Ransomware protection

ONTAP 9

NetApp
August 04, 2022

Table of Contents

Ransomware protection

Anti-ransomware overview

Beginning with ONTAP 9.10.1, the anti-ransomware 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, anti-ransomware also creates new Snapshot copies, in addition to existing protection from scheduled Snapshot copies.

The anti-ransomware feature is enabled with the following licenses.

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 anti-ransomware protection is already configured on your system, you do not need to purchase the new Anti-ransomware license. For new anti-ransomware 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 anti-ransomware protection with the Anti-ransomware license, you will see a warning message and might need to reconfigure anti-ransomware. Learn about reverting anti-ransomware protection.

You can configure anti-ransomware protection on a per-volume basis using either ONTAP System Manager or the ONTAP command line interface (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 wouldn't want to 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 ONTAP anti-ransomware 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 ONTAP anti-ransomware detects

There are two types of ransomware attacks:

1. Denial of service to files by encrypting data.

The attacker withholds access to this data unless a ransom is paid.

2. Theft of sensitive proprietary data.
   The attacker threatens to release this data to the public domain unless a ransom is paid.

ONTAP ransomware protection addresses the first type, with an anti-ransomware detection mechanism that is based on:

1. Identification of the incoming data as encrypted or plaintext.
2. Analytics, which detects
   - High data *entropy* (an evaluation of the randomness of data in a file)
   - A surge in abnormal volume activity with data encryption
   - An extension that does not conform to the normal extension type

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

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 to this proactively taken snapshot, minimizing the data loss.

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 snapshots.

Anti-ransomware 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

Anti-ransomware use cases and considerations

ONTAP platform support:

- The anti-ransomware feature is available for all on-premises ONTAP systems beginning with ONTAP 9.10.1.
- It is not currently available in Cloud Volumes ONTAP environments.

Suitable workloads:

- 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 greater possibility of false positives in this workload.

- Images and video

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

Unsuitable workloads:

- Workloads with a high frequency of file create or delete (hundreds of thousands of files in few seconds; for example, test/dev workloads)
- The anti-ransomware feature depends on the ability to recognize an unusual surge in file create 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
  The anti-ransomware feature 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 (create, delete, and overwrite) and file type.

Unsupported system configurations:

- SAN environments
- ONTAP S3 environments
- VMDKs on NFS

Volume requirements:

- Less than 100% full
- Junction path must be active

Unsupported volume types:

- offline volumes
- restricted volumes
- SnapLock volumes
- FlexGroup volumes
- FlexCache volumes (the anti-ransomware feature is supported on origin FlexVol volumes but not on cache volumes)
- SAN-only volumes
- volumes of stopped storage VMs
- root volumes of storage VMs
- data protection volumes

Anti-ransomware performance and frequency considerations

The anti-ransomware feature can have a minimal impact on system performance as measured in throughput and peak IOPS. The impact of the anti-ransomware feature is highly dependent on volume workloads. For most typical or 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 anti-ransomware analytics are run in a prioritized sequence, as the number of protected volumes increases, analytics are run on each volume less frequently.

How automatic Snapshot copies work when ransomware is detected

In order to obtain the best possible recovery point, the anti-ransomware feature creates an automatic Snapshot copy as soon as it detects abnormal file activity. However, the anti-ransomware feature does not immediately flag an alert; rather, analytics need to run and confirm that the suspicious activity matches a ransomware profile before generating an alert. This process could take up to 60 minutes. If the analytics determines the activity is not suspicious, then an alert is not generated, but the automatically created Snapshot copy remains present on the file system for a minimum of two days.

Beginning with ONTAP 9.11.1, you can control the number and retention period for anti-ransomware Snapshot copies that are automatically generated in response to suspected ransomware attacks. Learn how to modify options for automatic Snapshot copies.

Enable anti-ransomware

Beginning with ONTAP 9.10.1, anti-ransomware protection can be enabled on new or existing volumes. You first enable anti-ransomware in learning mode, in which the system analyzes the workload to characterize normal behavior, then you switch to active mode, in which abnormal activity is flagged for your evaluation.

What you'll need

- A storage VM enabled for NFS or SMB (or both).
- The correct license is installed for your ONTAP version.

ONTAP releases	License
ONTAP 9.8-9.10.1	MT_EK_MGMT (Multi-Tenant Key Management)
ONTAP 9.11.1 and later	Anti_ransomware

- An NAS workload with clients configured.
- The volume to be protected must have an active junction-path.
- Optional but recommended: The EMS system is configured to send email notifications, which will include notices of anti-ransomware activity. For more information, see Configure EMS events to send email notifications.

About this task

The NetApp anti-ransomware feature includes an initial learning period (also known as “dry run”), in which an ONTAP system learns which file extensions are valid and uses the analyzed data to develop alert profiles. After running anti-ransomware in learning mode for enough time to assess workload characteristics, you can switch to active mode and start protecting your data. Anti-ransomware continues to collect and analyze data to refine alert profiles.

During the learning period, the system automatically learns the workload characteristics of a configured volume, performing special observations and pattern analysis.

A learning period of 30 days is recommended. Although you can switch from learning to active mode anytime, switching early may lead to too many false positives.

In the ONTAP CLI, you can use the security anti-ransomware volume workload-behavior show command to show file extensions detected to date. However, it is recommended that you not use this tool to shorten the learning period.

You can enable ransomware protection on an existing volume, or you can create a new volume and enable ransomware protection from the beginning.

> 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 the anti-ransomware feature.

In the ONTAP CLI, a new command family has been introduced to manage this feature: `security anti-ransomware volume`. You can also use the `volume modify` command with the `-anti-ransomware` parameter to manage the feature.

System Manager procedure

1. Click **Storage > Volumes** and then select the volume you want to protect.
2. In the Security tab of the Volumes overview, click **Status** to switch from Disabled to Enabled in learning-mode in the Anti-ransomware box.
3. When the learning period is over, switch anti-ransomware to active mode.
   a. Click **Storage > Volumes** and then select the volume that is ready for active mode.
   b. In the Security tab of the Volumes overview, click **Switch** to active mode in the Anti-ransomware box.
4. You can always verify the anti-ransomware state of the volume in the Anti-ransomware box.
   To display anti-ransomware status for all volumes: In the Volumes pane, click **Show/Hide**, then ensure that Anti-ransomware status is checked.

CLI procedure

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

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

You can also enable ransomware with the `volume modify` command:

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

At the CLI, you can also 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
```

> You should always enable ransomware initially in the dry-run state. Beginning with the active state can lead to excessive false positive reports.

2. When the learning period is over, modify the protected volume to switch to active mode:

```
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 anti-ransomware state of the volume.

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

Enable anti-ransomware 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 anti-ransomware in learning mode.

What you'll need

- The correct license is installed for your ONTAP version.

ONTAP releases	License
ONTAP 9.11.1 and later	Anti_ransomware
ONTAP 9.8-9.10.1	MT_EK_MGMT (Multi-Tenant Key Management)

About this task

New volumes are created by default with anti-ransomware in disabled mode, but you can change this setting in System Manager and at the CLI. Volumes enabled by default are set to anti-ransomware in learning mode.

System Manager procedure

1. Click **Storage > Storage VMs** and then select the storage VM for default anti-virus.

2. In the **Settings** tab, [in the **Security** section], click in the **Anti-ransomware** box, then check the box to enable anti-ransomware for NAS volumes.

CLI procedure

1. Modify an existing SVM to enable anti-ransomware 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 anti-ransomware enabled by default for new volumes.
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

Pause anti-ransomware to exclude workload events from analysis

If you are expecting unusual workload events, you can temporarily suspend and resume anti-ransomware analysis at any time.

What you'll need

- Anti-ransomware is running in learning or active mode.

About this task

During an anti-ransomware 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 anti-ransomware disable function to pause analytics. Doing so disables anti-ransomware on the volume and all the existing information around learned workload behavior is lost. This would require a restart of the learning period.

System Manager procedure

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

CLI procedure

Pause ransomware protection on a volume:

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

To resume processing, use the resume parameter.

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

Respond to abnormal activity.

When anti-ransomware detects abnormal activity in a protected volume, it issues a warning. You should evaluate the notification to determine whether the activity is

expected and acceptable, or whether an attack is under way.

What you'll need

- Anti-ransomware is running in active mode.

About this task

Anti-ransomware 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, you can respond by marking 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; anti-ransomware records your evaluation, logs are updated with the new file types and using them for future analysis. However, 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. For more information, see How to recover from a ransomware attack.

There are no notices to clear if you restored an entire volume.

System Manager procedure

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

   Warnings are displayed in the Overview pane of the Events window.

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

   In the **Security** tab, click 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	Click **Update** and **Clear Suspect File Types** to record your decision and resume normal anti-ransomware monitoring.
Potential Ransomware Attack	Respond to the attack and restore protected data. Then click **Update** and **Clear Suspect File Types** to record your decision and resume normal anti-ransomware monitoring. There are no suspect file types to clear if you restored an entire volume.

CLI procedure

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 restore data. Then enter the following command to record your decision and resume normal anti-ransomware 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.

Restore data after an attack

Snapshot copies named “Anti_ransomware_backup” are created when anti-ransomware detects a potential attack. You can restore data from these anti-ransomware copies or other Snapshot copies.

If a ransomware attack occurs, see the Knowledge Base article Ransomware prevention and recovery in ONTAP for additional information on recovery and future mitigation.

What you’ll need

- Anti-ransomware enabled
- Reports from potential ransomware attacks

System Manager procedure

1. Display the Snapshot copies in volumes identified in a potential attack:
   Click **Storage > Volumes**, select the volume, then click the Snapshot Copies tab.
2. Restore the desired copies according to these instructions:
   Recover from Snapshot copies

CLI procedure

1. Display the Snapshot copies in volumes identified in a potential attack:
   `volume snapshot show -vserver svm_name -volume vol_name`
2. Restore the desired copies according to these instructions:
   Restoring files from Snapshot copies

Modify options for automatic Snapshot copies

Beginning with ONTAP 9.11.1, you can control the number and retention period for anti-ransomware (ARW) Snapshot copies that are automatically generated in response to suspected ransomware attacks.

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

The following options for automatic Snapshot copies can be modified:

arw.snap.max.count

Specifies the maximum number of ARW Snapshot copies that can exist in a volume at any given time. Older copies are deleted to ensure that the total number of ARW Snapshot copies are within this specified limit.

arw.snap.create.interval.hours

Specifies the interval (in hours) between ARW Snapshot copies. A new Snapshot copy will be created when an attack is suspected and the copy created previously is older than this specified interval.

arw.snap.normal.retain.interval.hours

Specifies the duration (in hours) for which an ARW Snapshot copy is retained. When an ARW Snapshot copy becomes this old, any other ARW Snapshot copy created before the latest copy to reach this age is deleted. No ARW Snapshot copy can be older than this duration.

arw.snap.max.retain.interval.days

Specifies the maximum duration (in days) for which an ARW Snapshot copy can be retained. Any ARW Snapshot copy older than this duration will be deleted if there is no attack reported on the volume.

arw.snap.create.interval.hours.post.max.count

Specifies the interval (in hours) between ARW Snapshot copies when the volume already contains the maximum number of ARW Snapshot copies. When the maximum number is reached, an ARW Snapshot copy is deleted to make room for a new copy. The new ARW Snapshot copy creation speed can be reduced to retain the older copy using this option. If the volume already contains maximum number of ARW Snapshot copies, then this interval specified in this option is used for next ARW Snapshot copy creation, instead of arw.snap.create.interval.hours.

arw.surge.snap.interval.days

Specifies the interval (in days) between ARW surge Snapshot copies. A new ARW Snapshot surge copy is created when there is a surge in IO traffic and the last created ARW Snapshot copy is older than this specified interval. This option also specifies the duration (in days) for which an ARW surge Snapshot copy is retained.

CLI procedure

To show all current ARW Snapshot copy settings, enter:
`vserver options -vserver` *`svm_name`* `arw*`

To show selected current ARW Snapshot copy settings, enter:
`vserver options -vserver` *`svm_name`* `-option-name` *`arw_setting_name`*

To modify ARW Snapshot copy settings, enter:

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