen finden Sie unter "Reagieren Sie auf ungewöhnliche Aktivitäten" .

Sie können Informationen über moderate Bedrohungen im Abschnitt **Ereignisse** des System Managers oder mit dem Befehl anzeigen `security anti-ransomware volume show`. Ereignisse mit geringen Bedrohungen können auch mit dem Befehl in Versionen vor ONTAP 9.16.1 angezeigt werden `security anti-ransomware volume show`, die nicht über ARP/AI verfügen. Erfahren Sie mehr über `security`

`anti-ransomware volume show` in der "ONTAP-Befehlsreferenz".

ARP-Schnappschüsse

ARP erstellt einen Snapshot, wenn erste Anzeichen eines Angriffs erkannt werden. Anschließend wird eine detaillierte Analyse durchgeführt, um den potenziellen Angriff zu bestätigen oder auszuschließen. Da ARP-Snapshots proaktiv erstellt werden, noch bevor ein Angriff vollständig bestätigt ist, können sie für bestimmte legitime Anwendungen auch in regelmäßigen Abständen generiert werden. Das Vorhandensein dieser Snapshots sollte nicht als Anomalie betrachtet werden. Wenn ein Angriff bestätigt wird, wird die Angriffswahrscheinlichkeit auf `Moderate` und eine Angriffsbenachrichtigung wird generiert.

Ab ONTAP 9.17.1 werden ARP-Snapshots in regelmäßigen Abständen sowohl für NAS- als auch für SAN-Volumes sowie als Reaktion auf erkannte Anomalien generiert. ONTAP stellt dem ARP-Snapshot einen Namen voran, um ihn leicht identifizierbar zu machen.

Ab ONTAP 9.11.1 können Sie die Aufbewahrungseinstellungen ändern. Weitere Informationen finden Sie unter "Ändern Sie die Optionen für Snapshots" .

Die folgende Tabelle fasst die Unterschiede der ARP-Snapshots nach Version zusammen.

Funktion	ONTAP 9.17.1 und höher	ONTAP 9.16.1 und früher
Erstellungstrigger	• Snapshots werden in festen 4-Stunden-Intervallen erstellt, unabhängig von einem bestimmten Auslöser • Bestätigung eines Angriffs Je nach Triggertyp wird ein „periodischer“ oder „Angriffs“-Snapshot erstellt.	• Hohe Entropie wird erkannt • Eine neue Dateierweiterung wurde erkannt (9.15.1 und früher) • Es wurde ein Anstieg der Dateivorgänge erkannt (9.15.1 und früher). Das Intervall zur Snapshot-Erstellung basiert auf dem Triggertyp.
Konvention für vorangestellte Namen	"Anti_ransomware_periodic_backup" "Anti_ransomware_attack_backup"	"Anti_ransomware_backup"
Löschverhalten	Der ARP-Snapshot ist gesperrt und kann vom Administrator nicht gelöscht werden	Der ARP-Snapshot ist gesperrt und kann vom Administrator nicht gelöscht werden
Maximale Snapshot-Anzahl	"Konfigurierbares Limit für sechs Snapshots"	"Konfigurierbares Limit für sechs Snapshots"

Funktion	ONTAP 9.17.1 und höher	ONTAP 9.16.1 und früher
Aufbewahrungsfrist	Snapshots werden normalerweise 12 Stunden lang aufbewahrt. • NAS-Volumes: Wenn ein Angriff durch eine Dateianalyse bestätigt wird, werden vor dem Angriff erstellte Snapshots aufbewahrt, bis der Administrator den Angriff als wahr oder falsch positiv (klar verdächtig) markiert. • SAN-Volume oder VM-Datenspeicher: Wenn ein Angriff durch eine Block-Entropie-Analyse bestätigt wird, werden vor dem Angriff erstellte Snapshots 10 Tage lang aufbewahrt (konfigurierbar).	• Wird anhand der Auslösebedingungen bestimmt (nicht festgelegt) • Vor dem Angriff erstellte Snapshots bleiben erhalten, bis der Administrator den Angriff als wahr oder falsch positiv (eindeutig verdächtig) markiert.
Eindeutig verdächtige Aktion	Administratoren können eine Clear-Suspect-Aktion ausführen, die die Aufbewahrung basierend auf einer Bestätigung festlegt: • 24 Stunden für falsch-positive Retention • 7 Tage für echte positive Retention	Administratoren können eine Clear-Suspect-Aktion ausführen, die die Aufbewahrung basierend auf einer Bestätigung festlegt: • 24 Stunden für falsch-positive Retention • 7 Tage für echte positive Retention Dieses vorsorgliche Aufbewahrungsverhalten gibt es vor ONTAP 9.16.1 nicht.
Ablaufzeit	Für alle Snapshots ist eine Ablaufzeit festgelegt	Keine

Wiederherstellung von Daten im ONTAP nach einem Ransomware-Angriff

ARP basiert auf der bewährten ONTAP Datenschutz- und Disaster-Recovery-Technologie, um auf Ransomware-Angriffe zu reagieren. ARP erstellt gesperrte Snapshots, wenn erste Anzeichen eines Angriffs erkannt werden. Sie müssen zunächst bestätigen, ob es sich um einen echten Angriff oder einen Fehlalarm handelt. Sobald der Angriff bestätigt ist, kann das Volume mithilfe des ARP-Snapshots wiederhergestellt werden.

Gesperrte Snapshots können nicht auf herkömmliche Weise gelöscht werden. Wenn Sie sich jedoch später dazu entschließen, den Angriff als falsch positiv zu markieren, löscht ONTAP die gesperrte Kopie.

Sie können betroffene Dateien aus ausgewählten Snapshots wiederherstellen, anstatt das gesamte Volume zurückzusetzen.

Weitere Informationen zum Reagieren auf einen Angriff und zur Wiederherstellung von Daten finden Sie in den folgenden Themen:

- "Reagieren Sie auf ungewöhnliche Aktivitäten"
- "Daten aus ARP-Snapshots wiederherstellen"
- "Wiederherstellung von ONTAP -Snapshots"
- "Intelligente Ransomware-Recovery"

Schutz zur Verifizierung durch mehrere Administratoren für ARP

Ab ONTAP 9.13.1 wird empfohlen, die Multi-Admin-Verifizierung (MAV) zu aktivieren, sodass für die ARP-Konfiguration (Autonomous Ransomware Protection) mindestens zwei authentifizierte Benutzeradministratoren erforderlich sind. Weitere Informationen finden Sie unter "Aktivieren Sie die Verifizierung durch mehrere Administratoren".

Autonomer Ransomware-Schutz mit künstlicher Intelligenz (ARP/AI)

Ab ONTAP 9.16.1 verbessert ARP die Cyber-Resilienz durch die Einführung eines Machine-Learning-Modells für Anti-Ransomware-Analysen, das sich ständig weiterentwickelnde Formen von Ransomware mit einer Genauigkeit von 99 % in NAS-Umgebungen erkennt. Machine-Learning-Modell von ARP wird vor und nach einem simulierten Ransomware-Angriff anhand eines großen Datensatzes vortrainiert. Dieses ressourcenintensive Training erfolgt außerhalb von ONTAP mithilfe von Open-Source-Datensätzen aus der forensischen Forschung. Kundendaten werden während der gesamten Modellierungspipeline nicht verwendet, und Datenschutzprobleme bestehen nicht. Das aus diesem Training resultierende vortrainierte Modell ist im Lieferumfang von ONTAP enthalten. Dieses Modell ist weder über die ONTAP CLI noch über die ONTAP API zugänglich oder veränderbar.

Sofortiger Übergang zum aktiven Schutz für ARP/AI

Mit ARP/AI gibt es keineLernzeitraum Die ARP/AI ist unmittelbar nach der Installation oder dem Upgrade für die folgenden unterstützten Datenträgertypen aktiv:

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

Bei bestehenden und neuen Volumes, bei denen die ARP-Funktionalität bereits aktiviert ist, wird der ARP/AI-Schutz automatisch aktiviert, nachdem Sie Ihren Cluster auf eine ARP/AI-fähige ONTAP Version aktualisiert haben.

Automatische ARP/AI Updates

Um den Schutz vor den neuesten Ransomware-Bedrohungen auf dem neuesten Stand zu halten, bietet ARP/AI regelmäßige automatische Updates, die außerhalb der regulären ONTAP -Upgrade- und Release-Kalender erfolgen. Wenn Sie "Automatische Updates aktiviert" Dann können Sie auch automatische Sicherheitsupdates für ARP/AI erhalten, nachdem Sie automatische Updates für Sicherheitsdateien ausgewählt haben. Sie können auch wählen, "Nehmen Sie diese Aktualisierungen manuell vor" und steuern Sie, wann die Aktualisierungen erfolgen.

Ab ONTAP 9.16.1 stehen über System Manager zusätzlich zu System- und Firmware-Updates Sicherheitsupdates für ARP/AI zur Verfügung.

"Weitere Informationen zu ARP/AI-Updates"

Unterschiede zwischen ARP/AI und ARP-Modellen auf einen Blick

Funktion	ARP	ARP/AI
ONTAP Versionen	ONTAP 9.10.1-9.15.1	ONTAP 9.16.1 und höher; 9.15.1 (tech preview)

Funktion	ARP	ARP/AI
Nachweismethode	Analysiert Dateiaktivität, Datenentropie und Dateierweiterungstypen	KI-/Maschinelles-Lernmodell, das auf großen forensischen Datensätzen trainiert wurde; analysiert Entropie und Dateiverhalten
Lernperiode	Erfordert einen 30-tägigen Lernmodus für NAS FlexVol volumes (Auto-Switch verfügbar in 9.13.1 und später)	Keine Einarbeitungszeit; sofort nach Aktivierung einsatzbereit
Unterstützung des Volume-Typs	• FlexVol: 9.10.1 und später • FlexGroup: 9.13.1 und später • SAN: Nicht unterstützt	• FlexVol: 9.16.1 und später • FlexGroup: 9.18.1 und später • SAN: 9.17.1 und höher (mit Evaluierungszeitraum)
Snapshot-Erstellung	Ausgelöst durch hohe Entropie, neue Dateierweiterungen oder Dateivorgangsanstiege	Erstellt in festen 4-Stunden-Intervallen und bei Angriffsbestätigung
Snapshot-Aufbewahrung	Wird aufbewahrt, bis der Administrator verdächtige Aktivitäten freigibt	Standardmäßig 12 Stunden; Verlängerung je nach Bestätigung des Angriffs (24 Stunden bei Fehlalarm, 7 Tage bei bestätigtem Angriff)
Aktualisierungen	Logik zur statischen Erkennung (wird nur mit ONTAP-Upgrades aktualisiert)	Automatische Sicherheitsupdates unabhängig von ONTAP-Releases
Bereitstellung	Manuelle Aktivierung pro Volume oder SVM-Level-Standardeinstellung	Manuelle Aktivierung pro Volume oder Standardeinstellung auf SVM-Ebene; standardmäßige Aktivierung auf allen neuen Volumes auf Clusterebene für unterstützte Systeme in 9.18.1 und später
Bewertungszeitraum	Keine Angabe	Erforderlich für SAN-Volumes (2-4 Wochen), um Basisverschlüsselungsschwellenwerte festzulegen

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Anwendungsfälle und Überlegungen zum autonomen Schutz vor ONTAP Ransomware

Autonomous Ransomware Protection (ARP) ist für NAS-Workloads ab ONTAP 9.10.1 und SAN-Workloads ab ONTAP 9.17.1 verfügbar. Bevor Sie ARP bereitstellen, sollten Sie sich über die empfohlenen Verwendungszwecke und unterstützten Konfigurationen sowie

die Leistungsauswirkungen informieren.

Unterstützte und nicht unterstützte Konfigurationen

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

Geeignete Workloads

ARP eignet sich für folgende Arten von Workloads:

- Datenbanken auf NFS- oder SAN-Speicher
- Home Directorys für Windows oder Linux

  In Umgebungen ohne ARP/AI können Benutzer Dateien mit Erweiterungen erstellen, die in der Lernphase nicht erkannt werden. Daher besteht bei dieser Arbeitslast eine größere Wahrscheinlichkeit für Fehlalarme.

- Bilder und Video

  Beispielsweise Gesundheitsdaten und EDA-Daten (Electronic Design Automation)

Ungeeignete Workloads

ARP ist für diese Arten von Workloads nicht geeignet:

- Workloads mit einer hohen Frequenz von Dateierstellungs- oder -löschvorgängen (Hunderttausende von Dateien in wenigen Sekunden, beispielsweise Test-/Entwicklungs-Workloads).
- Die Bedrohungserkennung von ARP basiert auf der Fähigkeit, einen ungewöhnlichen Anstieg von Dateierstellungs-, Umbenennungs- oder Löschvorgängen zu erkennen. Wenn die Anwendung selbst die Ursache der Dateiaktivität ist, lässt sie sich nicht effektiv von Ransomware-Aktivitäten unterscheiden.
- Workloads, bei denen die Anwendung oder der Host Daten verschlüsselt.

  ARP basiert auf der Unterscheidung eingehender Daten als verschlüsselt oder unverschlüsselt. Wenn die Anwendung selbst die Daten verschlüsselt, verringert sich die Wirksamkeit der Funktion. ARP kann jedoch weiterhin basierend auf der Dateiaktivität (Löschen, Überschreiben oder Erstellen bzw. Umbenennen mit einer neuen Dateierweiterung) und dem Dateityp funktionieren.

Unterstützte Konfigurationen

ARP ist für NAS NFS- und SMB FlexVol Volumes ab ONTAP 9.10.1 verfügbar. Ab 9.17.1 ist ARP für SAN FlexVol Volumes für iSCSI, FC und NVMe mit SAN-Speicher verfügbar.

ARP wird für MetroCluster-Konfigurationen ab ONTAP 9.10.1 unterstützt.

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

	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes sind mit dem asynchronen Modus von SnapMirror geschützt	✓	✓	✓	✓	✓	✓	✓		
SVMs gesichert mit asynchronem SnapMirror (SVM Disaster Recovery)	✓	✓	✓	✓	✓	✓	✓		
SVM Datenmobilität (`vserver migrate`)	✓	✓	✓	✓	✓	✓	✓		
FlexGroup Volumina[1]	✓	✓	✓	✓	✓	✓			
Überprüfung durch mehrere Administratoren	✓	✓	✓	✓	✓				
ARP/AI mit automatischen Updates	✓	✓							
ARP/AI-Standardaktivierung[2]	✓								

[1] ONTAP 9.16.1 und 9.17.1 bieten keine ARP/AI-Unterstützung für FlexGroup -Volumes. Nach einem Upgrade

auf diese Versionen funktionieren FlexGroup Volumes, die für ARP aktiviert sind, weiterhin mit dem gleichen ARP-Modell, das vor ARP/AI verwendet wurde. Ab ONTAP 9.18.1 verwenden FlexGroup Volumes das ARP/AI-Modell.

[2] Ab ONTAP 9.18.1 ist das standardmäßige Aktivierungsverhalten von ARP/AI für AFF A-Series und AFF C-Series, ASA und ASA r2 Systeme verfügbar. Dieses Verhalten aktiviert ARP/AI automatisch auf allen neuen Volumes nach einer 12-stündigen Übergangsfrist nach einem Upgrade oder sofort bei neuen ONTAP 9.18.1 Installationen. Sie müssen ARP manuell auf "bestehende Volumes" aktivieren.

SnapMirror und ARP-Interoperabilität

Ab ONTAP 9.12.1 wird ARP auf asynchronen SnapMirror Zielvolumes unterstützt. ARP wird weder von SnapMirror synchronous noch von SnapMirror active sync unterstützt.

Wenn ein SnapMirror -Quellvolume ARP-fähig ist, erhält das SnapMirror Zielvolume automatisch den ARP-Konfigurationsstatus (z. B. `dry-run` oder `enabled`), ARP-Trainingsdaten und ein von ARP erstellter Snapshot des Quellvolumes. Es ist keine explizite Aktivierung erforderlich.

Obwohl das Zielvolume aus schreibgeschützten (RO) Snapshots besteht, erfolgt keine ARP-Verarbeitung seiner Daten. Wenn das SnapMirror Zielvolume jedoch in einen schreibgeschützten (RW) Speicher konvertiert wird, wird ARP auf dem RW-konvertierten Zielvolume automatisch aktiviert. Das Zielvolume benötigt keine zusätzlichen Lernvorgänge außer den bereits auf dem Quellvolume aufgezeichneten.

In ONTAP 9.10.1 und 9.11.1 überträgt SnapMirror den ARP-Konfigurationsstatus, die Trainingsdaten und die Snapshots nicht von den SnapMirror auf die Zielvolumes. Daher muss ARP auf dem Zielvolume nach der Konvertierung in RW explizit im Lernmodus aktiviert werden.

ARP und Virtual Machines

ARP wird mit virtuellen Maschinen (VMs) auf VMware unterstützt. Die ARP-Erkennung verhält sich bei Änderungen innerhalb und außerhalb der VM unterschiedlich. ARP wird nicht für Workloads empfohlen, die eine große Anzahl stark komprimierter Dateien (z. B. 7z und ZIP) oder verschlüsselter Dateien (z. B. kennwortgeschützte PDF-, DOC- oder ZIP-Dateien) innerhalb der VM umfassen.

Änderungen außerhalb der VM

ARP kann Änderungen der Dateierweiterung auf einem NFS-Volume außerhalb der VM erkennen, wenn eine neue Erweiterung in verschlüsseltem Zustand auf das Volume gelangt oder wenn sich eine Dateierweiterung ändert.

Änderungen innerhalb der VM

Wenn ein Ransomware-Angriff Dateien innerhalb der VM ändert, ohne Änderungen außerhalb der VM vorzunehmen, erkennt ARP die Bedrohung, wenn die Standardentropie der VM niedrig ist (z. B. bei TXT-, DOCX- oder MP4-Dateien). Bei ONTAP 9.16.1 und früheren Versionen erstellt ARP in diesem Szenario einen schützenden Snapshot, generiert jedoch keine Bedrohungswarnung, da die Dateierweiterungen außerhalb der VM nicht manipuliert wurden. Ab der SAN-Unterstützung in ONTAP 9.17.1 generiert ARP zusätzlich eine Bedrohungswarnung, wenn es eine Entropieanomalie innerhalb der VM erkennt.

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

Für SAN analysiert ARP Entropiestatistiken auf Volumeebene und löst Erkennungen aus, wenn eine Entropieanomalie gefunden wird.

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

Nicht unterstützte Konfigurationen

ARP wird in ONTAP S3-Umgebungen nicht unterstützt.

ARP unterstützt die folgenden Volume-Konfigurationen nicht:

- FlexGroup -Volumes (in ONTAP 9.10.1 bis 9.12.1).

  Ab ONTAP 9.13.1 bis ONTAP 9.17.1 werden FlexGroup -Volumes unterstützt, sind aber auf das vor ARP/AI verwendete ARP-Modell beschränkt. FlexGroup Volumes werden mit ARP/AI ab ONTAP 9.18.1 unterstützt.

- FlexCache Volumes (ARP wird auf Ursprungs-FlexVol Volumes unterstützt, jedoch nicht auf Cache Volumes)
- Offline-Volumes
- SnapLock Volumes
- SnapMirror Active Sync
- SnapMirror Synchronous
- SnapMirror asynchron (in ONTAP 9.10.1 und 9.11.1). SnapMirror asynchron wird ab ONTAP 9.12.1 unterstützt. Weitere Informationen finden Sie unter [snapmirror] .
- Eingeschränkte Volumes
- Root-Volumes von Storage-VMs
- Volumes von angestoppten Storage VMs

ARP-Performance- und Frequenzüberlegungen

ARP kann die Systemleistung, gemessen am Durchsatz und den maximalen IOPS-Werten, nur minimal beeinträchtigen. Die Auswirkungen der ARP-Funktion hängen von der jeweiligen Volume-Workload ab. Für gängige Workloads werden die folgenden Konfigurationsgrenzen empfohlen:

Workload-Merkmale	**Empfohlene Volume-Beschränkung pro Node**	**Leistungseinbußen bei Überschreitung des Volumenlimits pro Knoten** [1]
Leseintensiv oder die Daten können komprimiert werden	150	4 % der maximalen IOPS
Schreibintensiv und die Daten können nicht komprimiert werden	60	• NAS: 10 % der maximalen IOPS für ONTAP 9.15.1 und früher • NAS: 5% 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 über diese Prozentsätze hinaus nicht beeinträchtigt, unabhängig von der Anzahl der hinzugefügten Volumes, die die empfohlenen Grenzwerte überschreiten.

Da die ARP-Analyse in einer priorisierten Reihenfolge ausgeführt wird, wird sie auf jedem Volume seltener ausgeführt, wenn die Anzahl der geschützten Volumes zunimmt.

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

Volumenbeschränkungen für ARP nach Plattform

Ab ONTAP 9.18.1 unterstützt ARP erhöhte Volume-Limits basierend auf Plattformtyp und CPU-Kernanzahl.

Plattformtyp	Maximale Anzahl ARP-fähiger Volumes pro Knoten
Low-end (Systeme mit bis zu 20 CPU-Kernen)	250
Mittel (Systeme mit bis zu 64 CPU-Kernen)	500
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.

Verifizierung mehrerer Administratoren mit Volumes, die mit ARP gesichert sind

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

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

Erfahren Sie mehr über `security anti-ransomware volume disable`, `security anti-ransomware volume pause` und `security anti-ransomware volume attack clear-suspect` in der "ONTAP-Befehlsreferenz".

Ab ONTAP 9.14.1 bietet ARP Warnmeldungen für die Erstellung eines ARP-Snapshots und für die Beobachtung einer neuen Dateierweiterung. Warnmeldungen für diese Ereignisse sind standardmäßig deaktiviert. Warnmeldungen können auf Volume- oder SVM-Ebene festgelegt werden. Sie können die Warnmeldungen aktivieren mit `security anti-ransomware vserver event-log modify` oder bei der Lautstärke mit `security anti-ransomware volume event-log modify`.

Erfahren Sie mehr über `security anti-ransomware vserver event-log modify` und `security anti-ransomware volume event-log modify` in der "ONTAP-Befehlsreferenz".

Nächste Schritte

- "Autonomer Schutz Vor Ransomware"
- "Aktivieren Sie MAV für ARP-geschützte Volumes"

ARP aktivieren

Aktivieren Sie den ONTAP Autonomous Ransomware Protection auf einem Volume

Ab ONTAP 9.10.1 können Sie den Autonomen Ransomware-Schutz (ARP) auf einem vorhandenen Volume aktivieren oder ein neues Volume erstellen und ARP von Anfang an aktivieren.

Über diese Aufgabe

Um ARP zu aktivieren, folgen Sie der für Ihre Umgebung passenden Vorgehensweise.Sie stellen sicher, dass Ihre Umgebung bestimmte Anforderungen erfüllt. :

- NAS mit FlexVol -Volumes
- NAS mit FlexGroup -Volumes
- SAN Volumes

Nach der Aktivierung von ARP kann ARP je nach Umgebung und ONTAP Version in eine Übergangsphase eintreten:

Volume-Typ	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 Sie ARP aktivieren, stellen Sie sicher, 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 aktiver"Verbindungspfad" für das Volumen.

SAN-spezifische Anforderungen

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

Allgemeine Anforderungen

- Der"Korrekte Lizenz" für Ihre ONTAP Version.
- (Empfohlen) Multi-Admin-Verifizierung (MAV) aktiviert (ONTAP 9.13.1 und höher). Sehen"Aktivieren Sie die Verifizierung durch mehrere Administratoren" .

ARP auf NAS FlexVol -Volumes aktivieren

Sie können ARP auf NAS FlexVol -Volumes mit dem System Manager oder der ONTAP CLI aktivieren. Der Ablauf variiert je nach Ihrer ONTAP Version.

ONTAP 9.16.1 und höher

Ab ONTAP 9.16.1 ist ARP/AI sofort aktiv, eine Lernphase ist nicht erforderlich.

System Manager

1. Wählen Sie **Storage > Volumes** und dann das zu schützende Volume aus.
2. Wählen Sie im Register **Sicherheit** der Übersicht **Volumes Status** aus, um von deaktiviert zu aktiviert zu wechseln.
3. Überprüfen Sie den ARP-Status des Volumes im **Anti-Ransomware**-Feld.

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

CLI

ARP auf einem vorhandenen Volume aktivieren:

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

Neues Volume mit aktiviertem ARP erstellen:

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

Überprüfen Sie den ARP-Status:

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

Erfahren Sie mehr über `security anti-ransomware volume show` in der "ONTAP-Befehlsreferenz".

ONTAP 9.10.1 bis 9.15.1

Für ONTAP 9.10.1 bis 9.15.1 sollten Sie ARP zunächst aktivieren."Lernmodus" (oder "Trockenlauf"-Zustand). Das System analysiert die Arbeitslast, um das normale Verhalten zu charakterisieren. Der Beginn im aktiven Modus kann zu übermäßig vielen falsch positiven Meldungen führen.

Es wird empfohlen, ARP mindestens 30 Tage lang im Lernmodus laufen zu lassen. Ab ONTAP 9.13.1 ermittelt ARP automatisch das optimale Lernintervall und automatisiert den Wechsel, der möglicherweise schon vor Ablauf der 30 Tage erfolgt.

System Manager

1. Wählen Sie **Storage > Volumes** und dann das zu schützende Volume aus.
2. Wählen Sie im Register **Sicherheit** der Übersicht **Volumes Status** aus, um von deaktiviert zu aktiviert zu wechseln.

3. Wählen Sie im Feld **Anti-Ransomware** die Option **Im Lernmodus aktiviert**.

> Du kannst"Automatisches Lernen für Übergänge zwischen aktiven Modi auf der zugehörigen Speicher-VM deaktivieren" Wenn Sie den Übergang vom Lernmodus zum aktiven Modus manuell steuern möchten.

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

4. Überprüfen Sie den ARP-Status des Volumes im **Anti-Ransomware**-Feld.

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

CLI

ARP auf einem vorhandenen Volume aktivieren:

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

Erfahren Sie mehr über `security anti-ransomware volume dry-run` in der "ONTAP-Befehlsreferenz".

Neues Volume mit aktiviertem ARP erstellen:

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

Automatische Umschaltung deaktivieren (optional):

Wenn Sie ein Upgrade von ONTAP 9.13.1 auf ONTAP 9.15.1 durchgeführt haben und den Switch für alle zugehörigen Volumes manuell vom Lern- in den Aktivmodus umschalten möchten, können Sie dies über die SVM tun:

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

Überprüfen Sie den ARP-Status:

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

ARP auf NAS FlexGroup -Volumes aktivieren

Sie können ARP auf NAS FlexGroup -Volumes mit dem System Manager oder der ONTAP CLI aktivieren. Der Ablauf variiert je nach Ihrer ONTAP Version.

ONTAP 9.18.1 und höher

Ab ONTAP 9.18.1 ist ARP/AI für FlexGroup -Volumes sofort aktiv, ohne dass eine Lernphase erforderlich ist.

System Manager

1. Wählen Sie **Speicher > Volumes** und anschließend das FlexGroup -Volume aus, das Sie schützen möchten.
2. Wählen Sie im Register **Sicherheit** der Übersicht **Volumes Status** aus, um von deaktiviert zu aktiviert zu wechseln.
3. Überprüfen Sie den ARP-Status des Volumes im **Anti-Ransomware**-Feld.

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

CLI

ARP auf einem vorhandenen FlexGroup Volume aktivieren:

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

Erstellen Sie ein neues FlexGroup Volume mit aktiviertem ARP:

```
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>
```

Überprüfen Sie den ARP-Status:

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

ONTAP 9.13.1 bis 9.17.1

Bei ONTAP 9.13.1 bis 9.17.1 beginnen FlexGroup -Volumes in"Lernmodus" Die Das System analysiert die Arbeitslast, um das normale Verhalten zu charakterisieren.

Es wird empfohlen, ARP mindestens 30 Tage lang im Lernmodus laufen zu lassen. ARP ermittelt automatisch das optimale Lernintervall und automatisiert den Wechsel, der auch vor Ablauf von 30 Tagen erfolgen kann.

System Manager

1. Wählen Sie **Speicher > Volumes** und anschließend das FlexGroup -Volume aus, das Sie schützen möchten.
2. Wählen Sie im Register **Sicherheit** der Übersicht **Volumes Status** aus, um von deaktiviert zu aktiviert zu wechseln.
3. Wählen Sie im Feld **Anti-Ransomware** die Option **Im Lernmodus aktiviert**.

Du kannst"Automatische Lernübergänge zwischen aktiven Modi deaktivieren" Wenn Sie den Übergang vom Lernmodus zum aktiven Modus manuell steuern möchten.

4. Überprüfen Sie den ARP-Status des Volumes im **Anti-Ransomware**-Feld.

CLI

ARP auf einem vorhandenen FlexGroup Volume aktivieren:

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

Erstellen Sie ein neues FlexGroup Volume mit aktiviertem ARP:

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

Automatische Umschaltung deaktivieren (optional):

Wenn Sie den Schalter vom Lern- in den Aktivmodus manuell steuern möchten:

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

Überprüfen Sie den ARP-Status:

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

ARP auf SAN-Volumes aktivieren

Ab ONTAP 9.17.1 können Sie ARP auf SAN-Volumes aktivieren. Die ARP/AI-Funktionalität wird automatisch aktiviert und beginnt sofort mit der aktiven Überwachung und dem Schutz von SAN-Volumes während des"Evaluierungszeitraum" gleichzeitig wird ermittelt, ob die Arbeitslasten für ARP geeignet sind, und ein optimaler Verschlüsselungsschwellenwert für die Erkennung festgelegt.

Sie können ARP auf SAN-Volumes mit dem System Manager oder der ONTAP CLI aktivieren.

System Manager

Schritte

1. Wählen Sie **Speicher > Volumes** und anschließend das SAN-Volume aus, das Sie schützen möchten.
2. Wählen Sie im Register **Sicherheit** der Übersicht **Volumes Status** aus, um von deaktiviert zu aktiviert zu wechseln.
3. ARP/AI tritt automatisch in die Evaluierungsphase ein.
4. Überprüfen Sie den ARP-Status und den Auswertungsstatus im **Anti-Ransomware**-Feld.

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

CLI

ARP auf einem vorhandenen SAN-Volume aktivieren:

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

Erstellen Sie ein neues SAN-Volume mit aktiviertem ARP:

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

Überprüfen Sie den ARP-Status und den Auswertungsstatus:

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

Überprüfen Sie die `Block device detection status` Feld zur Überwachung des Fortschritts im Evaluierungszeitraum.

Erfahren Sie mehr über `security anti-ransomware volume show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Nach einer Lernphase in den aktiven Modus wechseln"

Aktivieren Sie in neuen Volumes standardmäßig den autonomen ONTAP-Ransomware-Schutz

Ab ONTAP 9.10.1 können Sie Storage-VMs (SVMs) so konfigurieren, dass neue Volumes standardmäßig mit Autonomous Ransomware Protection (ARP) aktiviert sind. Sie können diese Einstellung mit dem System Manager oder der ONTAP CLI ändern.

Ab ONTAP 9.18.1 ist ARP auf allen neuen Volumes auf Clusterebene für "Unterstützte Systeme" nach einer 12-stündigen Übergangsfrist nach einem Cluster-Upgrade oder einer Neuinstallation standardmäßig aktiviert. Wenn Sie die automatische Standardaktivierung von ARP auf Clusterebene deaktivieren, können Sie ARP weiterhin standardmäßig manuell auf allen neuen Volumes auf SVM-Ebene aktivieren.

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

Über diese Aufgabe

Standardmäßig werden neue Volumes mit deaktivierter ARP-Funktionalität erstellt. Sie müssen die ARP-Funktionalität aktivieren und festlegen, dass sie standardmäßig für neu erstellte Volumes in der SVM aktiviert ist.

Bei bestehenden Volumes, bei denen ARP nicht aktiviert ist, ändert sich der ARP-Aktivierungsstatus nicht automatisch, wenn Sie den Standardwert für die SVM ändern. Die in diesem Verfahren beschriebenen Änderungen der SVM-Einstellungen wirken sich nur auf neue Volumina aus. Lerne, wie man"Aktivieren Sie ARP für vorhandene Volumes" Die

Nach der Aktivierung von ARP kann ARP je nach Umgebung und ONTAP Version in eine Übergangsphase eintreten:

Volume-Typ	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 Sie ARP aktivieren, stellen Sie sicher, dass Ihre Umgebung Folgendes aufweist:

NAS-spezifische Anforderungen

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

SAN-spezifische Anforderungen

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

Allgemeine Anforderungen

- Der"Korrekte Lizenz" für Ihre ONTAP Version.
- (Empfohlen) Multi-Admin-Verifizierung (MAV) aktiviert (ONTAP 9.13.1+). Sehen"Aktivieren Sie die Verifizierung durch mehrere Administratoren" .

Schritte

Sie können System Manager oder die ONTAP-CLI verwenden, um ARP auf neuen Volumes standardmäßig zu

aktivieren.

System Manager

1. Wählen Sie **Speicher** oder **Cluster** (je nach Ihrer Umgebung), wählen Sie **Speicher-VMs** und wählen Sie die Speicher-VM aus, die die Volumes enthalten soll, die Sie mit ARP schützen möchten.
2. Navigieren Sie zur Registerkarte **Einstellungen**. Suchen Sie unter **Sicherheit** die Kachel **Anti-Ransomware** und wählen Sie .
3. Aktivieren Sie das Kontrollkästchen, um Anti-Ransomware (ARP) zu aktivieren. Aktivieren Sie das zusätzliche Kontrollkästchen, um ARP auf allen berechtigten Volumes in der Speicher-VM zu aktivieren.
4. Bei ONTAP Versionen mit einer empfohlenen Lernzeit wählen Sie **Automatisch vom Lern- in den aktiven Modus wechseln nach ausreichendem Lernvorgang**. Dadurch kann ARP das optimale Lernintervall bestimmen und den Wechsel in den aktiven Modus automatisieren.

CLI

Ändern Sie eine bestehende SVM, um ARP standardmäßig in neuen Volumes zu aktivieren.

Wählen `dry-run` Wenn Ihre Version von ARP Folgendes erfordertLernzeitraum Die Andernfalls wählen Sie aus `enabled` Die

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

Erstellen Sie eine neue SVM, bei der ARP standardmäßig für neue Volumes aktiviert ist.

Wählen `dry-run` Wenn Ihre Version von ARP Folgendes erfordertLernzeitraum Die Andernfalls wählen Sie aus `enabled` Die

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

Modifizieren Sie die bestehende SVM, um den automatischen Übergang vom Lern- in den aktiven Modus zu deaktivieren.

Wenn Sie von ONTAP 9.13.1 auf ONTAP 9.15.1 aktualisiert haben und der Standardstatus `dry-run` (Lernmodus), adaptives Lernen ist aktiviert, so dass die Änderung auf `enabled` Der Status (aktiver Modus) wird automatisch festgelegt. Sie können diese automatische Umschaltung deaktivieren, sodass Sie die Umschaltung vom Lern- in den Aktivmodus für alle zugehörigen Volumes manuell steuern können:

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

Überprüfen Sie den ARP-Status

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

Verwandte Informationen

- "Nach einer Lernphase in den aktiven Modus wechseln"
- "Sicherheits-Anti-Ransomware-Volumenanzeige"

Deaktivieren Sie die standardmäßige Aktivierung des ONTAP Autonomous Ransomware Protection.

Ab ONTAP 9.18.1 ist der autonome Ransomware-Schutz (ARP) auf allen neuen Volumes für AFF A-Series und AFF C-Series, ASA und ASA r2-Systemen nach einer 12-stündigen Aufwärmphase nach einem Upgrade oder einer Neuinstallation standardmäßig automatisch aktiviert, sofern eine ARP-Lizenz installiert ist. Sie können diese Standardaktivierung während oder nach der 12-stündigen Übergangsphase mit System Manager oder der ONTAP CLI deaktivieren.

Vorhandene Volumes müssen "manuell aktiviert" für ARP sein.

Über diese Aufgabe

Die für dieses Verfahren gewählte Einstellung kann später geändert werden. Nach Ablauf der Kulanzfrist haben Sie jederzeit die Flexibilität, die 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 Standardaktivierungsoptionen für ARP zu verwalten.

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
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 angibt. Wählen Sie **Don't enable**.
     ii. Wählen Sie im nächsten Dialogfeld **Deaktivieren**, um zu bestätigen, dass die standardmäßige ARP-Aktivierung für neue Volumes ausgeschaltet ist.
   - Nach Ablauf der Kulanzfrist deaktivieren:
     i. Im Abschnitt **Anti-ransomware** wählen Sie .
     ii. Aktivieren Sie das Kontrollkästchen und dann auf **Speichern**, um die standardmäßige ARP-Aktivierung für neue Volumes zu deaktivieren.

CLI

1. Überprüfen Sie den standardmäßigen Aktivierungsstatus:

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

2. Standardmäßige Aktivierung für neue Volumes deaktivieren:

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

Verwandte Informationen

- "Aktivieren Sie den autonomen Ransomware-Schutz von ONTAP auf einem einzelnen Volume"

Nach einer Lernphase in ONTAP ARP in den aktiven Modus wechseln

In NAS-Umgebungen können Sie ein ARP-fähiges Volume manuell oder automatisch vom Lernmodus in den aktiven Modus umschalten. Sie müssen den Modus wechseln, wenn Sie ARP mit ONTAP 9.15.1 oder älter verwenden oder wenn ARP auf FlexGroup -Volumes mit ONTAP 9.17.1 oder älter ausgeführt wird.

Nachdem ARP einen Lernmodus-Lauf von mindestens 30 Tagen absolviert hat, können Sie manuell in den aktiven Modus wechseln. Ab ONTAP 9.13.1 ermittelt ARP automatisch das optimale Lernintervall und automatisiert den Wechsel, der möglicherweise schon vor Ablauf der 30 Tage erfolgt.

Wenn Sie ARP mit ARP/AI-Schutz verwenden, wird ARP automatisch aktiviert. ist keine Einarbeitungszeit erforderlich.

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

Nach dem Lernen manuell in den aktiven Modus wechseln

Bei ONTAP 9.10.1 bis 9.15.1 (ONTAP 9.17.1 und früher mit FlexGroup -Volumes) können Sie nach Abschluss der Lernphase manuell vom ARP-Lernmodus in den aktiven Modus über den System Manager oder die ONTAP CLI wechseln.

Über diese Aufgabe

Der in diesem Verfahren beschriebene manuelle Übergang in den aktiven Modus nach einer Lernphase ist spezifisch für NAS-Umgebungen.

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um vom Lernmodus in den aktiven Modus zu wechseln.

System Manager

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

CLI

1. Ändern Sie das geschützte Volume, um in den aktiven Modus zu wechseln, falls dies nicht bereits automatisch erfolgt ist:

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

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

   ```
   volume modify -volume <vol_name> -vserver <svm_name> -anti
   -ransomware-state enabled
   ```

2. Überprüfen Sie den ARP-Status des Volumes.

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

Automatisches Umschalten vom Lernmodus in den aktiven Modus

Ab ONTAP 9.13.1 wurde die ARP-Analyse um adaptives Lernen erweitert, und der Wechsel vom Lernmodus in den aktiven Modus erfolgt automatisch. Die autonome Entscheidung von ARP, automatisch vom Lernmodus in den aktiven Modus zu wechseln, basiert auf den Konfigurationseinstellungen der folgenden Optionen:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

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

Weitere Informationen zu ARP-Konfigurationsoptionen, einschließlich Standardwerten, finden Sie im "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Sicherheit Anti-Ransomware Volumen"

Erfahren Sie mehr über den ONTAP ARP-Evaluierungszeitraum für SAN-Volumes

Ab ONTAP 9.17.1 benötigt ARP einen Evaluierungszeitraum, um festzustellen, ob die Entropiewerte von SAN-Volume-Workloads für den Schutz vor Ransomware geeignet sind. Sobald ARP auf einem SAN-Volume aktiviert ist, überwacht und schützt ARP/AI das Volume während des Evaluierungszeitraums aktiv und ermittelt gleichzeitig einen optimalen Verschlüsselungsschwellenwert. Erkennungen und Warnungen können während der Evaluierungsphase anhand eines konservativen Schwellenwerts erfolgen, während die Basisschwellenwerte festgelegt werden. ARP unterscheidet zwischen geeigneten und ungeeigneten Workloads im ausgewerteten SAN-Volume und legt, wenn die Workloads als schutzwürdig eingestuft werden, automatisch einen Verschlüsselungsschwellenwert basierend auf den Statistiken des Evaluierungszeitraums fest.

Entropiebewertung verstehen

Das System erfasst kontinuierlich Verschlüsselungsstatistiken in 10-Minuten-Intervallen. Während der Auswertung werden außerdem kontinuierlich alle vier Stunden ARP-periodische Snapshots erstellt. Wenn der Verschlüsselungsprozentsatz innerhalb eines Intervalls den für dieses Volume ermittelten optimalen Verschlüsselungsschwellenwert überschreitet, wird eine Warnung ausgelöst, ein `Anti_ransomware_attack_backup` Es wird ein Snapshot erstellt und die Snapshot-Aufbewahrungszeit wird für alle regelmäßigen ARP-Snapshots erhöht.

Bestätigen Sie, dass der Testzeitraum aktiv ist

Sie können bestätigen, dass die Auswertung aktiv ist, indem Sie den folgenden Befehl ausführen und einen

Status von `evaluation_period`. Wenn ein Band nicht zur Evaluierung berechtigt 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
```

Überwachen der Datenerfassung im Auswertungszeitraum

Sie können die Verschlüsselungserkennung in Echtzeit überwachen, indem Sie den folgenden Befehl ausführen. Der 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> -name <lun_name> -duration real_time
```

Beispielantwort:

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

Geeignete Arbeitslasten und adaptive Schwellenwerte

Die Auswertung endet mit einem der folgenden Ergebnisse:

- *Die Arbeitslast ist für ARP geeignet. * ARP setzt den adaptiven Schwellenwert automatisch auf über 10 % des im Evaluierungszeitraum beobachteten maximalen Verschlüsselungsgrads. ARP sammelt außerdem fortlaufend Statistiken und erstellt regelmäßig ARP-Snapshots.
- **Die Arbeitslast ist für ARP ungeeignet.** ARP setzt den adaptiven Schwellenwert automatisch auf den maximalen Verschlüsselungsgrad, der während des Evaluierungszeitraums erreicht wurde. ARP sammelt weiterhin Statistiken und erstellt regelmäßig ARP-Snapshots. Das System empfiehlt jedoch, ARP auf dem Volume zu deaktivieren.

Evaluierungsergebnisse ermitteln

Nach Ablauf des Evaluierungszeitraums legt ARP den adaptiven Schwellenwert automatisch basierend auf den Evaluierungsergebnissen fest.

Sie können die Ergebnisse der Auswertung mit dem folgenden Befehl ermitteln. Die Eignung des Volumens wird in der `Block device detection status` Feld:

```
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 sich außerdem die Wertschwelle anzeigen lassen, die als Ergebnis der Auswertung angenommen wurde:

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

Beispielantwort:

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

Halten Sie die autonome Ransomware-Sicherung von ONTAP an, um Workload-Ereignisse aus der Analyse auszuschließen

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

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

"Erfahren Sie mehr über MAV".

Über diese Aufgabe

Während einer ARP-Pause protokolliert ONTAP keine Ereignisse oder Aktionen für neue Schreibvorgänge; die Analyse früherer Protokolle wird jedoch im Hintergrund fortgesetzt.

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

Schritte

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

System Manager

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

   > Ab ONTAP 9.13.1 werden Sie bei Verwendung von MAV zum Schutz der ARP-Einstellungen während des Pausenvorgangs aufgefordert, die Zustimmung eines oder mehrerer zusätzlicher Administratoren einzuholen. "Die Genehmigung muss von allen Administratoren eingeholt werden" Die Operation muss der MAV-Genehmigungsgruppe zugeordnet sein, sonst schlägt sie fehl.

3. Um die Überwachung fortzusetzen, wählen Sie **Anti-Ransomware fortsetzen**.

CLI

1. ARP auf einem Volume anhalten:

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

2. Um die Verarbeitung fortzusetzen, verwenden Sie den `resume` folgenden Befehl:

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

   Erfahren Sie mehr über `security anti-ransomware volume` in der "ONTAP-Befehlsreferenz".

3. Wenn Sie MAV (verfügbar mit ARP ab ONTAP 9.13.1) zum Schutz der ARP-Einstellungen verwenden, werden Sie beim Anhalten aufgefordert, die Zustimmung eines oder mehrerer zusätzlicher Administratoren einzuholen. Die Genehmigung muss von allen Administratoren der MAV-Genehmigungsgruppe eingeholt werden, andernfalls schlägt der Vorgang fehl.

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

   a. Anfrage anzeigen:

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

   b. Genehmigen Sie die Anforderung:

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

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

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

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

+
Erfahren Sie mehr über `security multi-admin-verify request` in der "ONTAP-Befehlsreferenz".

Managen Sie die Parameter für die Erkennung von Angriffen vor ONTAP Autonomous Ransomware Protection

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

Wie die Angriffserkennung funktioniert

Wenn sich Autonomous Ransomware Protection (ARP) im Lern- oder Evaluierungsmodus befindet, entwickelt es Basiswerte für das Volume-Verhalten. Dazu gehören Entropie, Dateierweiterungen und ab ONTAP 9.11.1 auch IOPS. Diese Basiswerte dienen zur Bewertung von Ransomware-Bedrohungen. Weitere Informationen zu diesen Kriterien finden Sie unter "Was ARP erkennt" .

Bestimmte Datenmengen und Arbeitslasten erfordern unterschiedliche Erkennungsparameter. Beispielsweise kann das ARP-fähige Volume zahlreiche Arten von Dateierweiterungen enthalten. In diesem Fall sollten Sie die Schwellenwertanzahl für noch nie gesehene Dateierweiterungen auf eine Zahl größer als den Standardwert von 20 ändern oder Warnungen basierend auf noch nie gesehenen Dateierweiterungen deaktivieren. Ab ONTAP 9.11.1 können Sie die Parameter der Angriffserkennung so anpassen, dass sie besser zu Ihren spezifischen Arbeitslasten passen.

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

Angriffserkennung in NAS-Umgebungen

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

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

Ab ONTAP 9.11.1 gibt ARP eine Bedrohungswarnung aus, wenn *only* eine Bedingung erfüllt ist. Wenn beispielsweise mehr als 20 Dateien mit Dateierweiterungen, die zuvor nicht im Volume beobachtet wurden, innerhalb eines Zeitraums von 24 Stunden beobachtet werden, kategorisiert ARP diese Datei als Bedrohung

unabhängig der beobachteten Entropie. Die 24-Stunden- und 20-Dateiwerte sind Standardwerte, die geändert werden können.

> Um die Anzahl falscher Alarme zu reduzieren, gehen Sie zu **Speicher > Volumes > Sicherheit > Workload-Eigenschaften konfigurieren** und deaktivieren Sie **Neue Dateitypen überwachen**. Diese Einstellung ist in ONTAP 9.14.1 P7, 9.15.1 P1, 9.16.1 und höher standardmäßig deaktiviert.

Angriffserkennung in SAN-Umgebungen

Ab ONTAP 9.17.1 gibt ARP eine Warnung aus, wenn es hohe Verschlüsselungsraten erkennt, die einen automatisch ermittelten Schwellenwert überschreiten. Dieser Schwellenwert wird nach einem "Evaluierungszeitraum" kann aber geändert werden.

Parameter für die Angriffserkennung ändern

Je nach dem zu erwartenden Verhalten des ARP-fähigen Volumes sollten Sie die Parameter der Angriffserkennung anpassen.

Schritte

1. Anzeigen der vorhandenen Angriffserkennungsparameter:

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

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume 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 können mit Booleschen oder ganzzahligen Werten geändert werden. Um ein Feld zu ändern, verwenden Sie die `security anti-ransomware volume attack-detection-parameters modify` Befehl.

   Erfahren Sie mehr über `security anti-ransomware volume attack-detection-parameters`

`modify` in der "ONTAP-Befehlsreferenz".

Bekannte Überspannungen melden

ARP ändert weiterhin Basiswerte für Erkennungsparameter, auch wenn diese aktiv sind. Wenn Sie von Überspannungen in Ihrer Volumenaktivität, entweder einmaligen Überspannungen oder einem Anstieg, der für eine neue Normalität charakteristisch ist, wissen, sollten Sie diese als sicher melden. Die manuelle Meldung dieser Überspannungen als sicher hilft, die Genauigkeit der ARP-Bedrohungsbewertungen zu verbessern.

Melden Sie einen einmaligen Anstieg

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

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

   Erfahren Sie mehr über `security anti-ransomware volume workload-behavior clear-surge` in der "ONTAP-Befehlsreferenz".

Änderung des Basislinienspunges

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

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

   Erfahren Sie mehr über `security anti-ransomware volume workload-behavior update-baseline-from-surge` im "ONTAP-Befehlsreferenz" .

Konfigurieren von ARP-Warnungen

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

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

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

Ereigniswarnungen können mit der Multi-Admin-Verifizierung gesteuert werden. Weitere Informationen finden Sie unter "Verifizierung mehrerer Administratoren mit Volumes, die mit ARP gesichert sind" .

Schritte

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

System Manager

Festlegen von Warnmeldungen für ein Volume

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

Festlegen von Warnmeldungen für eine SVM

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

CLI

Festlegen von Warnmeldungen für ein Volume

- So legen Sie Warnungen für eine neue Dateierweiterung fest:

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

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

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

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

Festlegen von Warnmeldungen für eine SVM

- So legen Sie Warnungen für eine neue Dateierweiterung fest:

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

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

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

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

Erfahren Sie mehr über `security anti-ransomware vserver event-log` Befehle in der "ONTAP-Befehlsreferenz" .

Verwandte Informationen

- "Autonome Ransomware-Schutzangriffe und den Überblick über den autonomen Ransomware-Schutz".
- "ONTAP-Befehlsreferenz"

Reagieren Sie auf ungewöhnliche Aktivität, die durch ONTAP ARP erkannt wurde

Wenn Autonomous Ransomware Protection (ARP) abnormale Aktivitäten in einem geschützten Volume erkennt, wird eine Warnung ausgegeben. Sie sollten die Benachrichtigung bewerten, um festzustellen, ob die Aktivität akzeptabel ist (falsch positiv) oder ob ein Angriff schädlich erscheint. Nachdem Sie den Angriff kategorisiert haben, können Sie die Warnungen und Hinweise zu verdächtigen Dateien löschen.

Wenn Sie einen Angriff kategorisieren, werden ARP-Snapshots entweder für einen verkürzten Zeitraum aufbewahrt, der durch den Kategorisierungsvorgang eingeleitet wird (ONTAP 9.16.1 und höher), oder sofort gelöscht (ONTAP 9.15.1 und früher).

Ab ONTAP 9.11.1 können Sie die "Aufbewahrungseinstellungen" für ARP-Snapshots.

Über diese Aufgabe

ARP zeigt eine Liste verdächtiger Dateien an, wenn es eine Kombination aus hoher Datenentropie, anormaler Volume-Aktivität mit Datenverschlüsselung und ungewöhnlichen Dateierweiterungen erkennt. Ab ONTAP 9.17.1 für NAS- und SAN-Umgebungen werden Details zu Entropiespitzen auch auf der Anti-Ransomware-Seite im System Manager gemeldet.

Wenn eine ARP-Warnmeldung ausgegeben wird, reagieren Sie, indem Sie die Aktivität auf eine der beiden folgenden Arten kennzeichnen:

- **Falsch positiv**

  Der identifizierte Dateityp oder die Entropiespitze ist in Ihrer Arbeitslast zu erwarten und kann ignoriert werden.

- **Potenzieller Ransomware-Angriff**

  Der identifizierte Dateityp oder die Entropiespitze ist in Ihrer Arbeitslast unerwartet und sollte als potenzieller Angriff behandelt werden.

Die normale Überwachung wird fortgesetzt, nachdem Sie Ihre Entscheidung aktualisiert und die ARP-

Benachrichtigungen gelöscht haben. ARP zeichnet Ihre Bewertung im Bedrohungsbewertungsprofil auf und nutzt Ihre Auswahl zur Überwachung nachfolgender Dateiaktivitäten.

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

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

Bevor Sie beginnen

ARP muss ein Volume aktiv schützen und darf sich nicht im Lern- oder Evaluierungsmodus befinden.

Schritte

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

System Manager

1. Wenn Sie eine Benachrichtigung über ungewöhnliche Aktivitäten erhalten, folgen Sie dem Link. Alternativ können Sie in der Übersicht „Volumes“ zur Registerkarte „Sicherheit“ navigieren.

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

2. Überprüfen Sie auf der Registerkarte **Sicherheit** den Bericht zu verdächtigen Dateitypen oder Entropiespitzen.
   - Untersuchen Sie bei verdächtigen Dateien jeden Dateityp im Dialogfeld **Verdächtige Dateitypen** und markieren Sie jeden einzeln.
   - Untersuchen Sie den Entropiebericht auf Entropiespitzen.
3. Notieren Sie Ihre Antwort:

Wenn Sie diesen Wert auswählen…	Führen Sie diese Aktion durch…
Falsch Positiv	a. Führen Sie einen der folgenden Schritte aus: ◦ Wählen Sie bei Dateitypwarnungen **Aktualisieren und verdächtige Dateitypen löschen**. ◦ Wählen Sie für Entropiespitzen **Als falsch positiv markieren**. Diese Aktionen löschen Warnhinweise zu verdächtigen Dateien oder Aktivitäten. ARP nimmt anschließend die normale Überwachung des Volumes wieder auf. Bei ARP/AI in ONTAP 9.16.1 und höher werden ARP-Snapshots nach einer durch den Kategorisierungsvorgang ausgelösten verkürzten Aufbewahrungsfrist automatisch gelöscht. Bei ONTAP 9.15.1 und früheren Versionen werden zugehörige ARP-Snapshots automatisch gelöscht, nachdem Sie verdächtige Dateitypen gelöscht haben. ⓘ Ab ONTAP 9.13.1 werden Sie bei Verwendung von MAV zum Schutz der ARP-Einstellungen durch den Clear Suspect-Vorgang aufgefordert, die Zustimmung eines oder mehrerer zusätzlicher Administratoren einzuholen. "Die Genehmigung muss von allen Administratoren eingeholt werden" Die Operation muss der MAV-Genehmigungsgruppe zugeordnet sein, sonst schlägt sie fehl.

Möglicher Angriff Durch Ransomware	a. Reagieren Sie auf den Angriff: ◦ Markieren Sie bei Dateitypwarnungen ausgewählte Dateien als **Potenzieller Ransomware-Angriff** und "Stellen Sie geschützte Daten wieder her" . ◦ Bei Entropiespitzen, die auf einen Angriff hinweisen, wählen Sie **Als potenziellen Ransomware-Angriff markieren** und "Stellen Sie geschützte Daten wieder her" . b. Nachdem die Datenwiederherstellung abgeschlossen ist, protokollieren Sie Ihre Entscheidung und nehmen Sie die normale ARP-Überwachung wieder auf: ◦ Wählen Sie bei Dateitypwarnungen **Aktualisieren und verdächtige Dateitypen löschen**. ◦ Wählen Sie für Entropiespitzen **Als potenziellen Ransomware-Angriff markieren** und dann **Speichern und verwerfen**. ⓘ Es gibt keine Hinweise zu verdächtigen Dateitypen, die gelöscht werden müssen, wenn Sie ein ganzes Volume wiederhergestellt haben. Durch die Aufzeichnung Ihrer Entscheidung wird der Angriffsbericht gelöscht. Bei ARP/AI in ONTAP 9.16.1 und höher werden ARP-Snapshots nach einer durch den Kategorisierungsvorgang ausgelösten verkürzten Aufbewahrungsfrist automatisch gelöscht. Bei ONTAP 9.15.1 und früheren Versionen werden die ARP-Snapshots nach der Wiederherstellung eines Volumes automatisch gelöscht.

CLI

Überprüfen Sie den Angriff

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

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

Probenausgabe:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 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. Erstellen 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]>
```

Beispielbefehl:

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

Probenausgabe:

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

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

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

Handeln Sie!

1. Führen Sie basierend auf Ihrer Auswertung der Dateierweiterungen oder Entropiespitzen eine der folgenden Aktionen aus:

   - Falsch positiv

     Führen Sie einen der folgenden Befehle aus, um Ihre Entscheidung zu protokollieren und die normale Überwachung des autonomen Ransomware-Schutzes fortzusetzen:

     - Für Dateierweiterungen:

```
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 zu identifizieren:

       - `[-extension <text>, … ]`: Dateierweiterungen

- Für Entropiespitzen:

```
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
```

◦ Möglicher Ransomware-Angriff

Reagieren Sie auf den Angriff und "Wiederherstellen von Daten aus dem ARP-erstellten Backup-Snapshot". Nachdem die Daten wiederhergestellt wurden, führen Sie einen der folgenden Befehle aus, um Ihre Entscheidung zu protokollieren und die normale ARP-Überwachung fortzusetzen

- Für Dateierweiterungen:

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

Mit dem folgenden optionalen Parameter können Sie nur bestimmte Erweiterungen als potenzielle Ransomware identifizieren:

- `[-extension <text>, … ]`: Dateierweiterung

- Für Entropiespitzen:

```
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
```

Das `clear-suspect` Der Vorgang löscht den Angriffsbericht. Es gibt keine Hinweise zu verdächtigen Dateitypen, die gelöscht werden müssen, wenn Sie ein ganzes Volume wiederhergestellt haben. Bei ARP/AI in ONTAP 9.16.1 und höher werden ARP-Snapshots nach einer durch den Kategorisierungsvorgang ausgelösten verkürzten Aufbewahrungsfrist automatisch gelöscht. Bei ONTAP 9.15.1 und früheren Versionen werden ARP-Snapshots automatisch gelöscht, nachdem Sie ein Volume wiederhergestellt oder ein verdächtiges Ereignis gelöscht haben.

2. Ab Version 9.18.1 können Sie den Status des/der `clear-suspect` Betrieb:

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

MAV-Optionen

1. Wenn Sie MAV verwenden und für einen erwarteten `clear-suspect` Vorgang zusätzliche Genehmigungen erforderlich sind, muss jeder Genehmiger der MAV-Gruppe:

a. Anfrage anzeigen:

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

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

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

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

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

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

Verwandte Informationen

- "NetApp Knowledge Base: Autonomous Ransomware Protection-Angriffe und den Autonomous Ransomware Protection-Snapshot verstehen"
- "Ändern Sie die Optionen für automatische Snapshots"
- "Sicherheit Anti-Ransomware Volumen"
- "Sicherheits-Multi-Admin-Verify-Anfrage"

Wiederherstellung von Daten aus ONTAP ARP Snapshots nach einem Ransomware-Angriff

Autonomous Ransomware Protection (ARP) erstellt Snapshots zum Schutz vor potenziellen Ransomware-Bedrohungen. Sie können einen dieser ARP-Snapshots oder einen anderen Snapshot Ihres Volumes zur Datenwiederherstellung verwenden.

Über diese Aufgabe

Das ARP erstellt Snapshots mit einem der folgenden vorangestellten Namen:

- `Anti_ransomware_periodic_backup` : Wird in ONTAP 9.17.1 und höher für Snapshots verwendet, die in regelmäßigen Abständen erstellt werden. Beispiel: `Anti_ransomware_periodic_backup.2025-06-01_1248` .
- `Anti_ransomware_attack_backup`: Wird in ONTAP 9.17.1 und höher für Snapshots verwendet, die als Reaktion auf Anomalien erstellt wurden. Beispiel: `Anti_ransomware_attack_backup.2025-08-25_1248` .
- `Anti_ransomware_backup` : Wird in ONTAP 9.16.1 und früheren Versionen mit Snapshots verwendet,

die als Reaktion auf Anomalien erstellt werden. Beispiel: `Anti_ransomware_backup.2022-12-20_1248`.

Um eine Wiederherstellung von einem anderen Snapshot als dem `Anti_ransomware` Snapshot nach der Erkennung eines Systemangriffs müssen Sie zunächst den ARP-Snapshot freigeben.

Wenn kein Systemangriff gemeldet wird, müssen Sie zuerst vom `Anti_ransomware` Erstellen Sie einen Snapshot und führen Sie anschließend eine Wiederherstellung des Volumes aus dem von Ihnen ausgewählten Snapshot durch.

> Wenn das ARP-geschützte Volume Teil einer SnapMirror -Beziehung ist, müssen Sie alle Spiegelkopien des Volumes nach der Wiederherstellung aus einem Snapshot manuell aktualisieren. Wenn Sie diesen Schritt überspringen, werden die Spiegelkopien möglicherweise unbrauchbar und müssen gelöscht und neu erstellt werden.

Bevor Sie beginnen

"Sie müssen den Angriff als potenziellen Ransomware-Angriff markieren" bevor Sie Daten aus einem Snapshot wiederherstellen.

Schritte

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

System Manager

Wiederherstellung nach einem Systemangriff

1. fahren Sie mit Schritt 2 fort, um die Wiederherstellung aus dem ARP-Snapshot durchzuführen. Zum Wiederherstellen aus einem früheren Snapshot müssen Sie zuerst die Sperre des ARP-Snapshots freigeben.
   a. Wählen Sie **Storage > Volumes**.
   b. Wählen Sie **Sicherheit** und dann **vermutete Dateitypen anzeigen**.
   c. Markieren Sie die Dateien als „potenzieller Ransomware-Angriff“.
   d. Wählen Sie **Update** und **Verdächtige Dateitypen löschen**.
2. Snapshots in Volumes anzeigen:

   Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies** aus.
3. Wählen Sie ⋮ neben dem Snapshot, den Sie wiederherstellen möchten, dann **Wiederherstellen**.

Wiederherstellung, wenn ein Systemangriff nicht erkannt wurde

1. Snapshots in Volumes anzeigen:

   Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies** aus.
2. Wählen ⋮ wählen Sie dann die `Anti_ransomware` Schnappschuss.
3. Wählen Sie **Wiederherstellen**.
4. Kehren Sie zum Menü **Snapshot-Kopien** zurück, und wählen Sie dann den gewünschten Snapshot aus. Wählen Sie **Wiederherstellen**.

CLI

Wiederherstellung nach einem Systemangriff

fahren Sie mit Schritt 2 fort, um die Wiederherstellung aus dem ARP-Snapshot durchzuführen. Um Daten aus früheren Snapshots wiederherzustellen, müssen Sie die Sperre für den ARP-Snapshot freigeben.

> ⓘ Es ist nur notwendig, die Anti-Ransomware-SnapLock vor der Wiederherstellung aus früheren Snapshots freizugeben, wenn Sie den Befehl wie unten beschrieben verwenden `volume snapshot restore`. Wenn Sie Daten mit FlexClone, Single File Snap Restore oder anderen Methoden wiederherstellen, ist dies nicht erforderlich.

1. Markieren Sie den Angriff als potenziellen Ransomware-Angriff (`-false-positive false`) und löschen Sie verdächtige Dateien (`clear-suspect`):

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

   Verwenden Sie einen der folgenden Parameter, um die Erweiterungen zu identifizieren:

   - `[-seq-no` *`integer`*`]` : Sequenznummer der Datei in der Verdächtigenliste.
   - `[-extension` *`text`*`, … ]` : Dateierweiterungen

- `[-start-time date_time -end-time date_time]` : Start- und Endzeiten für den zu löschenden Dateibereich im Format „MM/TT/JJJJ HH:MM:SS“.

2. Listen Sie die Snapshots in einem Volume auf:

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

Das folgende Beispiel zeigt den Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Wiederherstellen des Inhalts eines Volumes aus einem Snapshot:

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

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

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

Wiederherstellung, wenn ein Systemangriff nicht erkannt wurde

1. Listen Sie die Snapshots in einem Volume auf:

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

Das folgende Beispiel zeigt den Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Wiederherstellen des Inhalts eines Volumes aus einem Snapshot:

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

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

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

Erfahren Sie mehr über `volume snapshot` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "NetApp Knowledge Base: Ransomware-Prävention und -Wiederherstellung in ONTAP"
- "ONTAP-Befehlsreferenz"

Einstellungen für automatisch generierte ARP-Snapshots anpassen

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

Bevor Sie beginnen

Sie können ARP-Snapshot-Optionen nur auf einem "Knoten-SVM" und nicht auf anderen SVM-Typen.

Schritte

1. Zeigt alle aktuellen ARP-Snapshot-Einstellungen an:

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

2. Ausgewählte aktuelle ARP-Snapshot-Einstellungen anzeigen:

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

3. Ändern der ARP-Snapshot-Einstellungen:

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

Sie können folgende Einstellungen ändern:

Einige der beschriebenen Befehle sind ab ONTAP 9.17.1 veraltet. Die in ONTAP 9.17.1 eingeführten Befehle unterstützen sowohl NAS- als auch SAN-Umgebungen.

Einstellung	Beschreibung	Unterstützte Versionen
`arw.snap.max.count`	Gibt die maximale Anzahl von ARP-Snapshots an, die gleichzeitig in einem Volume vorhanden sein können. Ältere Kopien werden gelöscht, um sicherzustellen, dass die Gesamtzahl der ARP-Snapshots innerhalb dieses Grenzwerts liegt.	ONTAP 9.11.1 und höher
`arw.snap.create.interval.hours`	Gibt das Intervall in Stunden zwischen ARP-Snapshots an. Ein neuer ARP-Snapshot wird erstellt, wenn ein datenentropiebasierter Angriff vermutet wird und der zuletzt erstellte ARP-Snapshot älter als das angegebene Intervall ist.	ONTAP 9.11.1 und höher
`arw.snap.normal.retain.interval.hours`	Gibt die Dauer in Stunden an, für die ein ARP-Snapshot aufbewahrt wird. Wenn ein ARP-Snapshot den Aufbewahrungsschwellenwert erreicht, wird er gelöscht.	• ONTAP 9.11.1 bis ONTAP 9.16.1 • Veraltet in ONTAP 9.17.1 und höher

Einstellung	Beschreibung	Unterstützte Versionen
`arw.snap.max.retain.interval.days`	Gibt die maximale Dauer *in Tagen* an, für die ein ARP-Snapshot beibehalten werden kann. Jeder ARP-Snapshot, der älter als diese Dauer ist, wird gelöscht, wenn kein Angriff auf dem Volume gemeldet wird. Das maximale Aufbewahrungsintervall für ARP-Snapshots wird ignoriert, wenn eine mäßige Bedrohung erkannt wird. Der als Antwort auf die Bedrohung erstellte ARP-Snapshot wird beibehalten, bis Sie auf die Bedrohung reagiert haben. Wenn Sie eine Bedrohung als „falsch positiv“ markieren, löscht ONTAP die ARP-Schnappschüsse für das Volume.	• ONTAP 9.11.1 bis ONTAP 9.16.1 • Veraltet in ONTAP 9.17.1 und höher
`arw.snap.create.interval.hours.post.max.count`	Gibt das Intervall in Stunden zwischen ARP-Snapshots an, wenn das Volume bereits die maximale Anzahl an ARP-Snapshots enthält. Sobald die maximale Anzahl erreicht ist, wird ein ARP-Snapshot gelöscht, um Platz für eine neue Kopie zu schaffen. Mit dieser Option kann die Geschwindigkeit der Erstellung neuer ARP-Snapshots reduziert werden, um die ältere Kopie beizubehalten. Wenn das Volume bereits die maximale Anzahl an ARP-Snapshots enthält, wird für die nächste ARP-Snapshot-Erstellung das in dieser Option angegebene Intervall verwendet, anstatt `arw.snap.create.interval.hours` .	• ONTAP 9.11.1 bis 9.16.1 • Veraltet in ONTAP 9.17.1 und höher
`arw.snap.low.encryption.retain.duration.hours`	Gibt die Aufbewahrungsdauer *in Stunden* für ARP-Snapshots an, die während Zeiten geringer Verschlüsselungsaktivität erstellt wurden.	• ONTAP 9.17.1 und höher
`arw.snap.new.extns.interval.hours`	Gibt das Intervall in Stunden zwischen den ARP-Snapshots an, die beim Erkennen einer neuen Dateierweiterung erstellt werden. Ein neuer ARP-Snapshot wird erstellt, wenn eine neue Dateierweiterung erkannt wird; der vorherige Snapshot, der beim Erkennen einer neuen Dateierweiterung erstellt wurde, ist älter als das angegebene Intervall. Bei einer Arbeitslast, die häufig neue Dateierweiterungen erstellt, hilft dieses Intervall, die Häufigkeit der ARP-Snapshots zu steuern. Diese Option existiert unabhängig von `arw.snap.create.interval.hours` , das das Intervall für auf Datenentropie basierende ARP-Snapshots angibt.	• ONTAP 9.11.1 bis ONTAP 9.16.1 • Veraltet in ONTAP 9.17.1 und höher

Einstellung	Beschreibung	Unterstützte Versionen
`arw.snap.retain.hours.after.clear.suspect.false.alert`	Gibt das Intervall in Stunden an, in dem ein ARP-Snapshot vorsorglich aufbewahrt wird, nachdem ein Angriffsvorfall vom Administrator als falsch positiv markiert wurde. Nach Ablauf dieser Aufbewahrungsfrist kann der Snapshot gemäß der in den Optionen definierten Standardaufbewahrungsdauer gelöscht werden. `arw.snap.normal.retain.interval.hours` Und `arw.snap.max.retain.interval.days` .	• ONTAP 9.16.1 und höher
`arw.snap.retain.hours.after.clear.suspect.real.attack`	Gibt das Intervall in Stunden an, in dem ein ARP-Snapshot vorsorglich aufbewahrt wird, nachdem ein Angriff vom Administrator als echter Angriff markiert wurde. Nach Ablauf dieser Aufbewahrungsfrist kann der Snapshot gemäß der in den Optionen definierten Standardaufbewahrungsdauer gelöscht werden. `arw.snap.normal.retain.interval.hours` Und `arw.snap.max.retain.interval.days` .	• ONTAP 9.16.1 und höher
`arw.snap.surge.interval.days`	Gibt das Intervall *in Tagen* zwischen ARP-Snapshots an, die als Reaktion auf I/O-Überspannungen erstellt wurden. ONTAP erzeugt eine ARP-Snapshot Überspannungskopie, wenn es einen Anstieg des IO-Verkehrs gibt und der letzte erstellte ARP-Snapshot ist älter als dieses angegebene Intervall. Mit dieser Option wird auch die Aufbewahrungsfrist *in Tag* für einen ARP-Überspannungsabschuss festgelegt.	ONTAP 9.11.1 und höher
`arw.high.encryption.alert.enabled`	Aktiviert Warnmeldungen bei hohen Verschlüsselungsstufen. Wenn diese Option auf `on` (Standard) sendet ONTAP eine Warnung, wenn der Prozentsatz der Verschlüsselung den in `arw.high.encryption.percentage.threshold` .	ONTAP 9.17.1 und höher
`arw.high.encryption.percentage.threshold`	Gibt den maximalen Verschlüsselungsgrad für ein Volume an. Überschreitet der Verschlüsselungsgrad diesen Schwellenwert, behandelt ONTAP die Erhöhung als Angriff und erstellt einen ARP-Snapshot. `arw.high.encryption.alert.enabled` muss eingestellt werden auf `on` damit diese Option wirksam wird.	ONTAP 9.17.1 und höher
`arw.snap.high.encryption.retain.duration.hours`	Gibt das Aufbewahrungsdauerintervall *in Stunden* für Snapshots an, die während eines Ereignisses mit hohem Verschlüsselungsschwellenwert erstellt wurden.	ONTAP 9.17.1 und höher

4. Wenn Sie ARP mit 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`	Gibt den minimalen Prozentwert für den Verschlüsselungsschwellenwert während der automatischen Lernphase der Auswertung für Blockgeräte an.	ONTAP 9.17.1 und höher
`arw.block_device.auto.learn.threshold.max_value`	Gibt den maximalen Prozentwert für den Verschlüsselungsschwellenwert während der automatischen Lernphase der Auswertung für Blockgeräte an.	ONTAP 9.17.1 und höher
`arw.block_device.evaluation.phase.min_hours`	Gibt das Mindestintervall *in Stunden* an, in dem die Auswertungsphase ausgeführt werden 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 ausgeführt werden muss, bevor der Verschlüsselungsschwellenwert festgelegt wird.	ONTAP 9.17.1 und höher
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	Gibt die Mindestmenge an Daten *in GB* an, die während der Evaluierungsphase aufgenommen 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 Evaluierungsphase von ARP auf Blockgeräten aktiviert sind. Der Standardwert ist `True`.	ONTAP 9.17.1 und höher
`arw.block_device.evaluation.phase.alert.threshold`	Gibt den Schwellenwertprozentsatz während der ARP-Evaluierungsphase auf Blockgeräten an. Wenn der Verschlüsselungsprozentsatz diesen Schwellenwert überschreitet, wird eine Warnung ausgelöst.	ONTAP 9.17.1 und höher

Verwandte Informationen

- "Bedrohungsbewertung und ARP-Snapshots"
- "SAN-Entropie-Auswertungszeitraum"

Autonomer ONTAP-Schutz mit KI (ARP/AI) aktualisieren

Um den Schutz vor neuesten Ransomware-Bedrohungen auf dem neuesten Stand zu halten, bietet ARP/AI automatische Updates, die außerhalb der regelmäßigen ONTAP-Release-Intervalle stattfinden.

Ab ONTAP 9.16.1 sind Sicherheitsupdates für ARP/AI zusätzlich zu System- und Firmware-Updates in den Software-Downloads des System Managers verfügbar. Wenn Ihr ONTAP Cluster bereits registriert ist in "Automatische Updates von System und Firmware" werden Sie automatisch benachrichtigt, wenn ARP/AI-Sicherheitsupdates verfügbar sind. Sie können auch Ihre Update-Einstellungen damit ONTAP Sicherheitsupdates automatisch installiert.

Wenn Sie möchtenManuelles Update von ARP/AI, können Sie Updates von der NetApp-Support-Website herunterladen und mit dem System-Manager installieren.

Über diese Aufgabe

Sie können ARP/AI nur mit System Manager aktualisieren.

Wählen Sie eine Aktualisierungseinstellung für ARP/AI aus

Im System Manager sind die Einstellungen auf der Seite Automatische Updates für Sicherheitsdateien aktivieren auf `Show notifications` wenn Sie bereits für automatische Firmware- und Systemupdates registriert sind. Sie können die Update-Einstellungen ändern, um `Automatically update` Wenn Sie möchten, dass ONTAP die neuesten Updates automatisch einspielt. Wenn Sie eine Dark Site verwenden oder Updates lieber manuell durchführen, können Sie Benachrichtigungen anzeigen oder Sicherheitsupdates automatisch ablehnen.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im System Manager auf **Cluster > Einstellungen > Softwareupdates**.
2. Wählen Sie im Abschnitt **Software-Updates** die Option →.
3. Wählen Sie auf der Seite **Software-Updates** die Registerkarte **Alle anderen Updates** aus.
4. Wählen Sie die Registerkarte **Alle anderen Updates** und klicken Sie auf **Mehr**.
5. Wählen Sie **Einstellungen für automatische Aktualisierung bearbeiten**.
6. Wählen Sie auf der Seite Einstellungen für die automatische Aktualisierung die Option **Sicherheitsdateien** aus.
7. Geben Sie die Aktion an, die für Sicherheitsdateien (ARP/AI-Updates) ausgeführt werden soll.

   Sie können auswählen, ob Updates automatisch aktualisiert, angezeigt oder automatisch geschlossen werden sollen.

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

8. Akzeptieren Sie die Bedingungen und wählen Sie **Speichern**.

ARP/AI manuell mit dem neuesten Sicherheitspaket aktualisieren

Befolgen Sie das entsprechende Verfahren, je nachdem, ob Sie bei Active IQ Unified Manager registriert sind.

ⓘ Stellen Sie sicher, dass Sie nur ein aktuelleres ARP-Update als Ihre aktuelle Version installieren, um unbeabsichtigte ARP-Downgrades zu vermeiden.

ONTAP 9.16.1 und höher mit Digital Advisor

1. Gehen Sie im System Manager zu **Dashboard**.

   Im Abschnitt **Health** wird eine Meldung angezeigt, ob es empfohlene Sicherheitsupdates für den Cluster

gibt.

2. Klicken Sie auf die Warnmeldung.
3. Wählen Sie neben den Sicherheitsupdates in der Liste der empfohlenen Updates **Actions** aus.
4. Klicken Sie auf **Update**, um das Update sofort zu installieren, oder auf **Schedule**, um es für später zu planen.

   Wenn das Update bereits geplant ist, können Sie es **Bearbeiten** oder **Abbrechen**.

ONTAP 9.16.1 und höher ohne digitalen Berater

1. Navigieren Sie zum"NetApp Support-Website", und melden Sie sich an.
2. Füllen Sie die Eingabeaufforderungen aus und laden Sie das Sicherheitspaket herunter, das Sie zum Aktualisieren der Cluster-ARP/AI verwenden möchten.
3. Kopieren Sie die Dateien auf einen HTTP- oder FTP-Server in Ihrem Netzwerk oder in einen lokalen Ordner, auf den das Cluster mit ARP/AI zugreifen kann.
4. Klicken Sie im System Manager auf **Cluster > Einstellungen > Softwareupdates**.
5. Wählen Sie unter **Software-Updates** die Registerkarte **Alle anderen Updates** aus.
6. Klicken Sie im Bereich **Manuelle Updates** auf **Sicherheitsdateien hinzufügen** und fügen Sie die Dateien mit einer der folgenden Einstellungen hinzu:
   - **Download vom Server**: Geben Sie die URL für das Sicherheitsdateipaket ein.
   - **Upload vom lokalen Client**: Navigieren Sie zur heruntergeladenen TGZ-Datei.

   > Stellen Sie sicher, dass der Dateiname mit beginnt `ontap_security_file_arpai_` und `.tgz` als Dateierweiterung verwendet wird.

7. Klicken Sie auf **Hinzufügen**, um die Updates anzuwenden.

Überprüfung von ARP/AI Updates

Gehen Sie wie folgt vor, um den Verlauf der automatischen Aktualisierungen anzuzeigen, die verworfen oder nicht installiert wurden:

1. Klicken Sie im System Manager auf **Cluster > Einstellungen > Softwareupdates**.
2. Wählen Sie im Abschnitt **Software-Updates** die Option →.
3. Wählen Sie auf der Seite **Software Updates** die Registerkarte **Alle anderen Updates** aus und klicken Sie auf **Mehr**.
4. Wählen Sie **Alle automatischen Updates anzeigen**.

Verwandte Informationen

- "Erfahren Sie mehr über ARP/KI"
- "E-Mail-Abonnements für Software-Updates"