ARP/AI aktivieren

ONTAP 9

NetApp
September 09, 2026

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

Inhalt

ARP/AI aktivieren . . . 1
ONTAP ARP/AI auf einem Volume aktivieren . . . 1
ARP/AI auf NAS FlexVol Volumes aktivieren . . . 2
ARP/AI auf NAS FlexGroup Volumes aktivieren . . . 2
ARP/AI auf SAN Volumes aktivieren . . . 3
Verwandte Informationen . . . 4
ONTAP ARP/AI ist in neuen Volumes standardmäßig aktiviert . . . 4
Automatische Aktivierung von ONTAP ARP/AI während Upgrades verwalten . . . 6

ARP/AI aktivieren

ONTAP ARP/AI auf einem Volume aktivieren

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

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

Über diese Aufgabe

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

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

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

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

Bevor Sie beginnen

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

NAS-spezifische Anforderungen

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

SAN-spezifische Anforderungen

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

Allgemeine Anforderungen

- Die "korrekte Lizenz" für Ihre ONTAP Version.
- (Empfohlen) Multi-Admin-Verifizierung (MAV) aktiviert (ONTAP 9.13.1 und höher). Siehe "Multi-Admin-Verifizierung aktivieren".

ARP/AI auf NAS FlexVol Volumes aktivieren

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

System Manager

1. **Storage > Volumes** auswählen und dann das Volume auswählen, das geschützt werden soll.
2. Im Tab **Sicherheit** der **Volumes**-Übersicht **Status** auswählen, um von Deaktiviert auf Aktiviert zu wechseln.
3. Der ARP/AI-Status des Volumes im **Anti-ransomware**-Feld kann überprüft werden.

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

CLI

ARP/AI auf einem vorhandenen Volume aktivieren:

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

Neues Volume mit aktiviertem ARP/AI erstellen:

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

Den ARP/AI-Status überprüfen:

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

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

ARP/AI auf NAS FlexGroup Volumes aktivieren

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

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

System Manager

1. **Speicher > Volumes** auswählen und dann das FlexGroup Volume auswählen, das geschützt werden soll.
2. Im Tab **Sicherheit** der **Volumes**-Übersicht **Status** auswählen, um von Deaktiviert auf Aktiviert zu wechseln.
3. Der ARP/AI-Status des Volumes im **Anti-ransomware**-Feld kann überprüft werden.

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

CLI

ARP/AI auf einem vorhandenen FlexGroup Volume aktivieren:

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

Ein neues FlexGroup Volume mit aktiviertem ARP/AI erstellen:

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

Den ARP/AI-Status überprüfen:

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

ARP/AI auf SAN Volumes aktivieren

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

System Manager

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

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

CLI

ARP/AI auf einem vorhandenen SAN Volume aktivieren:

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

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

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

Den ARP/AI-Status und den Auswertungsstatus überprüfen:

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

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

Verwandte Informationen

- "ARP/AI Entropieauswertungszeitraum für SAN Volumes"

ONTAP ARP/AI ist in neuen Volumes standardmäßig aktiviert

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

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

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

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

Über diese Aufgabe

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

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

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

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

Bevor Sie beginnen

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

NAS-spezifische Anforderungen

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

SAN-spezifische Anforderungen

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

Allgemeine Anforderungen

- Die "korrekte Lizenz" für Ihre ONTAP Version.
- (Empfohlen) Multi-Admin-Verifizierung (MAV) aktiviert (ONTAP 9.13.1 und höher). Siehe "Multi-Admin-Verifizierung aktivieren".

Schritte

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

System Manager

1. **Speicher** oder **Cluster** (je nach Umgebung) auswählen, **Speicher-VMs** auswählen und die Speicher-VM auswählen, die die Volumes enthält, die mit ARP/AI geschützt werden sollen.
2. Navigieren Sie zum Tab **Einstellungen**. Unter **Sicherheit** die Kachel **Anti-ransomware** suchen und dann auswählen.

3. Aktivieren Sie das Kontrollkästchen, um Anti-Ransomware (ARP/AI) zu aktivieren. Aktivieren Sie das zusätzliche Kontrollkästchen, um ARP/AI auf allen geeigneten Volumes in der Storage-VM zu aktivieren.

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

CLI

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

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

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

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

Den ARP/AI-Status überprüfen

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

Verwandte Informationen

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

Automatische Aktivierung von ONTAP ARP/AI während Upgrades verwalten

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

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

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

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

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

Über diese Aufgabe

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

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

Schritte

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

System Manager

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

CLI

1. Status der automatischen Aktivierung prüfen:

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

2. Automatische Standardaktivierung für neue Volumes deaktivieren:

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

Verwandte Informationen

- "ARP/AI auf einem einzelnen Volume aktivieren"

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.