Autonomous Ransomware Protection

ONTAP 9

NetApp
February 06, 2026

Table of Contents

Autonomous Ransomware Protection

Learn about ONTAP Autonomous Ransomware Protection

Beginning with ONTAP 9.10.1, ONTAP administrators can enable Autonomous Ransomware Protection (ARP) to perform workload analysis in NAS (NFS and SMB) environments to proactively detect and warn about abnormal activity that might indicate a ransomware attack. Beginning with ONTAP 9.17.1, ARP also supports block-device volumes, including SAN volumes containing LUNs or NVMe namespaces, or NAS volumes containing virtual disks from hypervisors such as VMware.

ARP is built directly into ONTAP, ensuring integrated control and coordination with ONTAP's other features. ARP operates in real-time, processing data as it's written to or read from the file system, and detecting and responding to potential ransomware attacks quickly.

ARP creates locked snapshots at regular intervals alongside scheduled ones for added protection. It smartly manages how long snapshots are kept. If no unusual activity is detected, snapshots are quickly recycled. However, if an attack is detected, a snapshot created before the start of an attack is kept for an extended period. For more information, including changes added by ONTAP version, see ARP snapshots.

Licenses and enablement

You need a license to use ARP. Decide whether to enable ARP by default on new volumes or enable it manually per volume.

License options for ARP

ARP support is included with the ONTAP One license. If you do not have the ONTAP One license, other licenses are available for ARP use that differ depending on your version of ONTAP.

ONTAP releases	License
ONTAP 9.11.1 and later	`Anti_ransomware`
ONTAP 9.10.1	`MT_EK_MGMT` (Multi-Tenant Key Management)

- If you are upgrading from ONTAP 9.10.1 to ONTAP 9.11.1 or later and ARP is already configured on your system, you do not need to install the new `Anti-ransomware` license. For new ARP configurations, the new license is required.
- If you are reverting from ONTAP 9.11.1 or later to ONTAP 9.10.1, and you have enabled ARP with the Anti_ransomware license, you will see a warning message and might need to reconfigure ARP. Learn about reverting ARP.

Enablement options for ARP

ARP provides flexible enablement options at the cluster, SVM, and volume levels, allowing you to configure automatic default enablement for new volumes or enable ARP manually on existing volumes as needed.

Automatic default enablement on new volumes

Beginning with ONTAP 9.18.1, ARP is enabled by default automatically on all new volumes for AFF A series and AFF C series, ASA, and ASA r2 systems. This automatic default ARP enablement does not apply to unsupported volumes or configurations.

ARP default enablement on new volumes goes into effect after a 12-hour grace period following an upgrade or immediately for a new ONTAP 9.18.1 installation, provided that an ARP license is installed in either case. You must enable ARP manually on existing volumes.

During the grace period, you can opt out of default enablement for new volumes at the cluster level using System Manager or the ONTAP CLI. If you do not opt out, ARP is automatically enabled for all new volumes created after the end of the grace period. If needs change after the grace period, you also have the flexibility to turn on or turn off default enablement at any time.

Manual default enablement on new volumes

If you disabled automatic default enablement of ARP at the cluster level, you can also choose to manually enable ARP by default on all new volumes at the SVM level. For ONTAP 9.17.1 and earlier, this is the only way to configure ARP to be enabled by default on new volumes.

ARP enablement on all or specific existing volumes

Beginning with 9.18.1, you can manually enable ARP on all existing volumes from the cluster level (select **Cluster > Security** and ⋮ in the **Anti-ransomware** section then select **Enable on all existing volumes**).

If you'd prefer to limit ARP enablement to a specific volume, you can enable ARP on a per-volume basis.

ONTAP ransomware protection strategy

Effective ransomware protection requires many layers of protection working together.

While ONTAP includes features like FPolicy, snapshots, SnapLock, and Active IQ Digital Advisor (also known as Digital Advisor) to help protect from ransomware, ARP provides an additional layer of defense.

To learn more about other features in the NetApp portfolio that safeguard against ransomware, see:

- Ransomware and NetApp's protection portfolio
- ONTAP cyber vault hardening with PowerShell

What ARP detects

ONTAP ARP is designed to protect against denial-of-service attacks where the attacker withholds data until a ransom is paid. ARP offers real-time ransomware detection based on the following:

- Identification of incoming data as either encrypted or plain text.
- Analytics that detect:
    - **Entropy**: (Used in NAS and SAN) An evaluation of the randomness of data in a file
    - **File extension types**: (Used in NAS only) A file extension that does not conform to expected extension types
    - **File IOPS**: (Used in NAS only beginning with ONTAP 9.11.1) A surge in abnormal volume activity with data encryption

ARP detects the spread of most ransomware attacks after only a small number of files are encrypted, responds automatically to protect data, and alerts you that a suspected attack is happening.

ⓘ No ransomware detection system can guarantee complete safety. ARP provides an extra layer of defense if anti-virus software fails to detect an intrusion.

Learn about ARP modes

After ARP is enabled for a volume, it enters a learning period to establish a baseline. ARP analyzes system metrics to develop an alert profile before transitioning to active detection mode. In active mode, ARP monitors abnormal activity, taking protective actions and generating alerts if it detects abnormal behavior.

For ARP, the learning mode and active mode behaviors differ by ONTAP version, volume type, and protocol (NAS or SAN).

NAS environments and mode types

The following table summarizes the differences between ONTAP 9.10.1 and later versions for NAS environments.

In versions with the earlier ARP model, a learning period is recommended before active monitoring begins. For NAS environments that support ARP/AI, there is no learning period and active monitoring begins immediately.

Mode	Description	Volume types and versions
Learning	For certain versions of ONTAP and certain volume types, ARP is automatically set to learning mode when you enable ARP. In learning mode, the ONTAP system develops an alert profile based on the analytic areas: entropy, file extension types, and file IOPS. It's recommended that you leave ARP in learning mode for 30 days. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning interval and automates the switch, which might occur before 30 days. For versions earlier than ONTAP 9.13.1, you can make the switch manually. Beginning with ONTAP 9.16.1 for FlexVol volumes, only active mode exists and learning mode is transitioned automatically to active mode for any FlexVol volumes upgraded to this version or later. For ONTAP 9.16.1 to 9.17.1, FlexGroup volumes are not yet supported by ARP/AI and continue to run the older ARP model. Because of this, a learning period is still recommended for these versions with FlexGroup volumes. Beginning with ONTAP 9.18.1, only active mode exists for both FlexVol and FlexGroup volumes. Any upgraded volumes are transitioned to active mode automatically. Learn more about switching from learning to active mode. The command `security anti-ransomware volume workload-behavior show` shows file extensions that have been detected in the volume. If you run this command early in learning mode and it shows an accurate representation of file types, you should not use that data as a basis to move to active mode, as ONTAP is still collecting other metrics. Learn more about `security anti-ransomware volume workload-behavior show` in the ONTAP command reference.	• FlexVol volumes with ONTAP 9.10.1 to 9.15.1 • FlexGroup volumes with ONTAP 9.13.1 to ONTAP 9.17.1
Active	In active mode, if a file extension is flagged as abnormal, you should evaluate the alert. You can act on the alert to protect your data, or you can mark the alert as a false positive. Marking an alert as a false positive updates the alert profile. For example, if the alert is triggered by a new file extension and you mark the alert as a false positive, you will not receive an alert the next time that the file extension is observed.	All supported ONTAP versions and FlexVol and FlexGroup volumes

SAN environments and mode types

SAN environments use *evaluation* periods (similar to learning modes in NAS environments) before transitioning to active detection automatically. The following table summarizes evaluation and active modes.

Mode	Description	Volume types and versions
Evaluation	A two- to four-week evaluation period is performed to determine baseline encryption behavior while ARP/AI provides immediate active protection for SAN volumes during the evaluation period. Detection and alerts can occur while baseline thresholds are being established. You can determine if the evaluation period is complete by running the `security anti-ransomware volume show` command and checking `Block device detection status`. Learn more about SAN volumes and the entropy evaluation period.	• FlexVol volumes with ONTAP 9.17.1 and later
Active	After the evaluation period, you can determine if the ARP SAN protection is active by running the `security anti-ransomware volume show` command and checking `Block device detection status`. A status of `Active_suitable_workload` indicates that the evaluated amount of entropy can be successfully monitored. ARP automatically adjusts the adaptive threshold according to data reviewed during the evaluation.	• FlexVol volumes with ONTAP 9.17.1 and later

Threat assessment and ARP snapshots

ARP assesses threat probability based on incoming data measured against learned analytics. When ARP detects an abnormality, a measurement is assigned. ARP might assign a snapshot at the time of detection or at regular intervals.

ARP thresholds

- **Low**: The earliest detection of an abnormality in the volume (for example, a new file extension is observed in the volume). This level of detection is only available in versions prior to ONTAP 9.16.1 that do not have ARP/AI.
    - Beginning with ONTAP 9.11.1, you can customize the detection parameters for ARP.
    - In ONTAP 9.10.1, the threshold for escalation to moderate is 100 or more files.
- **Moderate**: High entropy is detected or multiple files with the same never-seen-before file extension are observed. This is the baseline detection level in ONTAP 9.16.1 and later with ARP/AI.

The threat escalates to moderate after ONTAP runs an analytics report determining if the abnormality matches a ransomware profile. When the attack probability is moderate, ONTAP generates an EMS notification prompting you to assess the threat. ONTAP does not send alerts about low threats; however, beginning with ONTAP 9.14.1, you can modify default alert settings. For more information, see Respond to abnormal activity.

You can view information about moderate threats in System Manager's **Events** section or with the `security anti-ransomware volume show` command. Low threat events can also be viewed using the `security anti-ransomware volume show` command in versions prior to ONTAP 9.16.1 that do not have ARP/AI. Learn more about `security anti-ransomware volume show` in the ONTAP command reference.

ARP snapshots

ARP creates a snapshot when early signs of an attack are detected. A detailed analysis is then conducted to confirm or dismiss the potential attack. Because ARP snapshots are created proactively even before an attack is fully confirmed, they might also be generated at regular intervals for certain legitimate applications. The presence of these snapshots should not be regarded as an anomaly. If an attack is confirmed, the attack probability is escalated to `Moderate` and an attack notification is generated.

Beginning with ONTAP 9.17.1, ARP snapshots are generated at regular intervals for both NAS and SAN volumes as well as in response to detected anomalies. ONTAP prepends a name to the ARP snapshot to make it easily identifiable.

Beginning with ONTAP 9.11.1, you can modify the retention settings. For more information, see Modify options for snapshots.

The following table summarizes ARP snapshot differences by version.

Feature	ONTAP 9.17.1 and later	ONTAP 9.16.1 and earlier
Creation trigger	• Snapshots are created at fixed 4-hour intervals, regardless of any specific trigger • Confirmation of an attack A "periodic" or "attack" snapshot is created based on trigger type.	• High entropy is detected • A new file extension is detected (9.15.1 and earlier) • A surge of file operations is detected (9.15.1 and earlier) Snapshot creation interval is based on trigger type.
Prepended name convention	"Anti_ransomware_periodic_backup" "Anti_ransomware_attack_backup"	"Anti_ransomware_backup"
Deletion behavior	ARP snapshot is locked and cannot be deleted by the administrator	ARP snapshot is locked and cannot be deleted by the administrator
Maximum snapshot count	Six snapshot configurable limit	Six snapshot configurable limit
Retention period	Snapshots are normally retained for 12 hours. • NAS volumes: If an attack is confirmed by file-analysis, snapshots created before the attack are retained until the administrator marks the attack as true or a false positive (clear-suspect). • SAN volume or VM datastores: If an attack is confirmed by block-entropy analysis, snapshots created before the attack are retained for 10 days (configurable).	• Determined based on trigger conditions (not fixed) • Snapshots created before the attack are retained until administrator marks the attack as true or a false positive (clear-suspect).

Feature	ONTAP 9.17.1 and later	ONTAP 9.16.1 and earlier
Clear-suspect action	Administrators can perform a clear-suspect action which sets retention based on confirmation: • 24 hours for false-positive retention • 7 days for true-positive retention	Administrators can perform a clear-suspect action which sets retention based on confirmation: • 24 hours for false-positive retention • 7 days for true-positive retention This precautionary retention behavior doesn't exist earlier than ONTAP 9.16.1
Expiration time	An expiration time is set for all snapshots	None

How to recover data in ONTAP after a ransomware attack

ARP builds on proven ONTAP data protection and disaster recovery technology to respond to ransomware attacks. ARP creates locked snapshots when early signs of an attack are detected. You'll need to first confirm whether the attack is real or a false positive. If you confirm the attack, the volume can be restored using the ARP snapshot.

Locked snapshots cannot be deleted by normal means. However, if you decide later to mark the attack as a false positive, ONTAP deletes the locked copy.

You can recover affected files from select snapshots instead of reverting the entire volume.

See the following topics for more information on responding to an attack and recovering data:

- Respond to abnormal activity
- Recover data from ARP snapshots
- Recover from ONTAP snapshots
- Smart ransomware recovery

Multi-admin verification protection for ARP

Beginning with ONTAP 9.13.1, it's recommended that you enable multi-admin verification (MAV) so that two or more authenticated user admins are required for Autonomous Ransomware Protection (ARP) configuration. For more information, see Enable multi-admin verification.

Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI)

Beginning with ONTAP 9.16.1, ARP improves cyber resiliency by adopting a machine-learning model for anti-ransomware analytics that detects constantly evolving forms of ransomware with 99% accuracy in NAS environments. ARP's machine-learning model is pre-trained on a large dataset of files both before and after a simulated ransomware attack. This resource-intensive training is done outside ONTAP using open-source forensic research datasets to train the model. Customer data is not used throughout the entire modelling pipeline and privacy issues do not exist. The pre-trained model that results from this training is included on-box with ONTAP. This model is not accessible or modifiable through the ONTAP CLI or ONTAP API.

Immediate transition to active protection for ARP/AI

With ARP/AI, there is no learning period. ARP/AI is active immediately after installation or upgrade for the following supported volume types:

- NAS FlexVol volumes with ONTAP 9.16.1 and later
- NAS FlexGroup volumes with ONTAP 9.18.1 and later
- SAN volumes with ONTAP 9.17.1 and later (active immediately, even during the evaluation period)

For existing and new volumes with ARP functionality already enabled, ARP/AI protection will be active automatically after you upgrade your cluster to an ARP/AI supported ONTAP version.

ARP/AI automatic updates

To keep up-to-date protection against the latest ransomware threats, ARP/AI offers frequent automatic updates that occur outside of regular ONTAP upgrade and release cadences. If you have enabled automatic updates then you will also be able to start receiving automatic security updates to ARP/AI after you select automatic updates for security files. You can also choose to make these updates manually and control when the updates occur.

Beginning with ONTAP 9.16.1, security updates for ARP/AI are available using System Manager in addition to system and firmware updates.

Learn more about ARP/AI updates

Differences between ARP/AI and ARP models at a glance

Feature	ARP	ARP/AI
ONTAP versions	ONTAP 9.10.1-9.15.1	ONTAP 9.16.1 and later; 9.15.1 (tech preview)
Detection method	Analyzes file activity, data entropy, and file extension types	AI/machine learning model trained on large forensic datasets; analyzes entropy and file behavior
Learning period	Requires 30-day learning mode for NAS FlexVol volumes (auto-switch available in 9.13.1 and later)	No learning period; active immediately upon enablement
Volume type support	• FlexVol: 9.10.1 and later • FlexGroup: 9.13.1 and later • SAN: Not supported	• FlexVol: 9.16.1 and later • FlexGroup: 9.18.1 and later • SAN: 9.17.1 and later (with evaluation period)
Snapshot creation	Triggered by high entropy, new file extensions, or file operation surges	Created at fixed 4-hour intervals and on attack confirmation
Snapshot retention	Retained until admin clears suspect activity	12-hour default; extended based on attack confirmation (24 hours for false positive, 7 days for confirmed positive)
Updates	Static detection logic (updated with ONTAP upgrades only)	Automatic security updates independent of ONTAP releases

Feature	ARP	ARP/AI
Deployment	Manual enablement per volume or SVM-level default setting	Manual enablement per volume or SVM-level default setting; default enablement on all new volumes at cluster level for supported systems in 9.18.1 and later
Evaluation period	Not applicable	Required for SAN volumes (2-4 weeks) to establish baseline encryption thresholds

Related information

- ONTAP command reference

ONTAP Autonomous Ransomware Protection use cases and considerations

Autonomous Ransomware Protection (ARP) is available for NAS workloads beginning with ONTAP 9.10.1 and SAN workloads beginning in ONTAP 9.17.1. Before deploying ARP, you should be aware of the recommended uses and supported configurations as well as performance implications.

Supported and unsupported configurations

When deciding to use ARP, it's important to ensure that your volume's workload is suited to ARP and that it meets required system configurations.

Suitable workloads

ARP is suited for these types of workloads:

- Databases on NFS or SAN storage
- Windows or Linux home directories

  For environments without ARP/AI, users could create files with extensions that aren't detected in the learning period. Because of this, there is a greater possibility of false positives in this workload.

- Images and video

  For example, health care records and Electronic Design Automation (EDA) data

Unsuitable workloads

ARP is not suited for these types of workloads:

- Workloads with a high frequency of file create or delete operations (hundreds of thousands of files in few seconds; for example, test/development workloads).
- ARP's threat detection depends on its ability to recognize an unusual surge in file create, rename, or delete operations. If the application itself is the source of the file activity, it cannot be effectively distinguished from ransomware activity.

- Workloads where the application or the host encrypts data.

  ARP depends on distinguishing incoming data as encrypted or unencrypted. If the application itself is encrypting the data, then the effectiveness of the feature is reduced. However, ARP can still work based on file activity (delete, overwrite, or create, or a create or rename with a new file extension) and file type.

Supported configurations

ARP is available for NAS NFS and SMB FlexVol volumes beginning with ONTAP 9.10.1. Beginning in 9.17.1, ARP is available for SAN FlexVol volumes for iSCSI, FC, and NVMe with SAN storage.

ARP is supported for MetroCluster configurations beginning with ONTAP 9.10.1.

Support for other configurations and volume types is available in the following ONTAP versions:

	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 protected with SnapMirror asynchronous	✓	✓	✓	✓	✓	✓	✓		
SVMs protected with SnapMirror asynchronous (SVM disaster recovery)	✓	✓	✓	✓	✓	✓	✓		
SVM data mobility (`vserver migrate`)	✓	✓	✓	✓	✓	✓	✓		
FlexGroup volumes[1]	✓	✓	✓	✓	✓	✓			
Multi-admin verification	✓	✓	✓	✓	✓				

	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
ARP/AI with automatic updates	✓	✓							
ARP/AI default enablement[2]	✓								

[1] ONTAP 9.16.1 and 9.17.1 do not provide ARP/AI support for FlexGroup volumes. After an upgrade to these versions, FlexGroup volumes enabled for ARP continue to operate with the same ARP model used prior to ARP/AI. Beginning in ONTAP 9.18.1, FlexGroup volumes use the ARP/AI model.

[2] Beginning with ONTAP 9.18.1, ARP/AI default enablement behavior is available for AFF A-series and AFF C-series, ASA, and ASA r2 systems. This behavior automatically enables ARP/AI on all new volumes after a 12-hour grace period following an upgrade or immediately for new ONTAP 9.18.1 installations. You'll need to manually enable ARP on existing volumes.

SnapMirror and ARP interoperability

Beginning with ONTAP 9.12.1, ARP is supported on SnapMirror asynchronous destination volumes. ARP is *not* supported with SnapMirror synchronous or SnapMirror active sync.

If a SnapMirror source volume is ARP-enabled, the SnapMirror destination volume automatically acquires the ARP configuration state (such as `dry-run` or `enabled`), ARP training data, and ARP-created snapshot of the source volume. No explicit enablement is required.

Although the destination volume consists of read-only (RO) snapshots, no ARP processing is done on its data. However, when the SnapMirror destination volume is converted to read-write (RW), ARP is automatically enabled on the RW-converted destination volume. The destination volume does not require any additional learning procedures besides what is already recorded on the source volume.

In ONTAP 9.10.1 and 9.11.1, SnapMirror does not transfer the ARP configuration state, training data, and snapshots from source to destination volumes. Because of this, when the SnapMirror destination volume is converted to RW, ARP on the destination volume must be explicitly enabled in learning mode after conversion.

ARP and virtual machines

ARP is supported with virtual machines (VMs) on VMware. ARP detection behaves differently for changes inside and outside the VM. ARP is not recommended for workloads that involve a large number of highly compressed files (such as 7z and ZIP) or encrypted files (such as password-protected PDF, DOC, or ZIP) within the VM.

Changes outside the VM

ARP can detect file extension changes on an NFS volume outside of the VM if a new extension enters the volume in an encrypted state or if a file extension changes.

Changes inside the VM

If a ransomware attack changes files inside of the VM without making changes outside the VM, ARP detects the threat if the default entropy of the VM is low (for example, .txt, .docx, or .mp4 files). For ONTAP 9.16.1 and earlier, ARP creates a protective snapshot in this scenario but does not generate a threat alert because the file extensions outside of the VM have not been tampered with. Beginning with SAN support in ONTAP 9.17.1, ARP generates a threat alert additionally if it detects an entropy anomaly inside the VM.

If, by default, the files are high entropy (for example, .gzip or password-protected files), ARP’s detection capabilities are limited. ARP can still take proactive snapshots in this instance; however, no alerts will be triggered if the file extensions have not been tampered with externally.

For SAN, ARP analyzes entropy statistics at the volume level and triggers detections when an entropy anomaly is found.

> ⓘ Detection of attacks occurring within a VM is available only for FlexVol volumes and is not available if the VM datastore is configured on a FlexGroup volume in ONTAP 9.18.1 and later.

Unsupported configurations

ARP is not supported in ONTAP S3 environments.

ARP does not support the following volume configurations:

- FlexGroup volumes (in ONTAP 9.10.1 through 9.12.1).

  > ⓘ Beginning with ONTAP 9.13.1 to ONTAP 9.17.1, FlexGroup volumes are supported but are limited to the ARP model used prior to ARP/AI. FlexGroup volumes are supported with ARP/AI beginning in ONTAP 9.18.1.

- FlexCache volumes (ARP is supported on origin FlexVol volumes but not on cache volumes)
- Offline volumes
- SnapLock volumes
- SnapMirror active sync
- SnapMirror synchronous
- SnapMirror asynchronous (in ONTAP 9.10.1 and 9.11.1). SnapMirror asynchronous is supported beginning with ONTAP 9.12.1. For more information, see SnapMirror and ARP interoperability.
- Restricted volumes
- Root volumes of storage VMs
- Volumes of stopped storage VMs

ARP performance and frequency considerations

ARP can have a minimal impact on system performance as measured in throughput and peak IOPS. The impact of the ARP feature depends on the specific volume workload. For common workloads, the following configuration limits are recommended:

Workload characteristics	Recommended volume limit per node	Performance degradation when per-node volume limit is exceeded [1]
Read-intensive or the data can be compressed	150	4% of maximum IOPS

Workload characteristics	Recommended volume limit per node	Performance degradation when per-node volume limit is exceeded [1]
Write-intensive and the data cannot be compressed	60	• NAS: 10% of maximum IOPS for ONTAP 9.15.1 and earlier • NAS: 5% of maximum IOPS for ONTAP 9.16.1 and later • SAN: 5% of maximum IOPS for ONTAP 9.17.1 and later

[1] System performance is not degraded beyond these percentages regardless of the number of volumes added in excess of the recommended limits.

Because ARP analytics run in a prioritized sequence, analytics run on each volume less frequently as the number of protected volumes increases.

ⓘ Enabling ARP by default on large numbers of new volumes might increase system resource usage. Consider space demands for competing processes like snapshots when enabling ARP on volumes.

Volume limits for ARP by platform

Beginning with ONTAP 9.18.1, ARP supports increased volume limits based on platform type and CPU core count.

Platform type	Maximum ARP-enabled volumes per node
Low-end (systems with up to 20 CPU cores)	250
Medium (systems with up to 64 CPU cores)	500
High-end (systems with more than 64 CPU cores)	1000

ⓘ The CPU core count applies to each individual node in a 2-node HA pair.

Multi-admin verification with volumes protected with ARP

Beginning with ONTAP 9.13.1, you can enable multi-admin verification (MAV) for additional security with ARP. MAV ensures that at least two or more authenticated administrators are required to turn off ARP, pause ARP, or mark a suspected attack as a false positive on a protected volume. Learn how to enable MAV for ARP-protected volumes.

You need to define administrators for a MAV group and create MAV rules for the `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, and `security anti-ransomware volume attack clear-suspect` ARP commands you want to protect. Each administrator in the MAV group must approve each new rule request and add the MAV rule again within MAV settings.

Learn more about `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, and `security anti-ransomware volume attack clear-suspect` in the ONTAP command reference.

Beginning with ONTAP 9.14.1, ARP offers alerts for the creation of an ARP snapshot and for the observation of a new file extension. Alerts for these events are disabled by default. Alerts can be set at the volume or SVM level. You can enable the alerts using `security anti-ransomware vserver event-log modify` or at the volume level with `security anti-ransomware volume event-log modify`.

Learn more about `security anti-ransomware vserver event-log modify` and `security anti-ransomware volume event-log modify` in the ONTAP command reference.

Next steps

- Enable Autonomous Ransomware Protection
- Enable MAV for ARP-protected volumes

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

Switch to active mode in ONTAP ARP after a learning period

For NAS environments, manually or automatically switch an ARP-enabled volume from learning mode to active mode. You'll need to switch modes if you are using ARP with ONTAP 9.15.1 and earlier or if ARP is running on FlexGroup volumes with ONTAP 9.17.1 and earlier.

After ARP has completed a learning mode run of a recommended minimum of 30 days you can manually switch to active mode. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch, which might occur before 30 days.

If you are using ARP with ARP/AI protection, ARP becomes active automatically. No learning period is required.

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.

Manually switch to active mode after learning period

For ONTAP 9.10.1 to 9.15.1 (ONTAP 9.17.1 and earlier with FlexGroup volumes), you can manually transition from ARP learning mode to active mode using System Manager or the ONTAP CLI after the learning period is complete.

About this task

The manual transition to active mode after a learning period described in this procedure is specific to NAS environments.

Steps

You can use System Manager or the ONTAP CLI to switch from learning mode to active mode.

System Manager

1. Select **Storage > Volumes** and then select the volume that is ready for active mode.
2. In the **Security** tab of the **Volumes** overview, select **Switch to active mode** in the Anti-ransomware box.
3. You can verify the ARP state of the volume in the **Anti-ransomware** box.

CLI

1. Modify the protected volume to switch to active mode if not already done automatically:

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

   You can also switch to active mode with the modify volume command:

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

2. Verify the ARP state of the volume.

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

Automatic switching from learning mode to active mode

Beginning with ONTAP 9.13.1, adaptive learning has been added to ARP analytics and the switch from learning mode to active mode is done automatically. The autonomous decision by ARP to automatically switch from learning mode to active mode is based on the configuration settings of the following options:

```
-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
```

If auto-switch is enabled, the volume will switch to active mode automatically after a maximum of 30 days, even if all conditions are not met. This 30-day limit is fixed and cannot be changed.

For more information on ARP configuration options, including default values, see the ONTAP command reference.

Related information

- security anti-ransomware volume

Learn about the ONTAP ARP evaluation period for SAN volumes

Beginning with ONTAP 9.17.1, ARP requires an evaluation period to determine if entropy levels for SAN volume workloads are suitable for ransomware protection. After ARP is enabled on a SAN volume, ARP/AI actively monitors and protects the volume during the evaluation period while simultaneously determining an optimal encryption threshold. Detection and alerts can occur during the evaluation period using a conservative threshold while baseline thresholds are being established. ARP distinguishes between suitable and unsuitable workloads in the evaluated SAN volume and, if the workloads are determined to be suitable for protection, automatically sets an encryption threshold based on evaluation period statistics.

Understand entropy evaluation

The system collects continuous encryption statistics in 10-minute intervals. During the evaluation, ARP periodic snapshots are also continuously created every four hours. If the encryption percentage within an interval exceeds the optimal encryption threshold identified for this volume, an alert is triggered, an `Anti_ransomware_attack_backup` snapshot is created, and snapshot retention time is increased on any periodic ARP snapshots.

Confirm that the evaluation period is active

You can confirm that the evaluation is active by running the following command and confirming a status of `evaluation_period`. If a volume is not eligible for evaluation, the evaluation status will not be displayed.

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

Example response:

```
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
```

Monitor evaluation period data collection

You can monitor encryption detection in real time by running the following command. The command returns a histogram showing the amount of data in each encryption percentage range. The histogram is updated every 10 minutes.

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

Example response:

```
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.
```

Suitable workloads and adaptive thresholds

The evaluation ends with one of the following results:

- **The workload is suitable for ARP**. ARP automatically sets the adaptive threshold to higher than 10% of the maximum encryption percentage seen during the evaluation period. ARP also continues statistics collection and creates periodic ARP snapshots.
- **The workload is unsuitable for ARP**. ARP automatically sets the adaptive threshold to the maximum encryption percentage seen during the evaluation period. ARP also continues statistics collection and creates periodic ARP snapshots, but the system ultimately recommends disabling ARP on the volume.

Determine evaluation results

After the evaluation period ends, ARP automatically sets the adaptive threshold based on the evaluation results.

You can determine the evaluation results by running the following command. Volume suitability is indicated in the `Block device detection status` field:

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

Example response:

```
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
```

You can also show the value threshold adopted as a result of the evaluation:

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

Example response:

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

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

Pause ONTAP Autonomous Ransomware Protection to exclude workload events from analysis

If you are expecting unusual workload events, you can temporarily suspend and resume Autonomous Ransomware Protection (ARP) analysis at any time.

Beginning with ONTAP 9.13.1, you can enable multi-admin verification (MAV) so that two or more authenticated user admins are required to pause the ARP.

Learn more about MAV.

About this task

During an ARP pause, ONTAP does not log events or actions for new writes; however, analytics continue for earlier logs in the background.

> Do not use the ARP disable function to pause analytics. Doing so disables ARP on the volume and all the existing information around learned workload behavior is lost. This would require a restart of the learning period.

Steps

You can use System Manager or the ONTAP CLI to pause ARP.

System Manager

1. Select **Storage > Volumes** and then select the volume where you want to pause ARP.
2. In the **Security** tab of the Volumes overview, select **Pause anti-ransomware** in the **Anti-ransomware** box.

   > ⓘ Beginning with ONTAP 9.13.1, if you are using MAV to protect ARP settings, the pause operation prompts you to obtain the approval of one or more additional administrators. Approval must be received from all administrators associated with the MAV approval group or the operation will fail.

3. To resume monitoring, select **Resume anti-ransomware**.

CLI

1. Pause ARP on a volume:

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

2. To resume processing, use the `resume` command:

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

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

3. If you are using MAV (available with ARP beginning with ONTAP 9.13.1) to protect ARP settings, the pause operation prompts you to obtain the approval of one or more additional administrators. Approval must be received from all administrators associated with the MAV approval group or the operation will fail.

   If you are using MAV and an expected pause operation needs additional approvals, each MAV group approver does the following:

   a. Show the request:

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

   b. Approve the request:

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

      The response for the last group approver indicates that the volume has been modified and the state of ARP is paused.

If you are using MAV and you are a MAV group approver, you can reject a pause operation request:

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

Learn more about `security multi-admin-verify request` in the ONTAP command reference.

Manage ONTAP Autonomous Ransomware Protection attack detection parameters

Beginning with ONTAP 9.11.1, you can modify the parameters for ransomware detection on a specific volume with Autonomous Ransomware Protection enabled and report a known surge as normal file activity. Adjusting detection parameters helps improve the accuracy of reporting based on your specific volume workload.

How attack detection works

When Autonomous Ransomware Protection (ARP) is in a learning or evaluation mode, it develops baseline values for volume behaviors. These include entropy, file extensions, and, beginning with ONTAP 9.11.1, IOPS. These baselines are used to evaluate ransomware threats. For more information about these criteria, see what ARP detects.

Certain volumes and workloads require different detection parameters. For example, the ARP-enabled volume might host numerous types of file extensions, in which case you may want to modify the threshold count for never-before-seen file extensions to a number greater than the default of 20 or disable warnings based on never-before-seen file extensions. Beginning with ONTAP 9.11.1, you can modify the attack detection parameters so they better fit your specific workloads.

Beginning with ONTAP 9.14.1, you can configure alerts when ARP observes a new file extension and when ARP creates a snapshot. For more information, see Configure ARP alerts.

Attack detection in NAS environments

In ONTAP 9.10.1, ARP issues a warning if it detects both of the following conditions:

- More than 20 files with file extensions not previously observed in the volume
- High entropy data

Beginning with ONTAP 9.11.1, ARP issues a threat warning if *only* one condition is met. For example, if more than 20 files with file extensions that have not previously been observed in the volume are observed within a 24-hour period, ARP will categorize this as a threat *regardless* of observed entropy. The 24-hour and 20-file values are defaults, which can be modified.

ⓘ To reduce high numbers of false positive alerts, go to **Storage > Volumes > Security > Configure workload characteristics** and disable **Monitor new file types**. This setting is disabled by default in ONTAP 9.14.1 P7, 9.15.1 P1, 9.16.1, and later.

Attack detection in SAN environments

Beginning with ONTAP 9.17.1, ARP issues a warning if it detects high encryption rates that exceed an automatically learned threshold. This threshold is established after an evaluation period but can be modified.

Modify attack detection parameters

Depending on the expected behaviors of the ARP-enabled volume, you might want to modify the attack detection parameters.

Steps

1. View the existing attack detection parameters:

```
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. All the fields shown are modifiable with boolean or integer values. To modify a field, use the `security anti-ransomware volume attack-detection-parameters modify` command.

   Learn more about `security anti-ransomware volume attack-detection-parameters modify` in the ONTAP command reference.

Report known surges

ARP continues to modify baseline values for detection parameters even when active. If you know of surges in your volume activity, either one-time surges or a surge that is characteristic of a new normal, you should report them as safe. Manually reporting these surges as safe helps to improve the accuracy of ARP’s threat assessments.

Report a one-time surge

1. If a one-time surge is occurring under known circumstances and you want ARP to report a similar surge in future circumstances, clear the surge from the workload behavior:

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

   Learn more about `security anti-ransomware volume workload-behavior clear-surge` in the ONTAP command reference.

Modify baseline surge

1. If a reported surge should be considered normal application behavior, report the surge as such to modify the baseline surge value.

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

   Learn more about `security anti-ransomware volume workload-behavior update-baseline-from-surge` in the ONTAP command reference.

Configure ARP alerts

Beginning with ONTAP 9.14.1, ARP allows you to specify alerts for two ARP events:

- Observation of new file extension on a volume
- Creation of an ARP snapshot

Alerts for these two events can be set on individual volumes or for the entire SVM. If you enable alerts for the SVM, the alert settings are inherited only by volumes created after you enable alert. By default, alerts are not enabled on any volume.

Event alerts can be controlled with multi-admin verification. For more information, see Multi-admin verification with volumes protected with ARP.

Steps

You can use System Manager or the ONTAP CLI to set alerts for ARP events.

System Manager

Set alerts for a volume

1. Navigate to **Volumes**. Select the individual volume for which you want to modify settings.
2. Select the **Security** tab then **Event severity settings**.
3. To receive alerts for **New file extension detected** and **Ransomware snapshot created**, select the dropdown menu under the **Severity** heading. Modify the setting from **Don't generate event** to **Notice**.
4. Select **Save**.

Set alerts for an SVM

1. Navigate to **Storage VM** then select the SVM for which you want to enable settings.
2. Under the **Security** heading, locate the **Anti-ransomware** card. Select ⋮ then **Edit Ransomware Event Severity**.
3. To receive alerts for **New file extension detected** and **Ransomware snapshot created**, select the dropdown menu under the **Severity** heading. Modify the setting from **Don't generate event** to **Notice**.
4. Select **Save**.

CLI

Set alerts for a volume

- To set alerts for a new file-extension:

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

- To set alerts for the creation of an ARP snapshot:

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

- Confirm your settings with the `anti-ransomware volume event-log show` command.

Set alerts for an SVM

- To set alerts for a new file-extension:

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

- To set alerts for the creation of an ARP snapshot:

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

- Confirm your settings with the `security anti-ransomware vserver event-log show` command.

Learn more about `security anti-ransomware vserver event-log` commands in the ONTAP command reference.

Related information

- Understand Autonomous Ransomware Protection attacks and the Autonomous Ransomware Protection snapshot.
- ONTAP command reference

Respond to abnormal activity detected by ONTAP ARP

When Autonomous Ransomware Protection (ARP) detects abnormal activity in a protected volume, it issues a warning. You should evaluate the notification to determine whether the activity is acceptable (false positive) or whether an attack seems malicious. After you categorize the attack, you can clear the warning and notices about suspected files.

When you categorize an attack, ARP snapshots are either retained for an abbreviated period initiated by the categorization operation (ONTAP 9.16.1 and later), or deleted instantly (ONTAP 9.15.1 and earlier).

ⓘ Beginning with ONTAP 9.11.1, you can modify the retention settings for ARP snapshots.

About this task

ARP displays a list of suspected files when it detects any combination of high data entropy, abnormal volume activity with data encryption, and unusual file extensions. Beginning with ONTAP 9.17.1 for both NAS and SAN environments, details of entropy spikes are also reported on the Anti-ransomware page in System Manager.

When an ARP warning notification is issued, respond by designating the activity in one of two ways:

- **False positive**

  The identified file type or entropy spike is expected in your workload and can be ignored.

- **Potential ransomware attack**

  The identified file type or entropy spike is unexpected in your workload and should be treated as a potential attack.

Normal monitoring resumes after you update with your decision and clear the ARP notifications. ARP records your evaluation to the threat assessment profile, using your choice to monitor subsequent file activities.

In the case of a suspected attack, you must determine whether it is an attack, respond to it if it is, and restore protected data before clearing the notices. Learn more about how to recover from a ransomware attack.

If you restore an entire volume, there are no notices to clear.

Before you begin

ARP must be actively protecting a volume and not in a learning or evaluation mode.

Steps

You can use System Manager or the ONTAP CLI to respond to abnormal activity.

System Manager

1. When you receive an "abnormal activity" notification, follow the link. Alternatively, navigate to the **Security** tab of the **Volumes** overview.

   Warnings are displayed in the **Overview** pane of the **Events** menu.

2. In the **Security** tab, review the suspected file types or entropy spikes report.
   - For suspected files, examine each file type in the **Suspected File Types** dialog box and mark each individually.
   - For entropy spikes, examine the entropy report.
3. Record your response:

If you select this value…	Take this action…
False Positive	1. Do one of the following: ◦ For file type warnings, select **Update and Clear Suspect File Types**. ◦ For entropy spikes, select **Mark as false positive**. These actions clear warning notices about suspected files or activity. ARP then resumes normal monitoring of the volume. For ARP/AI in ONTAP 9.16.1 and later, ARP snapshots are automatically deleted after an abbreviated retention period triggered by the categorization operation. For ONTAP 9.15.1 and earlier, related ARP snapshots are automatically deleted after you clear suspected file types. ⓘ Beginning with ONTAP 9.13.1, if you are using MAV to protect ARP settings, the clear-suspect operation prompts you to obtain the approval of one or more additional administrators. Approval must be received from all administrators associated with the MAV approval group or the operation will fail.

Potential Ransomware Attack	1. Respond to the attack: ◦ For file type warnings, mark selected files as **Potential ransomware attack** and restore protected data. ◦ For entropy spikes that indicate an attack, select **Mark as potential ransomware attack** and restore protected data. 2. After data restoration is complete, record your decision and resume normal ARP monitoring: ◦ For file type warnings, select **Update and Clear Suspect File Types**. ◦ For entropy spikes, select **Mark as potential ransomware attack** and select **Save and dismiss**. ⓘ There are no suspected file type notices to clear if you've restored an entire volume. Recording your decision clears the attack report. For ARP/AI in ONTAP 9.16.1 and later, ARP snapshots are automatically deleted after an abbreviated retention period triggered by the categorization operation. For ONTAP 9.15.1 and earlier, after you restore a volume the ARP snapshots are automatically deleted.

CLI

Verify the attack

1. When you receive a notification of a suspected ransomware attack, verify the time and severity of the attack:

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

Sample output:

```
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
```

You can also check EMS messages:

```
event log show -message-name callhome.arw.activity.seen
```

2. Generate an attack report and specify where to save it:

   ```
   security anti-ransomware volume attack generate-report -vserver
   <svm_name> -volume <vol_name> -dest-path
   <[svm_name]:[junction_path/sub_dir_name]>
   ```

   Sample command:

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

   Sample output:

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

3. View the report on an admin client system. For example:

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

Take action

1. Take one of the following actions based on your evaluation of the file extensions or entropy spikes:

   - False positive

     Run one of the following commands to record your decision and resume normal Autonomous Ransomware Protection monitoring:

     - For file extensions:

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

       Use the following optional parameter to identify only specific extensions as false positives:

       - `[-extension <text>, … ]`: File extensions

     - For entropy spikes:

```
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
```

- Potential ransomware attack

  Respond to the attack and recover data from the ARP-created backup snapshot. After the data is recovered, run one of the following commands to record your decision and resume normal ARP monitoring:

  - For file extensions:

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

    Use the following optional parameter to identify only specific extensions as potential ransomware:

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

  - For entropy spikes:

    ```
    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
    ```

This `clear-suspect` operation clears the attack report. There are no suspected file type notices to clear if you restored an entire volume. For ARP/AI in ONTAP 9.16.1 and later, ARP snapshots are automatically deleted after an abbreviated retention period triggered by the categorization operation. For ONTAP 9.15.1 and earlier, ARP snapshots are automatically deleted after you restore a volume or clear a suspected event.

2. Beginning in 9.18.1, you can determine the status of the `clear-suspect` operation:

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

MAV options

1. If you are using MAV and an expected `clear-suspect` operation needs additional approvals, each MAV group approver must:

   a. Show the request:

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

b. Approve the request to resume normal anti-ransomware monitoring:

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

The response for the last group approver indicates that the volume has been modified and a false positive is recorded.

2. If you are using MAV and you are a MAV group approver, you can also reject a clear-suspect request:

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

Related information

- NetApp Knowledge Base: Understanding Autonomous Ransomware Protection attacks and the Autonomous Ransomware Protection snapshot
- Modify automatic snapshots options
- security anti-ransomware volume
- security multi-admin-verify request

Restore data from ONTAP ARP snapshots after a ransomware attack

Autonomous Ransomware Protection (ARP) creates snapshots to protect against a potential ransomware threat. You can use one of these ARP snapshots or another snapshot of your volume to restore data.

About this task

The ARP creates snapshots with one of the following prepended names:

- `Anti_ransomware_periodic_backup`: Used in ONTAP 9.17.1 and later for snapshots created at regular intervals. For example, `Anti_ransomware_periodic_backup.2025-06-01_1248`.
- `Anti_ransomware_attack_backup`: Used in ONTAP 9.17.1 and later for snapshots created in response to abnormalities. For example, `Anti_ransomware_attack_backup.2025-08-25_1248`.
- `Anti_ransomware_backup`: Used in ONTAP 9.16.1 and earlier with snapshots that are created in response to abnormalities. For example, `Anti_ransomware_backup.2022-12-20_1248`.

To restore from a snapshot other than the `Anti_ransomware` snapshot after a system attack is identified, you must first release the ARP snapshot.

If no system attack is reported, you must first restore from the `Anti_ransomware` snapshot then complete a subsequent restoration of the volume from the snapshot you choose.

> ⓘ If the ARP-protected volume is part of a SnapMirror relationship, you'll need to manually update all mirror copies of the volume after restoring it from a snapshot. If you skip this step, the mirror copies might become unusable and need to be deleted and recreated.

Before you begin

You must mark the attack as a potential ransomware attack before restoring data from a snapshot.

Steps

You can use System Manager or the ONTAP CLI to restore your data.

System Manager

Restore after a system attack

1. To restore from the ARP snapshot, skip to step two. To restore from an earlier snapshot, you must first release the lock on the ARP snapshot.
   1. Select **Storage > Volumes**.
   2. Select **Security** then **View Suspected File Types**.
   3. Mark the files as "Potential ransomware attack".
   4. Select **Update** and **Clear Suspect File Types**.
2. Display the snapshots in volumes:

   Select **Storage > Volumes**, then select the volume and **Snapshot Copies**.
3. Select ⋮ next to the snapshot you want to restore then **Restore**.

Restore if a system attack was not identified

1. Display the snapshots in volumes:

   Select **Storage > Volumes**, then select the volume and **Snapshot Copies**.
2. Select ⋮ then choose the `Anti_ransomware` snapshot.
3. Select **Restore**.
4. Return to the **Snapshot Copies** menu, then choose the snapshot you want to use. Select **Restore**.

CLI

Restore after a system attack

To restore from the ARP snapshot, skip to step two. To restore data from earlier snapshots, you must release the lock on the ARP snapshot.

> It is only necessary to release the anti-ransomware Snaplock before restoring from earlier snapshots if you are using the `volume snapshot restore` command as outlined below. If you are restoring data using FlexClone, Single File Snap Restore, or other methods, this is not necessary.

1. Mark the attack as a potential ransomware attack (`-false-positive false`) and clear suspect files (`clear-suspect`):

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

   Use one of the following parameters to identify the extensions:

   - [-seq-no *integer*]: Sequence number of the file in the suspect list.
   - [-extension *text*, …]: File extensions
   - [-start-time *date_time* -end-time *date_time*]: Starting and ending times for the range of files to be cleared, in the form "MM/DD/YYYY HH:MM:SS".

2. List the snapshots in a volume:

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

   The following example shows the 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. Restore the contents of a volume from a snapshot:

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

   The following example restores the contents of `vol1`:

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

Restore if a system attack was not identified

1. List the snapshots in a volume:

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

   The following example shows the 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. Restore the contents of a volume from a snapshot:

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

The following example restores the contents of `vol1`:

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

Learn more about `volume snapshot` in the ONTAP command reference.

Related information

- NetApp Knowledge Base: Ransomware prevention and recovery in ONTAP
- ONTAP command reference

Adjust settings for automatically generated ARP snapshots

Beginning with ONTAP 9.11.1, you can use the CLI to control the retention settings for Autonomous Ransomware Protection (ARP) snapshots that are automatically generated in response to suspected ransomware attacks.

Before you begin

You can only modify ARP snapshots options on a node SVM and not on other SVM types.

Steps

1. Show all current ARP snapshot settings:

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

2. Show selected current ARP snapshot settings:

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

3. Modify ARP snapshot settings:

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

You can modify the following settings:

> Some of the commands described are deprecated as of ONTAP 9.17.1. Commands introduced in ONTAP 9.17.1 support both NAS and SAN environments.

Setting	Description	Supported versions
`arw.snap.max.count`	Specifies the maximum number of ARP snapshots that can exist in a volume at any given time. Older copies are deleted to ensure that the total number of ARP snapshots is within this specified limit.	ONTAP 9.11.1 and later
`arw.snap.create.interval.hours`	Specifies the interval *in hours* between ARP snapshots. A new ARP snapshot is created when a data entropy-based attack is suspected and the most recently created ARP snapshot is older than the specified interval.	ONTAP 9.11.1 and later
`arw.snap.normal.retain.interval.hours`	Specifies the duration *in hours* for which an ARP snapshot is retained. When an ARP snapshot reaches the retention threshold, it is deleted.	• ONTAP 9.11.1 to ONTAP 9.16.1 • Deprecated in ONTAP 9.17.1 and later

Setting	Description	Supported versions
`arw.snap.max.retain.interval.days`	Specifies the maximum duration *in days* for which an ARP snapshot can be retained. Any ARP snapshot older than this duration is deleted when there is no attack reported on the volume. ⓘ The maximum retention interval for ARP snapshots is ignored if a moderate threat is detected. The ARP snapshot created in response to the threat is retained until you have responded to the threat. When you mark a threat as a false positive, ONTAP will delete the ARP snapshots for the volume.	• ONTAP 9.11.1 to ONTAP 9.16.1 • Deprecated in ONTAP 9.17.1 and later
`arw.snap.create.interval.hours.post.max.count`	Specifies the interval *in hours* between ARP snapshots when the volume already contains the maximum number of ARP snapshots. When the maximum number is reached, an ARP snapshot is deleted to make room for a new copy. The new ARP snapshot creation speed can be reduced to retain the older copy using this option. If the volume already contains the maximum number of ARP snapshots, the interval specified in this option is used for the next ARP snapshot creation, instead of `arw.snap.create.interval.hours`.	• ONTAP 9.11.1 to 9.16.1 • Deprecated in ONTAP 9.17.1 and later
`arw.snap.low.encryption.retain.duration.hours`	Specifies the retention duration *in hours* for ARP snapshots created during periods of low encryption activity.	• ONTAP 9.17.1 and later
`arw.snap.new.extns.interval.hours`	Specifies the interval *in hours* between the ARP snapshots created when a new file extension is detected. A new ARP snapshot is created when a new file extension is observed; the previous snapshot created upon observing a new file extension is older than this specified interval. On a workload that frequently creates new file extensions, this interval helps control the frequency of the ARP snapshots. This option exists independent of `arw.snap.create.interval.hours`, which specifies the interval for data entropy-based ARP snapshots.	• ONTAP 9.11.1 to ONTAP 9.16.1 • Deprecated in ONTAP 9.17.1 and later
`arw.snap.retain.hours.after.clear.suspect.false.alert`	Specifies the interval *in hours* an ARP snapshot is retained as a precaution after an attack incident is marked as a false positive by the administrator. After this precautionary retention period expires, the snapshot may be deleted according to the standard retention duration defined by the options `arw.snap.normal.retain.interval.hours` and `arw.snap.max.retain.interval.days`.	• ONTAP 9.16.1 and later

Setting	Description	Supported versions
`arw.snap.retain.hours.after.clear.suspect.real.attack`	Specifies the interval *in hours* an ARP snapshot is retained as a precaution after an attack incident is marked as a real attack by the administrator. After this precautionary retention period expires, the snapshot may be deleted according to the standard retention duration defined by the options `arw.snap.normal.retain.interval.hours` and `arw.snap.max.retain.interval.days`.	• ONTAP 9.16.1 and later
`arw.snap.surge.interval.days`	Specifies the interval *in days* between ARP snapshots created in response to IO surges. ONTAP creates an ARP snapshot surge copy when there's a surge in IO traffic and the last created ARP snapshot is older than this specified interval. This option also specifies retention period *in day* for an ARP surge snapshot.	ONTAP 9.11.1 and later
`arw.high.encryption.alert.enabled`	Enables alerts for high levels of encryption. When this option is set to `on` (default), ONTAP sends an alert when the percentage of encryption exceeds the threshold specified in `arw.high.encryption.percentage.threshold`.	ONTAP 9.17.1 and later
`arw.high.encryption.percentage.threshold`	Specifies the maximum percentage of encryption for a volume. If the percentage of encryption is more than this threshold, ONTAP handles the increase as an attack and creates an ARP snapshot. `arw.high.encryption.alert.enabled` must be set to `on` for this option to take effect.	ONTAP 9.17.1 and later
`arw.snap.high.encryption.retain.duration.hours`	Specifies the retention duration interval *in hours* for snapshots created during a high encryption threshold event.	ONTAP 9.17.1 and later

4. If you are using ARP with a SAN environment, you can also modify the following evaluation period settings:

Setting	Description	Supported versions
`arw.block_device.auto.learn.threshold.min_value`	Specifies the minimum encryption threshold percentage value during the auto-learn phase of evaluation for block devices.	ONTAP 9.17.1 and later
`arw.block_device.auto.learn.threshold.max_value`	Specifies the maximum encryption threshold percentage value during the auto-learn phase of evaluation for block devices.	ONTAP 9.17.1 and later
`arw.block_device.evaluation.phase.min_hours`	Specifies the minimum interval *in hours* the evaluation phase must run before the encryption threshold is set.	ONTAP 9.17.1 and later

Setting	Description	Supported versions
`arw.block_device.evaluation.phase.max_hours`	Specifies the maximum interval *in hours* the evaluation phase must run before the encryption threshold is set.	ONTAP 9.17.1 and later
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	Specifies the minimum amount of data *in GB* that must be ingested during the evaluation phase before the encryption threshold is set.	ONTAP 9.17.1 and later
`arw.block_device.evaluation.phase.alert.enabled`	Specifies whether alerts are enabled for the evaluation phase of ARP on block devices. Default value is `True`.	ONTAP 9.17.1 and later
`arw.block_device.evaluation.phase.alert.threshold`	Specifies the threshold percentage during the evaluation phase of ARP on block devices. If the percentage of encryption exceeds this threshold, an alert is triggered.	ONTAP 9.17.1 and later

Related information

- Threat assessment and ARP snapshots
- SAN entropy evaluation period

Update ONTAP Autonomous Ransomware Protection with AI (ARP/AI)

To keep protection up to date against the latest ransomware threats, ARP/AI offers automatic updates that occur outside of regular ONTAP release cadences.

Beginning with ONTAP 9.16.1, security updates for ARP/AI are available in System Manager software downloads in addition to system and firmware updates. If your ONTAP cluster is already enrolled in automatic system and firmware updates, you will be automatically notified when ARP/AI security updates are available. You can also change your update preferences so that ONTAP installs security updates automatically.

If you want to manually update ARP/AI, you can download updates from the NetApp Support Site and install them using System Manager.

About this task

You can only update ARP/AI using System Manager.

Select an update preference for ARP/AI

In System Manager, the settings on the Enable automatic updates page for security files are set to `Show notifications` if you are already enrolled in automatic firmware and system updates. You can change the update settings to `Automatically update` if you'd prefer ONTAP to apply the latest updates automatically. If you use a dark site or prefer to perform updates manually, you can choose to show notifications or automatically dismiss security updates.

Before you begin

For automatic security updates, AutoSupport and AutoSupport OnDemand should be enabled and the transport protocol should be set to HTTPS.

Steps

1. In System Manager, click **Cluster > Settings > Software updates**.
2. In the **Software updates** section, select →.
3. From the **Software updates** page, select the **All other updates** tab.
4. Select the **All other updates** tab and click **More**.
5. Select **Edit automatic update settings**.
6. From the Automatic update settings page, select **Security Files**.
7. Specify the action to be taken for security files (ARP/AI updates).

   You can choose to automatically update, show notifications, or automatically dismiss updates.

   > ⓘ For security updates to automatically update, AutoSupport and AutoSupport OnDemand should be enabled and the transport protocol should be set to HTTPS.

8. Accept the terms and conditions and select **Save**.

Manually update ARP/AI with the latest security package

Follow the appropriate procedure depending on whether you are registered with Active IQ Unified Manager.

> ⓘ Be sure to install only a more recent ARP update than your current version to avoid any unintended ARP downgrades.

ONTAP 9.16.1 and later with Digital Advisor

1. In System Manager, go to **Dashboard**.

   In the **Health** section, a message displays if there are any recommended security updates for the cluster.

2. Click on the alert message.
3. Next to the security updates in the list of recommended updates, select **Actions**.
4. Click **Update** to install the update immediately or **Schedule** to schedule it for later.

   If the update is already scheduled, you can **Edit** or **Cancel** it.

ONTAP 9.16.1 and later without Digital Advisor

1. Navigate to the NetApp Support Site and log in.
2. Complete the prompts and download the security package that you want to use to update your cluster ARP/AI.
3. Copy the files to an HTTP or FTP server on your network or to a local folder that can be accessed by the cluster with ARP/AI.
4. In System Manager, click **Cluster > Settings > Software updates**.
5. In **Software updates**, select the **All other updates** tab.

6. In the **Manual updates** pane, click **Add security files** and add the files using one of these preferences:
    - **Download from server**: Enter the URL for the security file package.
    - **Upload from local client**: Navigate to the downloaded TGZ file.

    > Ensure that the file name begins with `ontap_security_file_arpai_` and has `.tgz` as a file extension.

7. Click **Add** to apply the updates.

Verify ARP/AI updates

To view a history of automatic updates that were dismissed or failed to install, do the following:

1. In System Manager, click **Cluster > Settings > Software updates**.
2. In the **Software updates** section, select →.
3. From the **Software updates** page, select the **All other updates** tab and click **More**.
4. Select **View all automatic updates**.

Related information

- Learn about ARP/AI
- Email subscriptions for software updates

Copyright information

Trademark information