Protect against ransomware attacks

ASA r2

NetApp
February 11, 2026

Table of Contents

Protect against ransomware attacks

Create tamper-proof snapshots to protect against ransomware attacks on ASA r2 storage systems

For enhanced protection against ransomware attacks, replicate snapshots to a remote cluster, then lock the destination snapshots to make them tamper-proof. Locked snapshots cannot be deleted accidentally or maliciously. You can use locked snapshots to recover data if a storage unit is ever compromised by a ransomware attack.

Initialize the SnapLock compliance clock

Before you can create tamper-proof snapshots, you must initialize the SnapLock compliance clock on your local and destination clusters.

Steps

1. Select **Cluster > Overview**.
2. In the **Nodes** section, select **Initialize SnapLock Compliance Clock**.
3. Select **Initialize**.
4. Verify that the compliance clock is initialized.
   a. Select **Cluster > Overview**.
   b. In the **Nodes** section, select ; then select **SnapLock Compliance Clock**.

What's next?

After you have initialized the SnapLock compliance clock on your local and destination clusters, you are ready to create a replication relationship with locked snapshots.

Enable autonomous ransomware protection with AI on your ASA r2 storage systems

Beginning with ONTAP 9.17.1, you can use Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) to protect the data on your ASA r2 system. ARP/AI quickly detects potential ransomware threats, automatically creates an ARP snapshot to protect your data, and displays a warning message in System Manager to alert you of suspicious activity.

ARP improves cyber resiliency by adopting a machine-learning model for anti-ransomware analytics that detects constantly evolving forms of ransomware with 98% accuracy for SAN 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, and the pre-trained model that results from this training is included on-box with ONTAP. This model is not accessible or modifiable. ARP/AI is active immediately after enablement; there is no learning period.

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

About this task

- ARP/AI support is included with the ONTAP One license.
- ARP/AI is not supported on storage units protected by SnapMirror active sync, SnapMirror synchronous or SnapLock.
- Beginning with ONTAP 9.18.1, ARP/AI is enabled by default on all newly created storage units 12 hours after upgrading to ONTAP 9.18.1 or initializing a new ONTAP 9.18.1 ASA r2 cluster.
- After you have enabled ARP/AI, you should enable automatic updates for your security files to automatically receive new security updates.

Enable ARP/AI on all storage units in the cluster

If you are running ONTAP 9.17.1, you can enable ARP/AI on all storage units created in the cluster by default.

In ONTAP 9.18.1 and later, ARP/AI is enabled by default on all new storage units. If you have storage units created in ONTAP 9.17.1 for which ARP/AI is not enabled, you can enable it manually.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Next to **Anti-ransomware**, select ⋮ and then select **Enable on all existing storage units**.
3. Select **Enable**.

Enable ARP/AI on all storage units in a storage VM

If you are running ONTAP 9.17.1, you can enable ARP/AI on all storage units created in a storage virtual machine (VM) by default. This means that any new storage units created in the storage VM will have ARP/AI enabled automatically. You can also apply ARP/AI to existing storage units in the storage VM.

In ONTAP 9.18.1 and later, ARP/AI is enabled by default on all new storage units. If you have storage units created in ONTAP 9.17.1 for which ARP/AI is not enabled, you can enable it manually.

Steps

1. In System Manager, select **Cluster > Storage VMs**.
2. Select the storage VM on which you want to enable ARP/AI.
3. In the **Security** section, next to **Anti-ransomware**, select ⋮; then select **Edit anti-ransomware settings**.
4. Select **Enable anti-ransomware**.

   This enables ARP/AI on all future storage units created on the selected storage VM by default.

5. To apply ARP to existing storage units on the selected storage VM, select **Apply this change to all applicable existing storage units on this storage VM**.
6. Select **Save**.

Result

All new storage units you create on the storage VM are protected against ransomware attacks by default, and suspicious activity is reported to you in System Manager.

Enable ARP/AI on specific storage units in a storage VM

If you are running ONTAP 9.17.1, and you do not want ARP/AI enabled on all the storage units in an storage VM, you can select the specific units you want enabled.

In ONTAP 9.18.1 and later, ARP/AI is enabled by default on all new storage units. If you have storage units created in ONTAP 9.17.1 for which ARP/AI is not enabled, you can enable it manually.

Steps

1. In System Manager, select **Storage**.
2. Select the storage units for which you want to enable ARP/AI.
3. Select ⋮; then select **Enable anti-ransomware**.
4. Select **Enable**.

Result

The storage units you selected are protected against ransomware attacks, and suspicious activity is reported to you in System Manager.

Disable default autonomous ransomware protection on your ASA r2 storage systems

When you initialize a new ONTAP 9.18.1 ASA r2 cluster or upgrade your cluster to ONTAP 9.18.1, ARP/AI is automatically enabled by default on all new storage units after a 12-hour grace period. If you don’t disable ARP/AI during the grace period, it is enabled cluster-wide for new storage units when the grace period ends.

Storage units created in ONTAP 9.17.1 must be manually enabled for ARP/AI.

Steps

You can disable the default enablement during or after the initial 12-hour grace period.

System Manager

1. Select **Cluster > Settings**.
2. Disable ARP:
   - To disable during the 12-hour grace period:
     a. Under **Anti-ransomware**, select **Don't enable** and then select **Disable**.
   - To disable after the 12-hour grace period:
     a. Under **Anti-ransomware**, select and then deselect **Enable for new storage units**.
     b. Select **Save**

CLI

1. Check the default enablement status:

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

2. Disable default enablement for existing and new volumes:

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

Modify ARP/AI snapshot retention periods on ASA r2 storage systems

If Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) detects abnormal activity on one or more of your ASA r2 system storage units, it automatically creates an ARP snapshot to protect the storage unit's data. Depending upon your storage capacity and the business requirements for your data, you might want to increase or decrease the default ARP snapshot retention period. For example, you might want to increase the retention period for business critical applications so that, if needed, you have longer retention periods for data recovery, or you might want to decrease the retention period for non-critical applications to save storage space.

The default retention period for the ARP snapshot varies depending on the action you take in response to the abnormal activity.

If you take this action…	ARP snapshots are retained by default for…
Mark as false positive	12 hours
Mark as potential ransomware attack	7 days
Do not take immediate action	10 days

The default retention periods can be modified using the ONTAP command line interface (CLI). See Modify

options for ONTAP automatic snapshots for steps to change the default retention period.

Respond to autonomous ransomware protection with AI alerts on ASA r2 storage systems

If Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) detects abnormal activity on one or more of your ASA r2 system storage units, a warning is generated on the System Manager dashboard. You should view the warning, verify the activity and, if necessary, take action to stop any potential threat to your data.

If an ARP/AI warning message is displayed, before you take action, you should use the appropriate application integrity checker to verify the integrity of the data on the storage unit. Verifying the storage unit's data integrity helps you determine if the activity is acceptable or if it is a potential ransomware attack.

If the abnormal activity is …	Then do this…
Acceptable	Mark the activity as a false positive.
A potential ransomware attack	Mark the activity as a potential ransomware attack.
Indeterminate	Do not take immediate action. Monitor the storage unit to for up to 7 days. If the storage unit continues to operate normally, mark the activity as a false positive. If the storage unit continues to exhibit abnormal activity, mark the activity as a potential ransomware attack.

Steps

1. In System Manager, select **Dashboard**.

   If ARP has detected abnormal activity on one or more storage units, a message appears under **Warnings**.

2. Select the warning message.
3. Under **Events overview**, select the **Warnings** message that indicates the number of storage units with abnormal activity.
4. Under **Storage units with abnormal activity**, select the storage unit.
5. Select **Security**.

   If there is abnormal activity on the storage unit, a message is displayed under **Anti-ransomware**.

6. Select **Choose an action**.
7. Select **Mark as false positive** or select **Mark as potential ransomware attack**.

What's next?

If you know of surges in your storage unit 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. Learn how to report known ARP/AI surges.

Pause or resume autonomous ransomware protection with AI on your ASA r2 storage systems

Beginning with ONTAP 9.17.1, you can use Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) to protect the data on your ASA r2 system. If you are planning an unusual workload event, you can temporarily suspend ARP/AI analysis to prevent false positive detections of ransomware attacks. After your workload event is complete, you can resume ARP/AI analysis.

Pause ARP/AI

Before you begin an unusual workload event, you might need to temporarily suspend the ARP/AI analysis to prevent false positive detections of ransomware attacks.

Steps

1. In System Manager, select **Storage**.
2. Select the storage units for which you want to pause ARP/AI.
3. Select **Pause anti-ransomware**.

Result

ARP/AI analysis is paused for the selected storage units, and no suspicious activity is reported to you in System Manager until you resume ARP/AI.

Resume ARP/AI

If you pause ARP/AI during an unusual workload, after your workload is complete, you should resume it to protect your data against ransomware attacks.

Steps

1. In System Manager, select **Storage**.
2. Select the storage units for which you want to resume ARP/AI.
3. Select **Resume anti-ransomware**.

Result

Analysis of potential ransomware attacks is resumed, and suspicious activity is reported to you in System Manager.

Copyright information

Trademark information