Schutz vor Ransomware-Angriffen

ASA r2

NetApp
February 11, 2026

Inhalt

Schutz vor Ransomware-Angriffen

Erstellen Sie manipulationssichere Snapshots zum Schutz vor Ransomware-Angriffen auf ASA R2-Speichersysteme

Um besser gegen Ransomware-Angriffe zu schützen, replizieren Sie Snapshots in ein Remote-Cluster und sperren Sie dann die Ziel-Snapshots, damit sie manipulationssicher sind. Gesperrte Snapshots können nicht versehentlich oder böswillig gelöscht werden. Sie können gesperrte Snapshots verwenden, um Daten wiederherzustellen, wenn ein Storage-Gerät jemals durch einen Ransomware-Angriff kompromittiert wurde.

Initialisieren Sie die SnapLock Compliance-Uhr

Bevor Sie manipulationssichere Snapshots erstellen können, müssen Sie die SnapLock Compliance Uhr auf Ihren lokalen und Ziel-Clustern initialisieren.

Schritte

1. Wählen Sie **Cluster > Übersicht**.
2. Wählen Sie im Abschnitt **Knoten** die Option **SnapLock Compliance-Uhr initialisieren** aus.
3. Wählen Sie **Initialisieren**.
4. Vergewissern Sie sich, dass die Compliance-Uhr initialisiert ist.
   a. Wählen Sie **Cluster > Übersicht**.
   b. Wählen Sie im Abschnitt **Knoten** die Option ; und wählen Sie dann **SnapLock Compliance Uhr**.

Was kommt als Nächstes?

Nachdem Sie die SnapLock Compliance-Uhr auf Ihren lokalen und Ziel-Clustern initialisiert haben, sind Sie bereit zu "Erstellen Sie eine Replikationsbeziehung mit gesperrten Snapshots".

Aktivieren Sie autonomen Ransomware-Schutz mit KI auf Ihren ASA R2-Speichersystemen

Ab ONTAP 9.17.1 können Sie die Daten Ihres ASA r2-Systems mit Autonomous Ransomware Protection mit künstlicher Intelligenz (ARP/AI) schützen. ARP/AI erkennt potenzielle Ransomware-Bedrohungen schnell, erstellt automatisch einen ARP-Snapshot zum Schutz Ihrer Daten und zeigt im System Manager eine Warnmeldung an, um Sie auf verdächtige Aktivitäten aufmerksam zu machen.

ARP verbessert die Cyber-Resilienz durch die Einführung eines Machine-Learning-Modells für Anti-Ransomware-Analysen, das sich ständig weiterentwickelnde Formen von Ransomware mit 98 % Genauigkeit in SAN-Umgebungen erkennt. Das Machine-Learning-Modell von ARP ist auf einem großen Datensatz von Dateien sowohl vor als auch nach einem simulierten Ransomware-Angriff vortrainiert. Dieses ressourcenintensive Training erfolgt außerhalb von ONTAP, und das vortrainierte Modell, das aus diesem Training resultiert, ist mit ONTAP on-box enthalten. Dieses Modell ist nicht zugänglich oder veränderbar. ARP/AI ist unmittelbar nach der Aktivierung aktiv; es gibt kein "Lernphase".

Kein System zur Erkennung oder Abwehr von Ransomware kann absolute Sicherheit vor einem Ransomware-Angriff garantieren. Auch wenn ein Angriff unentdeckt bleibt, dient ARP/AI als wichtige zusätzliche Verteidigungsebene, falls Anti-Virus-Software einen Eindringling nicht erkennt.

Über diese Aufgabe

- ARP/AI-Unterstützung ist im Lieferumfang enthalten "ONTAP One-Lizenz" .
- ARP/AI wird auf Speichereinheiten, die durch SnapMirror active sync, SnapMirror synchron oder SnapLock geschützt sind, nicht unterstützt.
- Ab ONTAP 9.18.1 ist ARP/AI standardmäßig auf allen neu erstellten Speichereinheiten 12 Stunden nach dem Upgrade auf ONTAP 9.18.1 oder der Initialisierung eines neuen ONTAP 9.18.1 ASA r2 Clusters aktiviert.
- Nachdem Sie ARP/AI aktiviert haben, sollten Sie "Aktivieren Sie automatische Updates für Ihre Sicherheitsdateien" um automatisch neue Sicherheitsupdates zu erhalten.

Aktivieren Sie ARP/AI auf allen Speichereinheiten im Cluster

Wenn Sie ONTAP 9.17.1 verwenden, können Sie ARP/AI auf allen im Cluster erstellten Speichereinheiten standardmäßig aktivieren.

In ONTAP 9.18.1 und höher ist ARP/AI standardmäßig auf allen neuen Speichereinheiten aktiviert. Wenn Sie Speichereinheiten haben, die in ONTAP 9.17.1 erstellt wurden und für die ARP/AI nicht aktiviert ist, können Sie es manuell aktivieren.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Anti-ransomware** ⋮ und dann **Auf allen vorhandenen Speichereinheiten aktivieren** aus.
3. Wählen Sie **Aktivieren**.

Aktivieren Sie ARP/AI auf allen Speichereinheiten in einer Speicher-VM.

Wenn Sie ONTAP 9.17.1 verwenden, können Sie ARP/AI standardmäßig für alle in einer Storage-VM erstellten Speichereinheiten aktivieren. Das bedeutet, dass jede neue in der Storage-VM erstellte Speichereinheit ARP/AI automatisch aktiviert hat. Sie können ARP/AI auch auf bereits vorhandene Speichereinheiten in der Storage-VM anwenden.

In ONTAP 9.18.1 und höher ist ARP/AI standardmäßig auf allen neuen Speichereinheiten aktiviert. Wenn Sie Speichereinheiten haben, die in ONTAP 9.17.1 erstellt wurden und für die ARP/AI nicht aktiviert ist, können Sie es manuell aktivieren.

Schritte

1. Wählen Sie im System Manager **Cluster > Storage-VMs** aus.
2. Wählen Sie die Speicher-VM aus, auf der Sie ARP/AI aktivieren möchten.
3. Wählen Sie im Abschnitt **Sicherheit** neben **Anti-Ransomware** ⋮ ; wählen Sie dann **Anti-Ransomware-Einstellungen bearbeiten**.
4. Wählen Sie **Anti-Ransomware aktivieren**.

   Dadurch wird ARP/AI standardmäßig auf allen zukünftigen Speichereinheiten aktiviert, die auf der

ausgewählten Speicher-VM erstellt werden.

5. Um ARP auf vorhandene Speichereinheiten auf der ausgewählten Speicher-VM anzuwenden, wählen Sie **Diese Änderung auf alle zutreffenden vorhandenen Speichereinheiten auf dieser Speicher-VM anwenden**.
6. Wählen Sie **Speichern**.

Ergebnis

Alle neu erstellten Speichereinheiten auf der Speicher-VM sind standardmäßig vor Ransomware-Angriffen geschützt, und verdächtige Aktivitäten werden Ihnen im System Manager gemeldet.

Aktivieren Sie ARP/AI auf bestimmten Speichereinheiten in einer Speicher-VM.

Wenn Sie ONTAP 9.17.1 verwenden und ARP/AI nicht auf allen Speichereinheiten in einer Storage-VM aktivieren möchten, können Sie die spezifischen Einheiten auswählen, die Sie aktivieren möchten.

In ONTAP 9.18.1 und höher ist ARP/AI standardmäßig auf allen neuen Speichereinheiten aktiviert. Wenn Sie Speichereinheiten haben, die in ONTAP 9.17.1 erstellt wurden und für die ARP/AI nicht aktiviert ist, können Sie es manuell aktivieren.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die Speichereinheiten aus, für die Sie ARP/AI aktivieren möchten.
3. Wählen ⋮ ; wählen Sie dann **Anti-Ransomware aktivieren**.
4. Wählen Sie **Aktivieren**.

Ergebnis

Die von Ihnen ausgewählten Speichereinheiten sind vor Ransomware-Angriffen geschützt und verdächtige Aktivitäten werden Ihnen im System Manager gemeldet.

Deaktivieren Sie den standardmäßigen autonomen Ransomware-Schutz auf Ihren ASA r2-Speichersystemen

Bei der Initialisierung eines neuen ONTAP 9.18.1 ASA r2-Clusters oder beim Upgrade Ihres Clusters auf ONTAP 9.18.1 wird ARP/AI nach einer 12-stündigen Testphase standardmäßig auf allen neuen Speichereinheiten aktiviert. Wenn Sie ARP/AI während der Testphase nicht deaktivieren, wird es nach Ablauf der Testphase clusterweit für neue Speichereinheiten aktiviert.

In ONTAP 9.17.1 erstellte Speichereinheiten müssen "manuell aktiviert" für ARP/AI sein.

Schritte

Sie können die standardmäßige Aktivierung während oder nach der anfänglichen 12-stündigen Kulanzzeit deaktivieren.

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. ARP deaktivieren:
   - So deaktivieren Sie während der 12-stündigen Kulanzfrist:
     i. Unter **Anti-ransomware** wählen Sie **Don't enable** und anschließend **Disable**.
   - So deaktivieren Sie nach Ablauf der 12-stündigen Kulanzfrist:
     i. Unter **Anti-Ransomware** wählen Sie und deaktivieren anschließend **Für neue Speichereinheiten aktivieren**.
     ii. **Speichern** auswählen

CLI

1. Überprüfen Sie den standardmäßigen Aktivierungsstatus:

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

2. Standardmäßige Aktivierung für bestehende und neue Volumes deaktivieren:

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

Ändern Sie die Aufbewahrungsfristen für ARP/AI-Snapshots auf ASA R2-Speichersystemen

Wenn Autonomous Ransomware Protection mit Künstlicher Intelligenz (ARP/AI) ungewöhnliche Aktivitäten auf einer oder mehreren Ihrer ASA r2-Systemspeichereinheiten erkennt, erstellt es automatisch einen ARP-Snapshot, um die Daten der Speichereinheit zu schützen. Abhängig von Ihrer Speicherkapazität und den geschäftlichen Anforderungen an Ihre Daten können Sie die standardmäßige Aufbewahrungsdauer für ARP-Snapshots verlängern oder verkürzen. Beispielsweise können Sie die Aufbewahrungsdauer für geschäftskritische Anwendungen verlängern, um bei Bedarf längere Aufbewahrungsfristen für die Datenwiederherstellung zu haben, oder die Aufbewahrungsdauer für nicht-kritische Anwendungen verkürzen, um Speicherplatz zu sparen.

Die standardmäßige Aufbewahrungsdauer für den ARP-Snapshot variiert je nach der Aktion, die Sie als Reaktion auf die abnormale Aktivität ergreifen.

Wenn Sie diese Aktion ausführen …	ARP-Snapshots werden standardmäßig aufbewahrt für…
Als falsch positiv markieren	12 Stunden

Wenn Sie diese Aktion ausführen …	ARP-Snapshots werden standardmäßig aufbewahrt für…
Als potenziellen Ransomware-Angriff markieren	7 Tage
Ergreifen Sie keine sofortigen Maßnahmen	10 Tage

Die Standardaufbewahrungsfristen können über die ONTAP Befehlszeilenschnittstelle (CLI) geändert werden. Siehe "Optionen für automatische ONTAP -Snapshots ändern" für Schritte zum Ändern der Standardaufbewahrungsdauer.

Reagieren Sie auf autonomen Ransomware-Schutz mit KI-Warnungen auf ASA R2-Speichersystemen

Wenn der autonome Ransomware-Schutz mit künstlicher Intelligenz (ARP/AI) ungewöhnliche Aktivitäten auf einer oder mehreren Ihrer ASA r2-Systemspeichereinheiten erkennt, wird eine Warnung im System Manager-Dashboard angezeigt. Sie sollten die Warnung anzeigen, die Aktivität überprüfen und gegebenenfalls Maßnahmen ergreifen, um eine potenzielle Bedrohung Ihrer Daten zu verhindern.

Wenn eine ARP/AI-Warnmeldung angezeigt wird, sollten Sie vor dem Ergreifen von Maßnahmen die Integrität der Daten auf dem Speichergerät mit einem entsprechenden Anwendungsintegritätsprüfer überprüfen. Durch die Überprüfung der Datenintegrität des Speichergeräts können Sie feststellen, ob die Aktivität akzeptabel ist oder ob es sich um einen potenziellen Ransomware-Angriff handelt.

Wenn die abnormale Aktivität … ist.	Dann tun Sie Folgendes …
Akzeptabel	Markieren Sie die Aktivität als falsch-positiv.
Ein potenzieller Ransomware-Angriff	Markieren Sie die Aktivität als potenziellen Ransomware-Angriff.
Unbestimmt	Ergreifen Sie keine sofortigen Maßnahmen. Überwachen Sie den Speicher bis zu 7 Tage lang. Wenn der Speicher weiterhin normal funktioniert, markieren Sie die Aktivität als falsch positiv. Wenn der Speicher weiterhin ungewöhnliche Aktivitäten aufweist, markieren Sie die Aktivität als potenziellen Ransomware-Angriff.

Schritte

1. Wählen Sie in System Manager **Dashboard** aus.

   Wenn ARP auf einer oder mehreren Speichereinheiten eine ungewöhnliche Aktivität festgestellt hat, wird unter **Warnungen** eine Meldung angezeigt.

2. Wählen Sie die Warnmeldung aus.
3. Wählen Sie unter **Ereignisübersicht** die Meldung **Warnungen** aus, die die Anzahl der Speichereinheiten mit abnormaler Aktivität angibt.
4. Wählen Sie unter **Speichereinheiten mit ungewöhnlicher Aktivität** die Speichereinheit aus.
5. Wählen Sie **Sicherheit**.

Bei ungewöhnlichen Aktivitäten auf dem Speichergerät wird unter **Anti-Ransomware** eine Meldung angezeigt.

6. Wählen Sie **Aktion auswählen**.
7. Wählen Sie **Als falsch-positiv markieren** oder **Als potenziellen Ransomware-Angriff markieren**.

Was kommt als Nächstes?

Wenn Sie in Ihrer Speichereinheit Aktivitätsspitzen feststellen, entweder einmalige Spitzen oder eine Spitze, die für eine neue Normalität charakteristisch ist, sollten Sie diese als unbedenklich melden. Das manuelle Melden dieser Spitzen als unbedenklich trägt dazu bei, die Genauigkeit der Bedrohungsbewertungen von ARP zu verbessern. Erfahren Sie, wie Sie "Bekannte ARP/AI-Spitzen melden".

Autonomen Ransomware-Schutz mit KI auf Ihren ASA R2-Speichersystemen pausieren oder fortsetzen

Ab ONTAP 9.17.1 können Sie Autonomous Ransomware Protection mit künstlicher Intelligenz (ARP/AI) nutzen, um die Daten auf Ihrem ASA r2-System zu schützen. Bei einem ungewöhnlichen Workload-Ereignis können Sie die ARP/AI-Analyse vorübergehend aussetzen, um Fehlalarme bei Ransomware-Angriffen zu verhindern. Nach Abschluss des Workload-Ereignisses können Sie die ARP/AI-Analyse fortsetzen.

ARP/AI pausieren

Bevor Sie mit einem ungewöhnlichen Workload-Ereignis beginnen, müssen Sie die ARP/AI-Analyse möglicherweise vorübergehend aussetzen, um falsch positive Erkennungen von Ransomware-Angriffen zu verhindern.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die Speichereinheiten aus, für die Sie ARP/AI pausieren möchten.
3. Wählen Sie **Anti-Ransomware pausieren**.

Ergebnis

Die ARP/AI-Analyse wird für die ausgewählten Speichereinheiten angehalten und Ihnen werden im System Manager keine verdächtigen Aktivitäten gemeldet, bis Sie ARP/AI wieder aufnehmen.

ARP/AI fortsetzen

Wenn Sie ARP/AI während einer ungewöhnlichen Arbeitslast anhalten, sollten Sie es nach Abschluss der Arbeitslast fortsetzen, um Ihre Daten vor Ransomware-Angriffen zu schützen.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die Speichereinheiten aus, für die Sie ARP/AI fortsetzen möchten.
3. Wählen Sie **Anti-Ransomware fortsetzen**.

Ergebnis

Die Analyse potenzieller Ransomware-Angriffe wird fortgesetzt und verdächtige Aktivitäten werden Ihnen im System Manager gemeldet.