Lenovo

Ransomware protection

ONTAP

Fourth edition (September 2023)

Contents

Chapter 1. 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 actively 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.

The ARP feature is enabled with the following licenses.

ONTAP releases	License
ONTAP 9.10.1 to ONTAP 9.13.1	Multi-Tenant Key Management

You can configure ARP on a per-volume basis using either ThinkSystem Storage Manager for DM Series or the ONTAP command line interface (CLI).

1.1. 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, and SnapLock, the following information focuses on the ONTAP ARP on-box feature with machine-learning capabilities.

To learn more about ONTAP's other anti-ransomware features, see: Lenovo Solution for Ransomware

1.2. What ONTAP ARP 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 ARP 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, Lenovo ARP acts as an important additional layer of defense if anti-virus software has failed to detect an intrusion. 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.

1.3. 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 previously 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.

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 (Storage Manager)
- Restoring files from Snapshot copies (CLI)

Chapter 2. Autonomous Ransomware Protection use cases and considerations

ONTAP platform support:

- The Autonomous Ransomware Protection (ARP) feature is available for all on-premises ONTAP systems beginning with ONTAP 9.10.1.

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.

Beginning with ONTAP 9.12.1, ARP is available for these configurations:

- Volumes protected with SnapMirror
- SVMs protected with SnapMirror
- SVMs enabled for migration (SVM data mobility)

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)
- ARP depends on the ability to 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.

Unsupported system configurations:

- SAN environments
- ONTAP S3 environments
- VMDKs on NFS

- Cloud Volumes ONTAP

Volume requirements:

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

Unsupported volume types:

- Offline volumes
- Restricted volumes
- SnapLock volumes
- FlexGroup volumes (beginning with ONTAP 9.13.1, FlexGroup volumes are supported)
- FlexCache volumes (ARP is supported on origin FlexVol volumes but not on cache volumes)
- SAN-only volumes
- Volumes of stopped storage VMs
- Root volumes of storage VMs

2.1. SnapMirror and ARP interoperability

Beginning with ONTAP 9.12.1, ARP is supported on SnapMirror destination volumes. 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.

2.2. ARP performance and frequency considerations

The ARP feature can have a minimal impact on system performance as measured in throughput and peak IOPS. The impact of the ARP 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

Workload characteristics	Recommended volume limit per node	Performance degradation when per-node volume limit is exceeded *
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 are run in a prioritized sequence, as the number of protected volumes increases, analytics are run on each volume less frequently.

2.3. How automatic Snapshot copies work when ransomware is detected

In order to obtain the best possible recovery point, ARP creates an automatic Snapshot copy as soon as it detects abnormal file activity. However, ARP 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 ARP Snapshot copies that are automatically generated in response to suspected ransomware attacks. Learn how to modify options for automatic Snapshot copies.

2.4. Multi-admin verification with volumes protected with Autonomous Ransomware Protection (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'll 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.

Chapter 3. Enable Autonomous Ransomware Protection

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. Then you switch to active mode, in which abnormal activity is flagged for your evaluation. You can enable ARP on an existing volume, or you can create a new volume and enable ARP from the beginning.

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 9.10.1 to 9.13.1	Multi-Tenant Key Management

- 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 ARP activity. For more information, see Configure EMS events to send email notifications.
- Optional but recommended: Beginning in ONTAP 9.13.1, you can enable multi-admin verification (MAV) so that two or more authenticated user admins are required for Autonomous Ransomware Protection (ARP) configuration. Learn more.

About this task

The ARP 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 ARP in learning mode for 30 days recommended to assess workload characteristics, you can switch to active mode and start protecting your data. 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.

Although you can switch from learning to active mode anytime, a learning period of 30 days is recommended. Switching early might lead to too many false positives. The adaptive learning introduced in ONTAP 9.13.1 might determine that a shorter period is sufficient. In the ONTAP CLI, you can use the `security anti-ransomware volume workload-behavior show` command to show file extensions detected to date. It is recommended that you not use this tool to shorten the learning period.

In active mode, if a file extension is flagged as abnormal, but then you evaluate it and mark it as a false positive, the alert profile is updated so that the extension is not flagged as abnormal in future

alerts.

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.

To manage this feature in the ONTAP CLI, you can use the `security anti-ransomware volume` command. You can also use the `volume modify` command with the `-anti-ransomware` parameter.

Example 1. Steps

Storage Manager

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 ARP to active mode.

   If you have upgraded to 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. 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 ARP state of the volume in the **Anti-ransomware** box.
   To display ARP status for all volumes: In the **Volumes** pane, click **Show/Hide**, then ensure that **Anti-ransomware** status is checked.

CLI

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 protection 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 ARP initially in the dry-run (learning mode) state. Beginning in the active state can lead to excessive false positive reports.

   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, change the setting at the Vserver 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
   ```

Chapter 4. Enable Autonomous Ransomware Protection by default in new volumes

Beginning with ONTAP 9.10.1, anti-ransomware protection can be enabled by default for Autonomous Ransomware Protection (ARP) in learning mode.

What you'll need

- The correct license is installed for your ONTAP version.

ONTAP releases	License
ONTAP 9.10.1 to 9.13.1	Multi-Tenant Key Management

- Optional but recommended: Beginning in ONTAP 9.13.1, you can enable multi-admin verification (MAV) so that two or more authenticated user admins are required for anti-ransomware operations. Learn more.

About this task

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

Enabling ARP by default for new volumes in an SVM does not automatically enable ARP for existing volumes in that SVM. Learn how to enable ARP in an existing volume.

Autonomous ARP switching from learning to active mode

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. 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
```

Storage Manager

1. Click **Storage > Storage VMs** and then select the storage VM that contains volumes you want to protect with ARP.
2. In the **Settings** tab, [in the **Security** section], click  in the **Anti-ransomware** box, then 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`

Chapter 5. 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.

What you'll need

- ARP is running in learning or active mode.

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.

Example 2. Steps

Storage Manager

1. Click **Storage > Volumes** and then select the volume where you want to pause ARP.
2. In the Security tab of the Volumes overview, click **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` parameter.

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

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 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:

1. Show the request:

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

2. 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]
```

Chapter 6. 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 expected and acceptable, or whether an attack is under way.

What you'll need

- ARP is running in active mode.

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, 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; ARP 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.

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

Example 3. Steps

Storage Manager

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 ARP monitoring.  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.
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 ARP monitoring. There are no suspect file types to clear if you restored an entire volume.

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 does the following:

   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]
```

Chapter 7. Restore data after a ransomware attack

Snapshot copies named “Anti_ransomware_backup” are created when Autonomous Ransomware Protection (ARP) detects a potential attack. You can restore data from these ARP copies or from other Snapshot copies.

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.

What you’ll need

- ARP enabled
- Reports from potential ransomware attacks

Steps

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

Storage Manager

1. If you want to restore data from earlier Snapshot copies, instead of from the ARP copies, you must do the following to release the anti-ransomware Snapshot lock. If you want to restore from the ARP copies, it is not necessary to release the lock and you can skip this step.

If a system attack was identified do this…	If a system attack was not identified do this…
a. Click **Storage > Volumes**. b. Select **Security**, and click **View Suspected File Types** c. Mark the files as "False Positive" . d. Click **Update** and **Clear Suspect File Types**	To release the Snapshot lock, you must restore from the ARP copies before you restore from earlier Snapshot copies. Follow steps 2-3 to restore data from the ARP copies, then repeat the process to restore from earlier Snapshot copies.

2. Display the Snapshot copies in volumes:

   Click **Storage > Volumes**, select the volume, and click **Snapshot Copies**.

3. Click ⋮ next to the Snapshot copy you want to restore, and select **Restore**.

CLI

1. If you want to restore data from earlier Snapshot copies, instead of from the ARP copies, you must do the following to release the anti-ransomware Snapshot lock. If you want to restore from the ARP copies, it is not necessary to release the lock and you can skip this step.

   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.

If a system attack was identified do this…	If a system attack was not identified do this…
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".	To release the Snapshot lock, you must restore from the ARP copies before you restore from earlier Snapshot copies. Follow steps 2-3 to restore data from the ARP copies, then repeat the process to restore from earlier Snapshot copies.

2. 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.
```

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
```

Chapter 8. Modify options for automatic Snapshot copies

Beginning with ONTAP 9.11.1, you can use the CLI to control the number and retention period for Autonomous Ransomware Protection (ARP) 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 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.

arw.snap.create.interval.hours

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

arw.snap.max.retain.interval.days

Specifies the maximum duration (in days) for which an ARP Snapshot copy can be retained. Any ARP 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 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 maximum number of ARP Snapshot copies, then this interval specified in this option is used for next ARP Snapshot copy creation, instead of arw.snap.create.interval.hours.

arw.surge.snap.interval.days

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

ARP surge Snapshot copy is retained.

CLI procedure

To show all current ARP Snapshot copy settings, enter:

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

To show selected current ARP Snapshot copy settings, enter:

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

To modify ARP Snapshot copy settings, enter:

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

Chapter 9. Appendix

9.1. Contacting support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/supportphonelist for your region support details.

9.2. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

```
Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing
```

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information

contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

9.3. Trademarks