Datensicherung

ASA r2

NetApp
February 01, 2026

This PDF was generated from https://docs.netapp.com/de-de/asa-r2/secure-data/encrypt-data-at-rest.html on February 01, 2026. Always check docs.netapp.com for the latest.

Inhalt

Datensicherung . . . 1
Verschlüsselung von Daten im Ruhezustand auf ASA r2 Storage-Systemen . . . 1
Migrieren Sie die ONTAP Datenverschlüsselung zwischen Schlüsselmanagern in Ihrem ASA r2 System . . . 2
Migrieren Sie Schlüssel zwischen Schlüsselmanagern auf ONTAP-Cluster-Ebene . . . 2
Schlüsselmanagement auf ONTAP-Cluster- und Storage-VM-Ebene migrieren . . . 4
Schutz vor Ransomware-Angriffen . . . 4
Erstellen Sie manipulationssichere Snapshots zum Schutz vor Ransomware-Angriffen auf ASA R2-Speichersysteme . . . 4
Aktivieren Sie autonomen Ransomware-Schutz mit KI auf Ihren ASA R2-Speichersystemen . . . 5
Deaktivieren Sie den standardmäßigen autonomen Ransomware-Schutz auf Ihren ASA r2-Speichersystemen . . . 7
Ändern Sie die Aufbewahrungsfristen für ARP/AI-Snapshots auf ASA R2-Speichersystemen . . . 8
Reagieren Sie auf autonomen Ransomware-Schutz mit KI-Warnungen auf ASA R2-Speichersystemen . . . 9
Autonomen Ransomware-Schutz mit KI auf Ihren ASA R2-Speichersystemen pausieren oder fortsetzen . . . 10
Sichere NVMe-Verbindungen auf Ihren ASA r2 Storage-Systemen . . . 11
Sichere IP-Verbindungen auf Ihren ASA r2-Storage-Systemen . . . 11

Datensicherung

Verschlüsselung von Daten im Ruhezustand auf ASA r2 Storage-Systemen

Wenn Daten im Ruhezustand verschlüsselt werden, sind sie auch dann nicht lesbar, wenn ein Storage-Medium einem anderen Zweck zugewiesen, zurückgegeben, verlegt oder gestohlen wird. Sie können ONTAP System Manager zur Verschlüsselung Ihrer Daten auf Hardware- und Softwareebene für einen Dual-Layer-Schutz verwenden.

NetApp Storage Encryption (NSE) unterstützt Hardwareverschlüsselung über Self-Encrypting Drives (SEDs). SEDs verschlüsseln Daten beim Schreiben. Jede SED enthält einen eindeutigen Verschlüsselungsschlüssel. Verschlüsselte Daten, die auf der SED gespeichert sind, können ohne den SED-Verschlüsselungsschlüssel nicht gelesen werden. Knoten, die versuchen, von einer SED zu lesen, müssen authentifiziert werden, um auf den Verschlüsselungsschlüssel der SED zuzugreifen. Knoten werden authentifiziert, indem ein Authentifizierungsschlüssel von einem Schlüsselmanager abgerufen und dann der SED den Authentifizierungsschlüssel vorgelegt wird. Wenn der Authentifizierungsschlüssel gültig ist, gibt die SED dem Knoten seinen Verschlüsselungsschlüssel für den Zugriff auf die darin enthaltenen Daten.

> In ASA r2-Systemen werden SEDs nur für NVMe-basierte SSDs unterstützt.

Verwenden Sie den integrierten Schlüsselmanager von ASA r2 oder einen externen Schlüsselmanager, um Ihren Nodes Authentifizierungsschlüssel bereitzustellen.

Neben NSE können Sie auch Softwareverschlüsselung aktivieren, um Ihre Daten um eine weitere Sicherheitsebene zu erweitern.

Schritte

1. Wählen Sie im System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** unter **Verschlüsselung Konfigurieren** aus.
3. Konfigurieren Sie den Schlüsselmanager.

Option	Schritte
Konfigurieren Sie den Onboard Key Manager	a. Wählen Sie **Onboard Key Manager**, um die Schlüsselserver hinzuzufügen. b. Geben Sie eine Passphrase ein.
Konfigurieren Sie einen externen Schlüsselmanager	a. Wählen Sie **External Key Manager**, um die Schlüsselserver hinzuzufügen. b. Wählen Sie + Add diese Option aus, um die Schlüsselserver hinzuzufügen. c. Fügen Sie die CA-Zertifikate des KMIP-Servers hinzu. d. Fügen Sie die KMIP-Client-Zertifikate hinzu.

4. Wählen Sie **Dual-Layer-Verschlüsselung**, um die Softwareverschlüsselung zu aktivieren.

5. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Nachdem Sie nun Ihre Daten im Ruhezustand verschlüsselt haben, können Sie jetzt mit dem "Verschlüsseln Sie alle über das Netzwerk gesendeten Daten"NVMe-/TCP-Protokoll zwischen Ihrem NVMe-/TCP-Host und Ihrem ASA r2-System wechseln.

Migrieren Sie die ONTAP Datenverschlüsselung zwischen Schlüsselmanagern in Ihrem ASA r2 System

Sie können Ihre Datenschlüssel entweder über den integrierten ONTAP Schlüsselmanager auf Ihrem ASA r2 System oder über einen externen Schlüsselmanager (oder beides) managen. Externe Schlüsselmanager können nur auf Ebene der Storage-VM aktiviert werden. Auf ONTAP Cluster-Ebene können Sie entweder den Onboard-Schlüsselmanager oder einen externen Schlüsselmanager aktivieren.

Wenn Sie Ihren Schlüsselmanager im…	Sie können…
Nur Cluster-Ebene	Entweder dem Onboard-Schlüsselmanager oder einem externen Schlüsselmanager
Nur auf Speicher-VM-Ebene	Nur ein externer Schlüsselmanager
Sowohl auf Cluster- als auch auf Speicher-VM-Ebene	Eine der folgenden Kombinationen von Schlüsselmanagern: • Option 1 Cluster-Ebene: Onboard-Schlüsselmanager Speicher-VM-Ebene: Externer Schlüsselmanager • Option 2 Cluster-Ebene: Externer Schlüsselmanager Speicher-VM-Ebene: Externer Schlüsselmanager

Migrieren Sie Schlüssel zwischen Schlüsselmanagern auf ONTAP-Cluster-Ebene

Ab ONTAP 9.16.1 können Sie die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, um Schlüssel zwischen Schlüsselmanagern auf Cluster-Ebene zu migrieren.

Von Onboard zu extern

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Erstellen Sie eine inaktive externe Schlüsselmanager-Konfiguration:

```
security key-manager external create-config
```

3. Wechseln Sie zum externen Schlüsselmanager:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type KMIP
```

4. Löschen Sie die Onboard-Schlüsselmanager-Konfiguration:

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type OKM
```

5. Legen Sie die Berechtigungsebene auf admin fest:

```
set -privilege admin
```

Von extern zu Onboard

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Erstellen einer inaktiven Onboard-Schlüsselmanager-Konfiguration:

```
security key-manager onboard create-config
```

3. Aktivieren der Onboard-Konfiguration für Verschlüsselungsmanagement:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type OKM
```

4. Löschen Sie die externe Schlüsselmanager-Konfiguration

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type KMIP
```

5. Legen Sie die Berechtigungsebene auf admin fest:

```
set -privilege admin
```

Schlüsselmanagement auf ONTAP-Cluster- und Storage-VM-Ebene migrieren

Mithilfe der ONTAP Befehlszeilenschnittstelle (CLI) können Sie Schlüssel zwischen dem Schlüsselmanager auf Cluster-Ebene und einem Schlüsselmanager auf Storage-VM-Ebene migrieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Migrieren der Schlüssel:

```
security key-manager key migrate -from-vserver <storage_vm_name> -to
-vserver <storage_vm_name>
```

3. Legen Sie die Berechtigungsebene auf admin fest:

```
set -privilege admin
```

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
Als potenziellen Ransomware-Angriff markieren	7 Tage

Wenn Sie diese Aktion ausführen …	ARP-Snapshots werden standardmäßig aufbewahrt für…
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.

Sichere NVMe-Verbindungen auf Ihren ASA r2 Storage-Systemen

Bei Verwendung des NVMe-Protokolls können Sie die in-Band-Authentifizierung konfigurieren, um die Datensicherheit zu erhöhen. Die in-Band-Authentifizierung ermöglicht eine sichere bidirektionale und unidirektionale Authentifizierung zwischen den NVMe Hosts und dem ASA r2 System. Die in-Band-Authentifizierung ist für alle NVMe-Hosts verfügbar. Bei Verwendung des NVMe/TCP-Protokolls können Sie die Datensicherheit weiter erhöhen, indem Sie TLS (Transport Layer Security) für die Verschlüsselung aller Daten konfigurieren, die zwischen Ihren NVMe/TCP-Hosts und Ihrem ASA r2-System über das Netzwerk übertragen werden.

Schritte

1. Wählen Sie **Hosts** aus, und wählen Sie dann **NVMe** aus.
2. Wählen Sie + Add .
3. Geben Sie den Hostnamen ein, und wählen Sie dann das Host-Betriebssystem aus.
4. Geben Sie eine Hostbeschreibung ein, und wählen Sie dann die Speicher-VM aus, die mit dem Host verbunden werden soll.
5. Wählen Sie ⌄ neben dem Hostnamen aus.
6. Wählen Sie **bandinterne Authentifizierung** aus.
7. Wenn Sie das NVMe/TCP-Protokoll verwenden, wählen Sie **benötigt Transport Layer Security (TLS)** aus.
8. Wählen Sie **Hinzufügen**.

Ergebnis

Die Sicherheit Ihrer Daten wird durch die in-Band-Authentifizierung und/oder TLS erhöht.

Sichere IP-Verbindungen auf Ihren ASA r2-Storage-Systemen

Wenn Sie das IP-Protokoll auf Ihrem ASA r2-System verwenden, können Sie die IP-Sicherheit (IPsec) konfigurieren, um Ihre Datensicherheit zu erhöhen. IPsec ist ein Internetstandard, der Verschlüsselung von Daten während der Übertragung, Authentifizierung für den Datenverkehr zwischen den Netzwerkendpunkten auf IP-Ebene und Schutz vor Replay- und böswilligen man-in-the-Middle-Angriffen auf Ihre Daten bietet.

Für ASA r2-Systeme ist IPsec für iSCSI- und NVMe/TCP-Hosts verfügbar.

Auf bestimmten ASA r2-Systemen können mehrere kryptografische Vorgänge, wie z. B. Verschlüsselungs- und Integritätsprüfungen, auf eine unterstützte NIC-Karte (Network Interface Controller) ausgelagert werden. Der Durchsatz für auf die NIC-Karte ausgelagerte Vorgänge beträgt etwa 5 % oder weniger. Dies kann die Leistung und den Durchsatz des durch IPsec geschützten Netzwerkverkehrs erheblich verbessern.

Ab ONTAP 9.18.1 wird die Unterstützung für IPsec-Hardware-Offloading auf IPv6-Datenverkehr erweitert.

Die folgenden Netzwerkkarten werden für die Hardware-Auslagerung auf den folgenden ASA r2-Systemen und ONTAP Versionen unterstützt:

Unterstützte NIC-Karte	ASA r2-Systeme	ONTAP -Version
X50135A (2p, 40G/100G Ethernet-Controller)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.17.1 und höher
X60135A (2p, 40G/100G Ethernet-Controller)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.17.1 und höher
X50131A – (2P, 40 G/100 G/200 G/400 G Ethernet-Controller)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.16.1 und höher
X60132A – (4p, 10G/25G Ethernet-Controller)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 und höher

Siehe die"NetApp Hardware Universe" Weitere Informationen zu den unterstützten Systemen und Karten finden Sie hier.

Was kommt als Nächstes?

IPsec wird auf Ihrem ASA r2-System auf die gleiche Weise konfiguriert wie auf anderen ONTAP -Systemen. Weitere Informationen finden Sie unter "Bereiten Sie die Konfiguration der IP-Sicherheit für das ONTAP Netzwerk vor.".

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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