



Protect against ransomware

ONTAP 9

NetApp
June 04, 2024

Table of Contents

- Protect against ransomware. 1
 - Autonomous Ransomware Protection overview 1
 - Autonomous Ransomware Protection use cases and considerations 3
 - Enable Autonomous Ransomware Protection 7
 - Enable Autonomous Ransomware Protection by default in new volumes 10
 - Pause Autonomous Ransomware Protection to exclude workload events from analysis 12
 - Manage Autonomous Ransomware Protection attack detection parameters 14
 - Respond to abnormal activity 18
 - Restore data after a ransomware attack 21
 - Modify options for automatic Snapshot copies 24

Protect against ransomware

Autonomous Ransomware Protection overview

Beginning with ONTAP 9.10.1, the Autonomous Ransomware Protection (ARP) feature uses workload analysis in NAS (NFS and SMB) environments to proactively detect and warn about abnormal activity that might indicate a ransomware attack.

When an attack is suspected, ARP also creates new Snapshot copies, in addition to existing protection from scheduled Snapshot copies.

Licenses and enablement

ARP requires a license. ARP is available with the [ONTAP ONE license](#). If you do not have the the ONTAP One license, other licenses are available to use ARP, which 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 to ONTAP 9.11.1 or later and ARP is already configured on your system, you do not need to purchase 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](#).

You can configure ARP on a per-volume basis using either System Manager or the ONTAP CLI.

ONTAP ransomware protection strategy

An effective ransomware detection strategy should include more than a single layer of protection.

An analogy would be the safety features of a vehicle. You don't rely on a single feature, such as a seatbelt, to completely protect you in an accident. Air bags, anti-lock brakes, and forward-collision warning are all additional safety features that will lead to a much better outcome. Ransomware protection should be viewed in the same way.

While ONTAP includes features like FPolicy, Snapshot copies, SnapLock, and Active IQ Digital Advisor to help protect from ransomware, the following information focuses on the ARP on-box feature with machine learning capabilities.

To learn more about ONTAP's other anti-ransomware features, see [TR-4572: NetApp Solution for Ransomware](#).

What ARP detects

ARP is designed to protect against denial-of-service attacks where the attacker withholds data until a ransom

is paid. ARP offers anti-ransomware detection based on:

- Identification of the incoming data as encrypted or plaintext.
- Analytics, which detects
 - **Entropy**: an evaluation of the randomness of data in a file
 - **File extension types**: An extension that does not conform to the normal extension type
 - **File IOPS**: A surge in abnormal volume activity with data encryption (beginning in ONTAP 9.11.1)

ARP can detect the spread of most ransomware attacks after only a small number of files are encrypted, take action automatically to protect data, and alert you that a suspected attack is happening.



No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. Although it's possible an attack might go undetected, ARP acts as an important additional layer of defense if anti-virus software has failed to detect an intrusion.

Learning and active modes

ARP has two modes:

- **Learning** (or "dry run" mode)
- **Active** (or "enabled" mode)

When you enable ARP, it runs in *learning mode*. In learning mode, the ONTAP system develops an alert profile based on the analytic areas: entropy, file extension types, and file IOPS. After running ARP in learning mode for enough time to assess workload characteristics, you can switch to active mode and start protecting your data. Once ARP has switched to active mode, ONTAP creates ARP Snapshot copies to protect the data if a threat is detected.

It's recommended you leave ARP in learning mode for 30 days. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch, which may occur before 30 days.

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 file extension is observed. 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.)

Beginning in ONTAP 9.11.1, you can customize the detection parameters for ARP. For more information, see [manage ARP attack detection parameters](#).

Threat assessment and ARP Snapshot copies

In active mode, ARP assesses threat probability based on incoming data measured against learned analytics. A measurement is assigned when ARP detects a threat:

- **Low**: the earliest detection of an abnormality in the volume (for example, a new file extension is observed in the volume).

- **Moderate:** multiple files with the same never-seen-before file extension are observed.
 - In ONTAP 9.10.1, the threshold for escalation to moderate is 100 or more files. Beginning with ONTAP 9.11.1, the file quantity is modifiable; its default value is 20.

In a low threat situation, ONTAP detects an abnormality and creates a Snapshot copy of the volume to create the best recovery point. ONTAP prepends the name of the ARP Snapshot copy with `Anti-ransomware-backup` to make it easily identifiable, for example `Anti_ransomware_backup.2022-12-20_1248`.

The threat escalates to moderate after ONTAP runs an analytics report determining if the abnormality matches a ransomware profile. Threats that remain at the low level are logged and visible in the **Events** section of System Manager. 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 alerts settings](#). For more information, see [Respond to abnormal activity](#).

You can view information about a threat, regardless of level, in System Manager's **Events** section or with the `security anti-ransomware volume show` command.

ARP Snapshot copies are retained for a minimum of two days. Beginning with ONTAP 9.11.1, you can modify the retention settings. For more information, see [Modify options for Snapshot copies](#).

How to recover data in ONTAP after a ransomware attack

When an attack is suspected, the system takes a volume Snapshot copy at that point in time and locks that copy. If the attack is confirmed later, the volume can be restored using the ARP Snapshot copy.

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

With the knowledge of the affected files and the time of attack, it is possible to selectively recover the affected files from various Snapshot copies, rather than simply reverting the whole volume to one of the Snapshot copies.

ARP thus builds on proven ONTAP data protection and disaster recovery technology to respond to ransomware attacks. See the following topics for more information on recovering data.

- [Recover from Snapshot copies \(System Manager\)](#)
- [Restoring files from Snapshot copies \(CLI\)](#)
- [Smart ransomware recovery](#)

Autonomous Ransomware Protection use cases and considerations

Autonomous Ransomware Protection (ARP) is available for NAS workloads beginning with ONTAP 9.10.1. 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:

- Databases on NFS storage
- Windows or Linux home directories

Because users could create files with extensions that weren't detected in the learning period, 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:

- Workloads with a high frequency of file create or delete (hundreds of thousands of files in few seconds; for example, test/development workloads).
- ARP's threat detection depends on its ability recognize an unusual surge in file create, rename, or delete activity. 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, the feature 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 NFS and SMB volumes in on-premises ONTAP systems beginning with ONTAP 9.10.1.

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

	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 Asynchronous SnapMirror	✓	✓	✓	✓		
SVMs protected with Asynchronous SnapMirror (SVM disaster recovery)	✓	✓	✓	✓		
SVM data mobility (vserver migrate)	✓	✓	✓	✓		

	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
FlexGroup volumes	✓	✓	✓			
Multi-admin verification	✓	✓	✓			

SnapMirror and ARP interoperability

Beginning with ONTAP 9.12.1, ARP is supported on Asynchronous SnapMirror destination volumes. ARP is **not** supported with SnapMirror Synchronous.

If a SnapMirror source volume is ARP-enabled, the SnapMirror destination volume automatically acquires the ARP configuration state (learning, enabled, etc), ARP training data, and ARP-created Snapshot of the source volume. No explicit enablement is required.

While the destination volume consists of read-only (RO) Snapshot copies, 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 procedure 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 Snapshot copies from source to destination volumes. Hence 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). ARP detection behaves differently for changes inside and outside the VM. ARP is not recommended for workloads with high-entropy files inside 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 encrypted or a file extension changes. Detectable file extension changes are:

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

Changes inside the VM

If the ransomware attack targets the VM and files inside of the VM are altered 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). Although ARP creates a protective Snapshot in this scenario, it does not generate a threat alert because the file extensions outside of the VM have not been tampered with.

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.

Unsupported configurations

ARP is not supported in the following system configurations:

- ONTAP S3 environments
- SAN 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, FlexGroup volumes are supported)
- FlexCache volumes (ARP is supported on origin FlexVol volumes but not on cache volumes)
- Offline volumes
- SAN-only volumes
- SnapLock volumes
- SnapMirror Synchronous
- Asynchronous SnapMirror (Unsupported only in ONTAP 9.10.1 and 9.11.1. Asynchronous SnapMirror 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 workloads. 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 *
Read-intensive or the data can be compressed.	150	4% of maximum IOPS
Write-intensive and the data cannot be compressed.	60	10% of maximum IOPS

* 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, as the number of protected volumes increases, analytics run on each volume less frequently.

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.

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 create MAV rules at the SVM level using `security anti-ransomware vserver event-log modify` or at the volume level with `security anti-ransomware volume event-log modify`.

Next steps

- [Enable Autonomous Ransomware Protection](#)
- [Enable MAV for ARP-protected volumes](#)

Enable Autonomous Ransomware Protection

Beginning with ONTAP 9.10.1, Autonomous Ransomware Protection (ARP) can be enabled on new or existing volumes. You first enable ARP in learning mode, in which the system analyzes the workload to characterize normal behavior. You can enable ARP on an existing volume, or you can create a new volume and enable ARP from the beginning.

About this task

You should always enable ARP initially in learning (or dry-run) mode. Beginning in active mode can lead to excessive false positive reports.

It's recommended 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 may occur before 30 days. For more information, see [Learning and active modes](#).



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.

Before you begin

- You must have a storage VM (SVM) enabled for NFS or SMB (or both).
- The [correct license](#) must be installed for your ONTAP version.
- You must have NAS workload with clients configured.
- The volume you want to set ARP on needs to be protected and must have an active [junction path](#).
- The volume must be less than 100% full.
- It's recommended you configure the EMS system to send email notifications, which will include notices of ARP activity. For more information, see [Configure EMS events to send email notifications](#).

- Beginning in 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](#).

Enable ARP

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

System Manager

Steps

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 in learning-mode in the **Anti-ransomware** box.
3. When the learning period is over, switch ARP to active mode.



Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch. You can [disable this setting on the associated storage VM](#) if you want to control the learning mode to active mode switch manually.

- a. Select **Storage > Volumes** and then select the volume that is ready for active mode.
 - b. In the **Security** tab of the **Volumes** overview, select **Switch** to active mode in the Anti-ransomware box.
4. You can 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

The process to enable ARP with the CLI differs if you are enabling it on an existing volume versus a new volume.

Enable ARP on an existing volume

1. Modify an existing volume to enable ransomware protection in learning mode:

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

If you're running ONTAP 9.13.1 or later, adaptive learning is enabled so that the change to active state is done automatically. If you do not want this behavior to be automatically enabled, change the setting at the SVM level on all associated volumes:

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

2. When the learning period is over, 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 active
```

3. Verify the ARP state of the volume.

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

Enable ARP on a new volume

1. Create a new volume with anti-ransomware protection enabled before provisioning data.

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

If you're running ONTAP 9.13.1 or later, adaptive learning is enabled so that the change to active state is done automatically. If you do not want this behavior to be automatically enabled, change the setting at the SVM level on all associated volumes:

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

2. When the learning period is over, 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 active
```

3. Verify the ARP state of the volume.

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

Enable Autonomous Ransomware Protection by default in new volumes

Beginning with ONTAP 9.10.1, you can configure storage VMs (SVMs) such that new volumes are enabled by default for Autonomous Ransomware Protection (ARP) in learning mode.

About this task

By default, new volumes are created with ARP in disabled mode. You can modify this setting in System Manager and with the CLI. Volumes enabled by default are set to ARP in learning (or dry-run) mode.

ARP will only be enabled on volumes created in the SVM after you have changed the setting. ARP will not be enabled on existing volumes. Learn how to [enable ARP in an existing volume](#).

Beginning in ONTAP 9.13.1, adaptive learning has been added to ARP analytics, and the switch from learning mode to active mode is done automatically. For more information, see [Learning and active modes](#).

Before you begin

- The [correct license](#) must be installed for your ONTAP version.
- The volume must be less than 100% full.
- Junction paths must be active.
- Beginning in ONTAP 9.13.1, it's recommended you enable multi-admin verification (MAV) so that two or

more authenticated user admins are required for anti-ransomware operations. [Learn more.](#)

Switch ARP from learning to active mode

Beginning in ONTAP 9.13.1, adaptive learning has been added to ARP analytics. 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
```


After 30 days of learning, a volume is automatically switched to active mode even if one or more of these conditions are not satisfied. That is, if auto-switch is enabled, the volume switches to active mode after a maximum of 30 days. The maximum value of 30 days is fixed and not modifiable.

For more information on ARP configuration options, including default values, see the [ONTAP command reference](#).

Steps

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

System Manager

1. Select **Storage > Storage VMs** then select the storage VM that contains 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 ARP for NAS volumes. Check the additional box to enable ARP on all eligible NAS volumes in the storage VM.



If you have upgraded to ONTAP 9.13.1, the **Switch automatically from learning to active mode after sufficient learning** setting is enabled automatically. This allows ARP to determine the optimal learning period interval and automate the switch to active mode. Turn off the setting if you want to manually transition to active mode.

CLI

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

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

At the CLI, you can also create a new SVM with ARP enabled by default for new volumes.

```
vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]
```

If you upgraded to ONTAP 9.13.1 or later, adaptive learning is enabled so that the change to active state is done automatically. If you do not want this behavior to be automatically enabled, use the following command:

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

Pause 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 in 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 this task

During an ARP pause, no events are logged nor are any actions for new writes. However, the analytics operation continues 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 your 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.

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
```

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

Manage Autonomous Ransomware Protection attack detection parameters

Beginning in ONTAP 9.11.1, you can modify the parameters for ransomware detection on a specific Autonomous Ransomware Protection-enabled volume 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 learning mode, it develops baseline values for volume behaviors. These are entropy, file extensions, and, beginning in ONTAP 9.11.1, IOPS. These baselines are used to evaluate ransomware threats. For more information about these criteria, see [What ARP detects](#).

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 in 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.)

Beginning in 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](#)

Certain volumes and workloads require different detection parameters. For example, your ARP-enabled volume may 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.

Modify attack detection parameters

Depending on the expected behaviors of your ARP-enabled volume, you may 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
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 : 20
Never Seen before File Extensions Duration in Hour : 24
```

2. All of 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.

For a full list of parameters, see [ONTAP command reference](#).

Report known surges

ARP continues to modify baseline values for detection parameters even in active mode. 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 it as safe. Manually reporting these surges as safe helps to improve the accuracy of ARP's threat assessments.

Report a one-time surges

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
```

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
```

Configure ARP alerts

Beginning in 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](#).

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 Security 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 -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 -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.

More information

- [Understand Autonomous Ransomware Protection attacks and the Autonomous Ransomware Protection snapshot](#)

Respond to abnormal activity

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.

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.

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

- **False positive**

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

- **Potential ransomware attack**

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

In both cases, normal monitoring resumes after updating and clearing the notices. 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 running in active mode.

Steps

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

System Manager


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

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

2. When a “Detected abnormal volume activity” message is displayed, view the suspect files.

In the **Security** tab, select **View Suspected File Types**.

3. In the **Suspected File Types** dialog box, examine each file type and mark it as either “False Positive” or “Potential Ransomware attack”.

If you selected this value...	Take this action...
False Positive	<div>Select Update and Clear Suspect File Types to record your decision and resume normal ARP monitoring.</div> <div><div>Beginning with ONTAP 9.13.1, if you are using MAV to protect your 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.</div></div>
Potential Ransomware Attack	<div>Respond to the attack and restore protected data. Then select Update and Clear Suspect File Types to record your decision and resume normal ARP monitoring.</div> <div>There are no suspect file types to clear if you restored an entire volume.</div>

CLI

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: 9/14/2021 01:03:23
Number of Attacks: 1
```

You can also check EMS messages:

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

2. Generate an attack report and note the output location:

```
security anti-ransomware volume attack generate-report -volume vol_name
-dest-path file_location/
```

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:

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

19  "9/14/2021 01:03:23"    test_dir_1/test_file_1.jpg.lckd
20  "9/14/2021 01:03:46"    test_dir_2/test_file_2.jpg.lckd
21  "9/14/2021 01:03:46"    test_dir_3/test_file_3.png.lckd`
```

4. Take one of the following actions based on your evaluation of the file extensions:

- False positive

Enter the following command to record your decision, adding the new extension to the list of those allowed, and resume normal anti-ransomware monitoring:

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

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".

- Potential ransomware attack

Respond to the attack and [recover data from the ARP-created backup snapshot](#). After the data is recovered, enter the following command to record your decision and resume normal ARP monitoring:

```
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 extension

`[-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".

There are no suspect file types to clear if you restored an entire volume. The ARP-created backup snapshot will be removed and the attack report will be cleared.

5. 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.

6. 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]
```

More information

- [KB: Understanding Autonomous Ransomware Protection attacks and the Autonomous Ransomware Protection snapshot.](#)

Restore data after a ransomware attack

Autonomous Ransomware Protection (ARP) creates Snapshot copies named `Anti_ransomware_backup` when it detects a potential ransomware threat. You can use one of these ARP Snapshot copies or another Snapshot copy of your volume to restore data.

About this task

If the volume has SnapMirror relationships, manually replicate all mirror copies of the volume immediately after you restore from a Snapshot copy. Not doing so can result in unusable mirror copies that must be deleted and recreated.

To restore from a Snapshot other than the `Anti_ransomware_backup` Snapshot after a system attack was identified, you must first release the ARP Snapshot.

If no system attack was reported, you must first restore from the `Anti_ransomware_backup` Snapshot copy then complete a subsequent restoration of the volume from the Snapshot copy of your choosing.

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 copy, you must first release the lock on the ARP Snapshot.
 - a. Select **Storage > Volumes**.
 - b. Select **Security** then **View Suspected File Types**
 - c. Mark the files as "False Positive" .
 - d. Select **Update** and **Clear Suspect File Types**
2. Display the Snapshot copies in volumes:


Select **Storage > Volumes**, then select the volume and **Snapshot Copies**.

3. Select  next to the Snapshot copy you want to restore then **Restore**.

Restore if a system attack was not identified

1. Display the Snapshot copies in volumes:

Select **Storage > Volumes**, then select the volume and **Snapshot Copies**.

2. Select  then choose the `Anti_ransomware_backup` Snapshot.
3. Select **Restore**.
4. Return to the **Snapshot Copies** menu, then choose the Snapshot copy you want to use. Select **Restore**.

CLI

Restore after a system attack

1. To restore from the ARP Snapshot copy, skip to step two. To restore data from earlier Snapshot copies, you must release the lock on the ARP Snapshot.



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

Mark the attack as a "false positive" and "clear suspect":

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

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 Snapshot copies in a volume:

```
volume snapshot show -vserver SVM -volume volume
```

The following example shows the Snapshot copies in `vol11`:


```
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 copy:

```
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 Snapshot copies in a volume:

```
volume snapshot show -vserver SVM -volume volume
```

The following example shows the Snapshot copies 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 copy:

```
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
```

3. Repeat steps 1 and 2 to restore the volume using the desire Snapshot copy.

More information

- [KB: Ransomware prevention and recovery in ONTAP](#)

Modify options for automatic Snapshot copies

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

Before you begin

You can only modify ARP Snapshots options on a node SVM.

Steps

1. To show all current ARP Snapshot copy settings, enter:

```
vserver options -vserver svm_name arw*
```



The `vserver options` command is a hidden command. To view the man page, enter `man vserver options` at the ONTAP CLI.

2. To show selected current ARP Snapshot copy settings, enter:


```
vserver options -vserver svm_name -option-name arw_setting_name
```

3. To modify ARP Snapshot copy settings, enter:

```
vserver options -vserver svm_name -option-name arw_setting_name -option-value  
arw_setting_value
```

The following settings are modifiable:

ARW setting	Description
<code>arw.snap.max.count</code>	Specifies the maximum number of ARP Snapshot copies that can exist in a volume at any given time. Older copies are deleted to ensure that the total number of ARP Snapshot copies are within this specified limit. The <code>-option-value</code> parameter accepts integers between 3 and 8, inclusive. The default value is 6.

ARW setting	Description
<code>arw.snap.create.interval.hours</code>	<p>Specifies the interval <i>in hours</i> between ARP Snapshot copies. A new ARP Snapshot copy is created when an data entropy-based attack is suspected and the most recently created ARP Snapshot copy is older than the specified interval.</p> <p>The <code>-option-value</code> parameter accepts integers between 1 and 48, inclusive. The default value is 4.</p>
<code>arw.snap.normal.retain.interval.hours</code>	<p>Specifies the duration <i>in hours</i> for which an ARP Snapshot copy is retained. When an ARP Snapshot copy reaches the retention threshold, any other ARP Snapshots copy created before it is deleted. No more than one ARP Snapshot copy older than the retention threshold can exist.</p> <p>The <code>-option-value</code> parameter accepts integers between 4 and 96, inclusive. The default value is 48.</p>
<code>arw.snap.max.retain.interval.days</code>	<p>Specifies the maximum duration <i>in days</i> for which an ARP Snapshot copy can be retained. Any ARP Snapshot copy older than this duration is deleted when there is no attack reported on the volume.</p> <div>  <p>The maximum retention interval for ARP Snapshot copies is ignored if a moderate threat is detected. The ARP Snapshot copy created in response to the threat is retained until you have responded to the threat. Marking a threat as a false positive delete the ARP Snapshot copies on the volume.</p> <p>The <code>-option-value</code> parameter accepts integers between 1 and 365, inclusive. The default value is 5.</p> </div>
<code>arw.snap.create.interval.hours.post.max.count</code>	<p>Specifies the interval <i>in hours</i> between ARP Snapshot copies when the volume already contains the maximum number of ARP Snapshot copies. When the maximum number is reached, an ARP Snapshot copy is deleted to make room for a new copy. The new ARP Snapshot copy creation speed can be reduced to retain the older copy using this option. If the volume already contains the maximum number of ARP Snapshot copies, the interval specified in this option is used for next ARP Snapshot copy creation, instead of <code>arw.snap.create.interval.hours</code>.</p> <p>The <code>-option-value</code> parameter accepts integers between 4 and 48, inclusive. The default value is 8.</p>
<code>arw.surge.snap.interval.days</code>	<p>Specifies the interval <i>in days</i> between ARP Snapshot copies 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 copy is older than this specified interval. This option also specifies retention period <i>in day</i> for an ARP surge Snapshot copies.</p> <p>The <code>-option-value</code> parameter accepts integers between 1 and 365, inclusive. The default value is 5.</p>

ARW setting	Description
<code>arw.snap.new.extns .interval.hours</code>	<p>This option specifies the interval <i>in hours</i> between the ARP Snapshot copies created when a new file extension is detected. A new ARP Snapshot copy is created when</p> <p>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 in controlling the frequency of the ARP Snapshot copies. This option exists independent of <code>arw.snap.create.interval.hours</code>, which specifies the interval for data entropy-based ARP Snapshot copies.</p> <p>The <code>-option-value</code> parameter accepts integers between 24 and 8760. The default value is 48.</p>

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.