Enable ARP

ONTAP 9

NetApp
February 06, 2026

Table of Contents

Enable ARP

Enable ONTAP Autonomous Ransomware Protection on a volume

Beginning with ONTAP 9.10.1, you can enable Autonomous Ransomware Protection (ARP) on an existing volume or create a new volume and enable ARP from the beginning.

About this task

To enable ARP, follow the procedure that matches your environment after you ensure that your environment meets certain requirements:

- NAS with FlexVol volumes
- NAS with FlexGroup volumes
- SAN volumes

After you enable ARP, ARP might enter a transitional period depending on your environment and ONTAP version:

Volume type	ONTAP version	Behavior after enablement
NAS FlexGroup	ONTAP 9.18.1 and later	ARP/AI is active immediately with no learning period
	ONTAP 9.13.1 to 9.17.1	ARP starts in learning mode for 30 days
NAS FlexVol	ONTAP 9.16.1 and later	ARP/AI is active immediately with no learning period
	ONTAP 9.10.1 to 9.15.1	ARP starts in learning mode for 30 days
SAN volumes	ONTAP 9.17.1 and later	ARP/AI is active immediately, initiating an evaluation period to establish a suitable alert threshold before transitioning from an initial conservative threshold.

Before you begin

Before enabling ARP, ensure your environment has the following:

NAS-specific requirements

- A storage VM (SVM) with NFS or SMB (or both) protocol enabled.
- NAS workload with clients configured.
- An active junction path for the volume.

SAN-specific requirements

- A storage VM (SVM) with iSCSI, FC, or NVMe protocol enabled.
- SAN workload with clients configured.

General requirements

- The correct license for your ONTAP version.
- (Recommended) Multi-admin verification (MAV) enabled (ONTAP 9.13.1 and later). See Enable multi-admin verification.

Enable ARP on NAS FlexVol volumes

You can enable ARP on NAS FlexVol volumes using System Manager or the ONTAP CLI. The process differs based on your ONTAP version.

ONTAP 9.16.1 and later

Beginning with ONTAP 9.16.1, ARP/AI is active immediately with no learning period required.

System Manager

1. Select **Storage > Volumes**, then select the volume you want to protect.
2. In the **Security** tab of the **Volumes** overview, select **Status** to switch from Disabled to Enabled.
3. Verify the ARP state of the volume in the **Anti-ransomware** box.

   To display ARP status for all volumes: In the **Volumes** pane, select **Show/Hide** then ensure that **Anti-ransomware** status is checked.

CLI

Enable ARP on an existing volume:

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

Create a new volume with ARP enabled:

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

Verify the ARP state:

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

Learn more about `security anti-ransomware volume show` in the ONTAP command reference.

ONTAP 9.10.1 to 9.15.1

For ONTAP 9.10.1 to 9.15.1, you should enable ARP initially in learning mode (or "dry-run" state). The system analyzes the workload to characterize normal behavior. Beginning in active mode can lead to excessive false positive reports.

It's recommended that you let ARP run in learning mode for a minimum of 30 days. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch, which might occur before 30 days.

System Manager

1. Select **Storage > Volumes**, then select the volume you want to protect.
2. In the **Security** tab of the **Volumes** overview, select **Status** to switch from Disabled to Enabled.
3. Select **Enabled in learning-mode** in the **Anti-ransomware** box.

You can disable automatic learning to active modes transitions on the associated storage VM if you want to control the learning to active mode transition manually.

In existing volumes, learning and active modes only apply to newly written data, not to already existing data in the volume. The existing data is not scanned and analyzed, because the characteristics of earlier normal data traffic are assumed based on the new data after the volume is enabled for ARP.

4. Verify the ARP state of the volume in the **Anti-ransomware** box.

   To display ARP status for all volumes: In the **Volumes** pane, select **Show/Hide** then ensure that **Anti-ransomware** status is checked.

CLI

Enable ARP on an existing volume:

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

Learn more about `security anti-ransomware volume dry-run` in the ONTAP command reference.

Create a new volume with ARP enabled:

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

Disable automatic switching (optional):

If you upgraded to ONTAP 9.13.1 through ONTAP 9.15.1 and want to manually control the switch from learning to active mode for all associated volumes, you can do this from the SVM:

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

Verify the ARP state:

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

Enable ARP on NAS FlexGroup volumes

You can enable ARP on NAS FlexGroup volumes using System Manager or the ONTAP CLI. The process differs based on your ONTAP version.

ONTAP 9.18.1 and later

Beginning with ONTAP 9.18.1, ARP/AI is active immediately for FlexGroup volumes with no learning period required.

System Manager

1. Select **Storage > Volumes**, then select the FlexGroup volume you want to protect.
2. In the **Security** tab of the **Volumes** overview, select **Status** to switch from Disabled to Enabled.
3. Verify the ARP state of the volume in the **Anti-ransomware** box.

   To display ARP status for all volumes: In the **Volumes** pane, select **Show/Hide** then ensure that **Anti-ransomware** status is checked.

CLI

Enable ARP on an existing FlexGroup volume:

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

Create a new FlexGroup volume with ARP enabled:

```
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>
```

Verify the ARP state:

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

ONTAP 9.13.1 to 9.17.1

For ONTAP 9.13.1 to 9.17.1, FlexGroup volumes start in learning mode. The system analyzes the workload to characterize normal behavior.

It's recommended that you let ARP run in learning mode for a minimum of 30 days. ARP automatically determines the optimal learning period interval and automates the switch, which might occur before 30 days.

System Manager

1. Select **Storage > Volumes**, then select the FlexGroup volume you want to protect.
2. In the **Security** tab of the **Volumes** overview, select **Status** to switch from Disabled to Enabled.
3. Select **Enabled in learning-mode** in the **Anti-ransomware** box.

> You can disable automatic learning to active modes transitions if you want to control the learning to active mode transition manually.

4. Verify the ARP state of the volume in the **Anti-ransomware** box.

CLI

Enable ARP on an existing FlexGroup volume:

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

Create a new FlexGroup volume with ARP enabled:

```
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>
```

Disable automatic switching (optional):

If you want to manually control the switch from learning to active mode:

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

Verify the ARP state:

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

Enable ARP on SAN volumes

Beginning with ONTAP 9.17.1, you can enable ARP on SAN volumes. ARP/AI functionality is automatically enabled and immediately begins actively monitoring and protecting SAN volumes during the evaluation period while simultaneously determining if the workloads are suitable for ARP and setting an optimal encryption threshold for detection.

You can enable ARP on SAN volumes using System Manager or the ONTAP CLI.

System Manager

Steps

1. Select **Storage > Volumes**, then select the SAN volume you want to protect.
2. In the **Security** tab of the **Volumes** overview, select **Status** to switch from Disabled to Enabled.
3. ARP/AI automatically enters the evaluation period.
4. Verify the ARP state and evaluation status in the **Anti-ransomware** box.

   To display ARP status for all volumes: In the **Volumes** pane, select **Show/Hide** then ensure that **Anti-ransomware** status is checked.

CLI

Enable ARP on an existing SAN volume:

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

Create a new SAN volume with ARP enabled:

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

Verify the ARP state and evaluation status:

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

Check the `Block device detection status` field to monitor the evaluation period progress.

Learn more about `security anti-ransomware volume show` in the ONTAP command reference.

Related information

- Switch to active mode after a learning period

Enable ONTAP Autonomous Ransomware Protection by default in new volumes

Beginning with ONTAP 9.10.1, you can configure storage VMs (SVMs) so that new volumes are enabled by default with Autonomous Ransomware Protection (ARP). You can modify this setting using System Manager or with the ONTAP CLI.

Beginning with ONTAP 9.18.1, ARP is enabled by default on all new volumes at the cluster level for supported systems after a 12-hour grace period following a cluster upgrade or new installation. If you disable automatic

default enablement of ARP at the cluster level, you can still choose to manually enable ARP by default on all new volumes at the SVM level.

For ONTAP 9.17.1 and earlier, configuration at the SVM level is the only way to enable ARP by default on new volumes.

About this task

By default, new volumes are created with ARP functionality disabled. You'll need to enable ARP functionality and set it to be enabled by default on new volumes created in the SVM.

Existing volumes without ARP enabled will not change ARP enablement status automatically when you change the default for the SVM. The SVM setting changes described in this procedure only affect new volumes. Learn how to enable ARP for existing volumes.

After you enable ARP, ARP might enter a transitional period depending on your environment and ONTAP version:

Volume type	ONTAP version	Behavior after enablement
NAS FlexGroup	ONTAP 9.18.1 and later	ARP/AI is active immediately with no learning period
	ONTAP 9.13.1 to 9.17.1	ARP starts in learning mode for 30 days
NAS FlexVol	ONTAP 9.16.1 and later	ARP/AI is active immediately with no learning period
	ONTAP 9.10.1 to 9.15.1	ARP starts in learning mode for 30 days
SAN volumes	ONTAP 9.17.1 and later	ARP/AI is active immediately, initiating an evaluation period to establish a suitable alert threshold before transitioning from an initial conservative threshold.

Before you begin

Before enabling ARP, ensure your environment has the following:

NAS-specific requirements

- A storage VM (SVM) with NFS or SMB (or both) protocol enabled.
- An active junction path for the volume.

SAN-specific requirements

- A storage VM (SVM) with iSCSI, FC, or NVMe protocol enabled.

General requirements

- The correct license for your ONTAP version.
- (Recommended) Multi-admin verification (MAV) enabled (ONTAP 9.13.1+). See Enable multi-admin verification.

Steps

You can use System Manager or the ONTAP CLI to enable ARP by default on new volumes.

System Manager

1. Select **Storage** or **Cluster** (depending on your environment), select **Storage VMs**, and select the storage VM that will contain volumes you want to protect with ARP.
2. Navigate to the **Settings** tab. Under **Security**, locate the **Anti-ransomware** tile then select .
3. Check the box to enable anti-ransomware (ARP). Check the additional box to enable ARP on all eligible volumes in the storage VM.
4. For ONTAP versions with a recommended learning period, select **Switch automatically from learning to active mode after sufficient learning**. This allows ARP to determine the optimal learning period interval and automate the switch to active mode.

CLI

Modify an existing SVM to enable ARP by default in new volumes

Select `dry-run` if your version of ARP requires a learning period. Otherwise, select `enabled`.

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

Create a new SVM with ARP enabled by default for new volumes

Select `dry-run` if your version of ARP requires a learning period. Otherwise, select `enabled`.

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

Modify existing SVM to disable automatic learning to active mode transition

If you upgraded to ONTAP 9.13.1 through ONTAP 9.15.1 and the default state is `dry-run` (learning mode), adaptive learning is enabled so that the change to `enabled` state (active mode) is done automatically. You can disable this automatic switch so that you can manually control the switch from learning to active mode for all associated volumes:

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

Verify the ARP state

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

Related information

- Switch to active mode after a learning period
- security anti-ransomware volume show

Opt out of ONTAP Autonomous Ransomware Protection default enablement

Beginning with ONTAP 9.18.1, Autonomous Ransomware Protection (ARP) is automatically enabled by default on all new volumes for AFF A-series and AFF C-series, ASA, and ASA r2 systems after a 12-hour warmup period following an upgrade or new installation, provided an ARP license is installed. You can opt out of this default enablement during or after the 12-hour grace period using System Manager or the ONTAP CLI.

Existing volumes must be manually enabled for ARP.

About this task

The setting you choose for this procedure can be changed later. After the grace period, you always have the flexibility to turn on or turn off default enablement at any time:

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

Steps

You can use System Manager or the ONTAP CLI to manage ARP default enablement options.

System Manager

1. Select **Cluster > Settings**.
2. Do one of the following:
   - Disable during active grace period:
     a. In the **Anti-ransomware** section, you'll see a message indicating the hours remaining before ARP will be enabled. Select **Don't enable**.
     b. Select **Disable** in the next dialog box to confirm that default ARP enablement is turned off for new volumes.
   - Disable after grace period:
     a. In the **Anti-ransomware** section, select  .
     b. Select the checkbox and then **Save** to disable default ARP enablement for new volumes.

CLI

1. Check the default enablement status:

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

2. Disable default enablement for new volumes:

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

Related information

- Enable ONTAP Autonomous Ransomware Protection on an individual volume

Copyright information

Trademark information