



security anti-ransomware commands

Command reference

NetApp
July 17, 2026

Table of Contents

- security anti-ransomware commands 1
 - security anti-ransomware show 1
 - Description 1
 - Parameters 1
 - Examples 1
 - security anti-ransomware update-package-from-uri 1
 - Description 2
 - Parameters 2
 - Examples 2
 - security anti-ransomware auto-enable modify 2
 - Description 2
 - Parameters 2
 - Examples 3
 - security anti-ransomware auto-enable show 3
 - Description 3
 - Parameters 3
 - Examples 3
 - security anti-ransomware volume disable 4
 - Description 4
 - Parameters 4
 - Examples 4
 - security anti-ransomware volume dry-run 4
 - Description 5
 - Parameters 5
 - Examples 5
 - security anti-ransomware volume enable 5
 - Description 5
 - Parameters 5
 - Examples 5
 - security anti-ransomware volume pause 5
 - Description 6
 - Parameters 6
 - Examples 6
 - security anti-ransomware volume resume 6
 - Description 6
 - Parameters 6
 - Examples 6
 - security anti-ransomware volume show 6
 - Description 6
 - Parameters 7
 - Examples 8
 - security anti-ransomware volume attack clear-suspect 9
 - Description 9

Parameters	9
Examples	10
security anti-ransomware volume attack generate-report	10
Description	10
Parameters	10
Examples	10
security anti-ransomware volume attack-detection-parameters modify	11
Description	11
Parameters	11
Examples	13
security anti-ransomware volume attack-detection-parameters show	14
Description	15
Parameters	15
Examples	16
security anti-ransomware volume auto-switch-to-enable-mode show	17
Description	17
Parameters	17
Examples	18
security anti-ransomware volume entropy-stat show-encryption-percentage-histogram	18
Description	18
Parameters	19
Examples	19
security anti-ransomware volume entropy-stat show-recent-daily-stat	20
Description	20
Parameters	20
Examples	21
security anti-ransomware volume entropy-stat show-recent-high-encryption-stat	22
Description	22
Parameters	22
Examples	23
security anti-ransomware volume entropy-stat show-recent-hourly-stat	23
Description	23
Parameters	23
Examples	24
security anti-ransomware volume entropy-stat show-recent-sub-hourly-stat	24
Description	24
Parameters	24
Examples	25
security anti-ransomware volume event-log modify	26
Description	26
Parameters	26
Examples	26
security anti-ransomware volume event-log show	27
Description	27
Parameters	27

security anti-ransomware volume space show	28
Description	28
Parameters	28
Examples	28
security anti-ransomware volume workload-behavior clear-surge	29
Description	29
Parameters	29
Examples	29
security anti-ransomware volume workload-behavior show	30
Description	30
Parameters	31
Examples	32
security anti-ransomware volume workload-behavior update-baseline-from-surge	33
Description	33
Parameters	33
Examples	33
security anti-ransomware vserver event-log modify	34
Description	34
Parameters	34
security anti-ransomware vserver event-log show	35
Description	35
Parameters	35
Examples	35

security anti-ransomware commands

security anti-ransomware show

Display Anti-ransomware Package Version of the Node

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security anti-ransomware show` command displays the Anti-ransomware version of a node.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node {<nodename>|local}] - Node Name

If this parameter is specified, the command displays the Anti-ransomware version of specified node.

[-version <text>] - Anti-Ransomware Version

If this parameter is specified, the command displays node with the specified Anti-ransomware version.

Examples

The following example shows a sample output for this command:

```
C1_cluster::*> security anti-ransomware show-version
Node                      Version
-----
sti221-vsrm-sr049g      1.0
sti221-vsrm-sr049h      1.0
2 entries were displayed.
```

security anti-ransomware update-package-from-uri

Install the new Anti-ransomware package in the cluster

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security anti-ransomware update-package-from-uri` command downloads a new Anti-ransomware package to replace the version installed in all nodes of the cluster.

Use only Anti-ransomware package provided by NetApp support for ONTAP with this command."

To update the Anti-ransomware package, perform the following steps:

- Download the required Anti-ransomware package file from the NetApp support website.
- Place the downloaded package file (.tgz) on a local web server that the cluster can access without a password.
- Execute the `security anti-ransomware update-package-from-uri` command, passing the Universal Resource Identifier (URI) of the file as a parameter.



"The command only needs to be executed once for the entire cluster. It will then download and install the package on each node."

Parameters

-uri {scheme: //(hostname|IPv4 Address|['IPv6 Address'])...} - URI of Anti-ransomware package

URI of the new Anti-ransomware package.

Examples

The following example installs a new version of the Anti-ransomware to the cluster:

```
cluster1::> security anti-ransomware update-package-from-uri
http://www.example.com/auDev__ontap_arpml_package_v1.0.tgz__440ae2e4-fd8f-
4225-9bee-94e2da3f9d8d.tgz
```

security anti-ransomware auto-enable modify

security anti-ransomware auto-enable modify

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security anti-ransomware auto-enable modify` command changes the cluster-level auto enablement setting for new volumes.

Parameters

[-new-volume-auto-enable {true|false}] - Auto-enable ARP Setting for New Volumes

Sets the Auto-Enable Anti-Ransomware Protection setting for newly created volumes. Specify *true* to automatically enable Anti-Ransomware on new volumes.

`[-warm-up-period-total-duration <time_interval>]` - Warm-up Period Total Duration

Sets the total duration of the warm-up period.

Examples

```
cluster1::> security anti-ransomware auto-enable modify -new-volume-auto
-enable false -warm-up-period-total-duration 24h
```

Disables auto-enablement of Anti-Ransomware protection for new volumes and adjusts warm-up period duration to 24 hours.

```
cluster1::> security anti-ransomware auto-enable show
New Volume Auto-Enable:           false
Warm-Up Period Applicable:        true
Warm-Up Period Completed:         false
Warm-Up Period Duration:          24h
Warm-Up Period Time Remaining:    10h
```

After warm-up period ends, warm-up related fields wont be displayed.

```
cluster1::> security anti-ransomware auto-enable show
New Volume Auto-Enable:           false
```

security anti-ransomware auto-enable show

Show the auto-enable anti-ransomware setting for the cluster

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security anti-ransomware auto-enable show` command retrieves the current anti-ransomware auto enablement values, including details about warm-up period and auto enablement setting for new volumes.

Parameters

`[-instance ]`

If you specify the `-instance` parameter, the command displays detailed information about all fields.

Examples

The following example shows a sample output for this command:

```
cluster1::> security anti-ransomware auto-enable show
New Volume Auto-Enable:      true
Warm-Up Period Applicable:   true
Warm-Up Period Completed:    false
Warm-Up Period Duration:     12h
Warm-Up Period Time Remaining: 10h
```

After warm-up period ends, warm-up related fields wont be displayed.

```
cluster1::> security anti-ransomware auto-enable show
New Volume Auto-Enable:      true
```

security anti-ransomware volume disable

Disable anti-ransomware on a volume

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume disable` command disables anti-ransomware monitoring on a volume.

Parameters

-vserver <vserver name> - Vserver Name

Anti-ransomware monitoring is disabled on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

-volume <volume name> - Volume Name

Anti-ransomware monitoring is disabled on volumes matching the parameter value.

[-auto-enabled-volumes-only {true|false}] - Option to disable only on auto enabled volumes (privilege: advanced)

Anti-ransomware monitoring will be disabled on volumes matching the parameter value.

Examples

security anti-ransomware volume dry-run

(DEPRECATED) Dry-run anti-ransomware on a volume (DEPRECATED: All fields to this command are deprecated)

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume dry-run` command starts anti-ransomware monitoring in the evaluation mode on a volume. Depreciated: This command is no longer supported and may be removed in a future release.

Parameters

-vserver <vserver name> - Vserver Name

Anti-ransomware monitoring is enabled in the evaluation mode on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter. Depreciated: This parameter is no longer supported and may be removed in a future release.

-volume <volume name> - Volume Name

Anti-ransomware monitoring is enabled in the evaluation mode on volumes matching the parameter value. Depreciated: This parameter is no longer supported and may be removed in a future release.

Examples

security anti-ransomware volume enable

Enable anti-ransomware on a volume

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume enable` command enables anti-ransomware monitoring on a volume.

Parameters

-vserver <vserver name> - Vserver Name

Anti-ransomware monitoring is enabled on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

-volume <volume name> - Volume Name

Anti-ransomware monitoring is enabled on volumes matching the parameter value.

Examples

security anti-ransomware volume pause

Pause anti-ransomware on a volume

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume pause` command pauses Anti-ransomware monitoring on a volume.

Parameters

-vserver <vserver name> - Vserver Name

Anti-ransomware monitoring is paused in the evaluation mode on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

-volume <volume name> - Volume Name

Anti-ransomware monitoring is paused on volumes matching the parameter value.

Examples

security anti-ransomware volume resume

Resume anti-ransomware on a volume

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume resume` command resumes Anti-ransomware monitoring on a volume.

Parameters

-vserver <vserver name> - Vserver Name

Anti-ransomware monitoring is resumed on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

-volume <volume name> - Volume Name

Anti-ransomware monitoring is resumed on volumes matching the parameter value.

Examples

security anti-ransomware volume show

Show anti-ransomware related information of volumes

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume show` command displays information related to Anti-ransomware on the volumes in the cluster. The following information is displayed:

- Vserver Name: The Vserver on which the volume is located.
- Volume Name: The volume name
- State: The Anti-ransomware state of the volume. The possible values are *disabled*, *enabled*, *dry-run*, *dry-run-paused*, *enable-paused* and *disable-in-progress*.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-attack]

If this parameter is specified, ransomware attack details are displayed.

| [-clear-suspect-status]

If this parameter is specified, the command displays the progress of the clear suspect operation. This option will not display clear suspect operation progress for volumes that do not have *junction-path* set.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

If this parameter and the `-volume` parameter are specified, the command displays detailed information related to Anti-ransomware about the specified volume. If this parameter is specified by itself, the command displays information related to the Anti-ransomware about all volumes on the specified Vserver.

[-volume <volume name>] - Volume Name

If this parameter and the `-vserver` parameter are specified, the command displays detailed information related to Anti-ransomware about the specified volume. If this parameter is specified by itself, the command displays information related to the Anti-ransomware about all volumes matching the specified name.

[-state {disabled|enabled|dry-run|paused|dry-run-paused|enable-paused|disable-in-progress}] - State

If this parameter is specified, the command displays information only about the volume or volumes that have the specified Anti-ransomware state. The possible values are *disabled*, *enabled*, *dry-run*, *dry-run-paused*, *enable-paused* and *disable-in-progress*. The possible states are:

- disabled - Anti-ransomware is disabled on the volume.
- enabled - Anti-ransomware is enabled on the volume.
- dry-run - Anti-ransomware is enabled in the dry-run or evaluation mode on the volume.
- dry-run-paused - Anti-ransomware is paused from dry-run or evaluation mode on the volume.
- enable-paused - Anti-ransomware is paused on the volume.
- disable-in-progress - Anti-ransomware disable work is in progress on the volume.

[-attack-probability {none|low|moderate|high}] - Attack Probability

If this parameter is specified, the command displays information only about the volumes that have the specified probability. The possible values are *none*, *low*, *moderate*, and *high*.

- none - No data is suspected for ransomware activity.
- low - Small amount data is suspected for ransomware activity.
- moderate - Moderate amount of data is suspected for ransomware activity.
- high - Large amount data is suspected for ransomware activity.

[-attack-timeline <MM/DD/YYYY HH:MM:SS>,...] - Attack Timeline

If this parameter is specified, the command displays information only about the volumes that have the specified attack-timeline.

[-no-of-attacks <integer>] - Number of Attacks

This provides the number of ransomware attacks observed.

[-attack-detected-by <anti_ransomware_detection_type>] - Attack Detected By

If this parameter is specified, the command displays information only about the volumes that have the specified attack detection type. The possible values are *file*, *block*.

- file_analysis - Attack is detected by file activity analysis.
- encryption_percentage_analysis - Attack is detected by data encryption percentage.

[-block-device-detection-status <arw_block_device_detection_status>] - Block Device Detection Status

If this parameter is specified, the command displays information only about the volumes that have the specified block device detection status. The possible values are:

- evaluation_period - Attack detection is currently in its evaluation phase.
- active_unsuitable_workload - Attack detection is active, but the current workload is not suitable for Anti-ransomware protection.
- active_suitable_workload - Attack detection is active, and the current workload is appropriate for Anti-ransomware protection.

[-block-device-evaluation-start-time <MM/DD/YYYY HH:MM:SS>] - Block Device Evaluation Start-time

If this parameter is specified, the command displays information only about the volumes that have the specified evaluation start time.

[-clear-suspect-start-time <MM/DD/YYYY HH:MM:SS>] - Clear Suspect Start Time

If this parameter is specified, the command displays information only about the volumes that have the specified clear suspect start time.

[-clear-suspect-phase <arp_command_op_status>] - Clear Suspect Phase

If this parameter is specified, the command displays information only about the volumes that have the specified clear suspect phase.

Examples

The following example shows a sample output for this command:

```
cluster1::> security anti-ransomware volume show
```

Vserver	Volume	State
vs1	vol1	enabled

security anti-ransomware volume attack clear-suspect

Clear suspect record

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `anti-ransomware volume attack clear-suspect` command removes the specified files from suspect files report. When no optional parameters are provided, the suspect report file is cleared. If the attack is marked as a true positive, by setting the `false-positive` parameter to `false`, the snapshot is retained for 7 days. If marked as a false positive, by setting the `false-positive` parameter to `true`, the snapshot is retained for 24 hours.

Parameters

-vserver <vserver name> - Vserver Name

This parameter specifies the Vserver on which the volume is located.

-volume <volume name> - Volume Name

This parameter specifies the name of the volume on which anti-ransomware feature is enabled.

{ [-sequence-number <integer>] - Sequence Number

This optionally specifies the sequence number of the suspect file obtained from generated report.

| [-extensions <text>, ...] - File Extensions

This optionally specifies the extensions of ransomware attacked files that needs to be cleared from attack report.

| [-start-time <MM/DD/YYYY HH:MM:SS>] - Start Time

This optionally specifies the lower bound of the time to clear a suspect record. Any suspect record with time greater than or equal to start-time is cleared.

[-end-time <MM/DD/YYYY HH:MM:SS>] - End Time }

This optionally specifies upper bound of the time to clear a suspect record. Any suspect record with time less than or equal to end-time is cleared.

-false-positive {true|false} - False Positive?

This indicates whether the suspect record of specific extensions, time range, and so on, are to be considered a false positive.

Examples

The following example shows a sample output for clearing all the suspects observed with timestamp in the start-time and end-time range, and with given extension.

```
clus1::> security anti-ransomware volume attack clear-suspect -volume  
testvol -start-time "4/14/2021 04:16:48" -end-time "4/14/2021 06:16:50"  
5 suspect records cleared.
```

The following examples shows output when given sequence-number is not present.

```
clus1::*> security anti-ransomware volume attack clear-suspect -volume  
testvol -sequence-number 1000
```

```
Error: command failed: No suspect records found.
```

security anti-ransomware volume attack generate-report

Generates Report File of the Suspected Attack on the Volume

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `anti-ransomware volume attack generate-report` command copies the report file to the given path. The report file is not an exhaustive list of all suspected files during the attack, since the maximum number of entries allowed per file extension is 20.

Parameters

-vserver <vserver name> - Vserver Name

This parameter specifies the Vserver on which the volume is located.

-volume <volume name> - Volume Name

This parameter specifies the name of the volume on which anti-ransomware feature is enabled.

-dest-path <sub dir> - Destination path under the volume to copy the report file

This parameter specifies the destination junction-path where requested file is to be copied.

Examples

The following example shows sample output for generating report-file of volume copied to its own destination junction path.

```
cluster1::> volume show -fields junction-path -vserver vs0 -volume
test_vol

      vs0      test_vol  /test_vol_path
-----
vserver volume      junction-path
-----
vs0      test_vol  /test_vol_path
cluster1::> security anti-ransomware volume attack generate-report -volume
test_vol -dest-path vs0:/test_vol_path
Report "report_file_vs0_test_vol_08-07-2025_04-27-18"
available at path "vs0:/test_vol_path".
```

The following example shows sample output for generating report-file of volume copied to different volume's destination junction path.

```
cluster1::> volume show -fields junction-path -vserver vs1 -volume
test_vs1_vol

      vs1      test_vs1_vol  /ontap_vol
-----
vserver volume      junction-path
-----
vs1      test_vs1_vol  /ontap_vol
cluster1::> security anti-ransomware volume attack generate-report -volume
test_vol -vserver vs0 -dest-path vs1:/ontap_vol
Report "report_file_vs0_test_vol_08-07-2025_04-39-44"
available at path "vs1:/ontap_vol".
```

security anti-ransomware volume attack-detection-parameters modify

security anti-ransomware volume attack-detection-parameters modify

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume attack-detection-parameters modify` command can be used to modify the attack detection parameters of an anti-ransomware enabled volume.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume.

-volume <volume name> - Volume Name

This parameter specifies the anti-ransomware enabled volume for which the attack detection parameters need to be modified.

`[-based-on-high-entropy-data-rate {true|false}] - High Entropy Data Rate at Volume Level`

This parameter indicates whether ransomware detection is based on a high entropy data rate at the volume level. Ransomware detection is also done based on high entropy data rate at the file level and this method of detection is always enabled and has no dependency on this parameter.

`[-based-on-never-seen-before-file-extension {true|false}] - Never Seen before File Extension`

This parameter indicates whether ransomware detection is based on new file types not seen before at the volume level. This detection method is based only on the file extension not on the file entropy. Some variants of ransomware modify the data such that the file entropy remains unchanged. This method helps in detecting those ransomware but there is a possibility of false positives. Note that ransomware detection is also done based on combined file extension and file entropy and this method of detection is always enabled and has no dependency on this parameter.

`[-based-on-file-create-rate {true|false}] - Is Based on File Create Operation Rate`

This parameter indicates whether ransomware detection is based on the file create rate at the volume level. If this is true and the number of files created per timeslot surges by `-file-create-rate-surge-notify-percentage` percentage compared to the historically observed value, then it is considered an attack.

`[-based-on-file-rename-rate {true|false}] - Is Based on File Rename Operation Rate`

This parameter indicates whether ransomware detection is based on the file rename rate at the volume level. If this is true and the number of files renamed per timeslot surges by `-file-rename-rate-surge-notify-percentage` percentage compared to the historically observed value, then it is considered an attack.

`[-based-on-file-delete-rate {true|false}] - Is Based on File Delete Operation Rate`

This parameter indicates whether ransomware detection is based on the file delete rate at the volume level. If this is true and the number of files deleted per timeslot surges by `-file-delete-rate-surge-notify-percentage` percentage compared to the historically observed value, then it is considered an attack.

`[-relaxing-popular-file-extensions {true|false}] - Is Relaxing Popular File Extensions`

This parameter indicates whether ransomware detection is based on commonly used extensions. If true, then a predetermined commonly used extension, such as .mp3, is considered safe. If false, only those file extensions observed during the dry-run state are considered safe; any extension not observed during the dry-run state but observed later is a suspected ransomware attack, even if it is a commonly used extension.

`[-high-entropy-data-surge-notify-percentage <integer>] - High Entropy Data Surge Notify Percentage`

This parameter displays the surge value that is considered safe in the overall incoming data at the volume level.

`[-file-create-rate-surge-notify-percentage <integer>] - File Create Operation Rate Surge Notify Percentage`

This parameter displays the surge rate that is considered safe for file create operations at the volume level.

`[-file-delete-rate-surge-notify-percentage <integer>] - File Delete Operation Rate Surge Notify Percentage`

This parameter displays the surge rate that is considered safe for file delete operations at the volume level.

`[-file-rename-rate-surge-notify-percentage <integer>]` - File Rename Operation Rate Surge Notify Percentage

This parameter displays the surge rate that is considered safe for file rename operations at the volume level.

`[-never-seen-before-file-extn-count-notify-threshold <integer>]` - Never Seen before File Extension Count Notify Threshold

This parameter displays the threshold value of number of files observed with a new file extension not seen before for create/rename operations.

`[-never-seen-before-file-extn-duration-in-hours <integer>]` - Never Seen before File Extension Duration in Hours

This parameter displays the duration for new file extensions not seen before, in hours. If a new file extension is observed and `-never-seen-before-file-extn-count-notify-threshold` number of files are created/renamed with this new file extension for this duration, then it is reported as an attack.

Examples

The following example displays attack detection parameter information of a volume.

```
cluster1::> security anti-ransomware volume attack-detection-parameters
show -vserver vs1 -volume voll
```

```

Vserver Name : vs1
Volume Name : voll
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
```

```
cluster1::> security anti-ransomware volume attack-detection-parameters
modify -vserver vs1 -volume voll -file-delete-rate-surge-notify-percentage
25
```

```
cluster1::> security anti-ransomware volume attack-detection-parameters
show -vserver vs1 -volume voll
```

```

Vserver Name : vs1
Volume Name : voll
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 : 25
Never Seen before File Extensions Count Notify Threshold : 20
    Never Seen before File Extensions Duration in Hour : 24
```

security anti-ransomware volume attack-detection-parameters show

Show anti-ransomware volume attack detection parameters

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The security anti-ransomware volume attack-detection-parameters show command displays attack detection parameter details of an anti-ransomware enabled volume.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

-vserver <Vserver Name> - Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume.

-volume <volume name> - Volume Name

This parameter specifies the anti-ransomware enabled volume for which the attack detection parameters need to be displayed.

[-based-on-high-entropy-data-rate {true|false}] - High Entropy Data Rate at Volume Level

This parameter displays whether ransomware detection is based on a high entropy data rate at the volume level. Ransomware detection is also done based on high entropy data rate at the file level and this method of detection is always enabled and has no dependency on this parameter.

[-based-on-never-seen-before-file-extension {true|false}] - Never Seen before File Extension

This parameter indicates whether ransomware detection is based on new file types not seen before at the volume level. This detection method is based only on the file extension not on file entropy. Some variants of ransomware modify the data such that the file entropy remains unchanged. This method helps in detecting those ransomware but there is a possibility of false positives. Note that ransomware detection is also done based on combined file extension and file entropy and this method of detection is always enabled and has no dependency on this parameter.

[-based-on-file-create-rate {true|false}] - Is Based on File Create Operation Rate

This parameter displays whether ransomware detection is based on the file create rate at the volume level. If this is true and the number of files created per timeslot surges by `-file-create-rate-surge -notify-percentage` percentage compared to the historically observed value, then it is considered an attack.

[-based-on-file-rename-rate {true|false}] - Is Based on File Rename Operation Rate

This parameter displays whether ransomware detection is based on the file rename rate at the volume level. If this is true and the number of files renamed per timeslot surges by `-file-rename-rate-surge -notify-percentage` percentage compared to the historically observed value, then it is considered an attack.

[-based-on-file-delete-rate {true|false}] - Is Based on File Delete Operation Rate

This parameter displays whether ransomware detection is based on the file delete rate at the volume level. If this is true and the number of files deleted per timeslot surges by `-file-delete-rate-surge -notify-percentage` percentage compared to the historically observed value, then it is considered an

attack.

`[-relaxing-popular-file-extensions {true|false}] - Is Relaxing Popular File Extensions`

This parameter displays whether ransomware detection is based on commonly used extensions. If true, then a predetermined commonly used extension, such as .mp3, is considered safe. If false, only those file extensions observed during the dry run state are considered safe; any extension not observed during the dry-run state but observed later is suspected as a ransomware attack, even if it is a commonly used extension.

`[-high-entropy-data-surge-notify-percentage <integer>] - High Entropy Data Surge Notify Percentage`

This parameter displays the surge value that is considered safe in the overall incoming data at the volume level.

`[-file-create-rate-surge-notify-percentage <integer>] - File Create Operation Rate Surge Notify Percentage`

This parameter displays the surge rate that is considered safe for file create operations at the volume level.

`[-file-delete-rate-surge-notify-percentage <integer>] - File Delete Operation Rate Surge Notify Percentage`

This parameter displays the surge rate that is considered safe for file delete operations at the volume level.

`[-file-rename-rate-surge-notify-percentage <integer>] - File Rename Operation Rate Surge Notify Percentage`

This parameter displays the surge rate that is considered safe for file rename operations at the volume level.

`[-never-seen-before-file-extn-count-notify-threshold <integer>] - Never Seen before File Extension Count Notify Threshold`

This parameter displays the threshold value of new file extensions not seen before for create/rename operations.

`[-never-seen-before-file-extn-duration-in-hours <integer>] - Never Seen before File Extension Duration in Hours`

This parameter displays the duration for new file extensions not seen before, in hours. If a new file extension is observed and `-never-seen-before-file-extn-count-notify-threshold` number of files are created/renamed with this same new file extension for this duration, then it is reported as an attack.

`[-block-device-auto-learned-encryption-threshold <integer>] - Block Device Auto Learned Encryption Threshold`

This parameter displays block device auto learned encryption threshold.

Examples

The following example displays attack detection parameter information of a volume.

```

cluster1::> 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

```

security anti-ransomware volume auto-switch-to-enable-mode show

(DEPRECATED) Show anti-ransomware volume auto-switch to enable-mode stats

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume auto-switch-to-enable-mode show` command displays stats related to auto-switch to enable-mode of the volumes in dry-run state. Deprecated: This command is no longer supported and may be removed in a future release.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - (DEPRECATED) Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume. Deprecated: This parameter is no longer supported and may be removed in a future release.

[-volume <volume name>] - (DEPRECATED) Volume Name

This parameter specifies the anti-ransomware enabled volume for which the auto-switch info need to be displayed. Deprecated: This parameter is no longer supported and may be removed in a future release.

`[-total-writes <integer>] - (DEPRECATED) Total writes`

Total data writes size so far in dry-run period. Deprecated: This parameter is no longer supported and may be removed in a future release.

`[-dry-run-days-count <integer>] - (DEPRECATED) Dry run days count`

Number of days a volume is in learning mode. Deprecated: This parameter is no longer supported and may be removed in a future release.

`[-days-since-new-extn-seen <integer>] - (DEPRECATED) Days since new extn seen`

Number of days where no new extension is observed in the volume. Deprecated: This parameter is no longer supported and may be removed in a future release.

`[-dry-run-new-file-count <integer>] - (DEPRECATED) Dry run new file count`

Number of files created in a volume during learning period. Deprecated: This parameter is no longer supported and may be removed in a future release.

`[-dry-run-new-file-extension-count <integer>] - (DEPRECATED) Dry run new file extensions count`

Number of file extensions observed in a volume during learning period. Deprecated: This parameter is no longer supported and may be removed in a future release.

Examples

The following example displays attack detection parameter information of a volume. Deprecated: This example is no longer valid as the command may be removed in a future release.

```
cluster1::> security anti-ransomware volume auto-switch-to-enable-mode
show -vserver vs1 -volume vol1
      Vserver                                     : vs_1
      Volume                                       : vol1
      Amount of Write (KB) Received during Dry-run Mode :
23920640
      Number of Days Completed in Dry-run Mode      : 40
      Days Without a New Extension seen in Dry-run Mode : 2
      Number of Files created during Dry-run Period : 1991
      Number of File extensions observed in Dry-run period : 20
```

security anti-ransomware volume entropy-stat show-encryption-percentage-histogram

Display the volume encryption percentage histogram

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The security anti-ransomware volume entropy-stat show-encryption-percentage-

histogram command displays the histogram for the volume.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume for which the entropy stats histogram need to be displayed. If this parameter is specified, the command displays entropy stats histogram only for the specified Vserver.

[-volume <volume name>] - Volume Name

This parameter specifies the anti-ransomware enabled volume for which the entropy stats histogram need to be displayed. If this parameter is specified, the command displays entropy stats histogram only for the specified volume.

[-duration {real_time|evaluation_period|30days|90days|180days}] - Duration

This parameter specifies the duration for which other details will be displayed

[-encryption-percent-range {0-5%|6-10%|11-15%|16-20%|21-25%|26-30%|31-35%|36-40%|41-45%|46-50%|51-55%|56-60%|61-65%|66-70%|71-75%|76-80%|81-100%}] - Encryption Percent Range

This parameter specifies the range of encryption percentage for which additional details will be displayed.

[-count <integer>] - Count

This parameter specifies the number of times data is written within the given encryption percentage range.

[-data-written {<integer>[KB|MB|GB|TB|PB]}] - Data Written

This parameter specifies the amount of data written within the given encryption percentage range.

Examples

The following example displays the entropy stats histogram information of a volume.

```
cluster1::> security anti-ransomware volume entropy-stat show-encryption-
percentage-histogram -vserver vs1 -volume volume_1
```

		Encryption		
Vserver	volume	Percent Range	Count	Data Written
-----	-----	-----	-----	
vs1	volume_1	0-5	2	17MB
vs1	volume_1	6-10	11	2GB
vs1	volume_1	11-15	54	10GB
vs1	volume_1	16-20	41	3.23GB
vs1	volume_1	21-25	35	15GB
vs1	volume_1	26-30	0	0B
vs1	volume_1	31-35	0	0B
vs1	volume_1	36-40	0	0B
vs1	volume_1	41-45	0	0B
vs1	volume_1	46-50	0	0B
vs1	volume_1	51-55	0	0B
vs1	volume_1	56-60	0	0B
vs1	volume_1	61-65	0	0B
vs1	volume_1	66-70	0	0B
vs1	volume_1	71-75	0	0B
vs1	volume_1	76-80	0	0B
vs1	volume_1	81-100	0	0B

17 entries were displayed.

security anti-ransomware volume entropy-stat show-recent-daily-stat

Display the volume entropy recent daily stats

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume entropy-stat show-recent-daily-stat` command displays the percentage of data classified as encrypted using an entropy algorithm measured at daily intervals, at the volume level.

Parameters

```
{ [-fields <fieldname>,...]
```

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume for which the entropy stats need to be displayed. If this parameter is specified, the command displays entropy stats only for the specified Vserver.

[-volume <volume name>] - Volume Name

This parameter specifies the anti-ransomware enabled volume for which the entropy stats need to be displayed. If this parameter is specified, the command displays entropy stats only for the specified Volume.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Start Time

This parameter specifies the start time of entropy stats collection interval. If this parameter is specified, only rows that match the specified input for timestamp will be displayed.

[-total-data-written {<integer>[KB|MB|GB|TB|PB] }] - Total Data Blocks written

This parameter specifies the amount of data written in the interval. If this parameter is specified, only rows that match the specified input for total-data-written will be displayed.

[-encryption-percentage <percent>] - Encryption Percentage

This parameter specifies the encryption percentage of the interval. If this parameter is specified, only rows that match the specified input for encryption-percentage will be displayed.

[-duration <time_interval>] - Duration of the interval

This parameter specifies the duration of the interval. If this parameter is specified, only rows that match the specified input for duration will be displayed.

Examples

The following example displays the recent daily entropy stats information of a volume.

```
cluster1::> security anti-ransomware volume entropy-stat show-recent-  
daily-stat -vserver vs1 -volume vol1
```

Vserver	Volume	Start Time	Total Duration	Encrypted Data Written	Data%
vs0	vol1	1/21/2025 10:49:40	24h10m0s	100MB	10%
vs0	vol1	1/22/2025 10:59:40	24h10m4s	1GB	0%
vs0	vol1	1/23/2025 11:49:44	24h9m57s	500MB	0%
vs0	vol1	1/24/2025 11:59:41	24h9m59s	2GB	2%
vs0	vol1	1/25/2025 12:09:40	24h10m1s	400MB	14%
vs0	vol1	1/26/2025 12:19:41	24h10m2s	4GB	4%
vs0	vol1	1/27/2025 12:29:43	24h9m58s	150MB	5%

security anti-ransomware volume entropy-stat show-recent-high-encryption-stat

Display the volume entropy recent high encryption stats

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume entropy-stat show-recent-high-encryption-stat` command displays the intervals during which a high percentage of data was classified as encrypted using a data analysis algorithm. These intervals correspond to the reported attack timeline. This statistic is reset when the administrator runs the `attack clear-suspect` command.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume for which the entropy stats need to be displayed. If this parameter is specified, the command displays entropy stats only for the specified Vserver.

[-volume <volume name>] - Volume Name

This parameter specifies the anti-ransomware enabled volume for which the entropy stats need to be displayed. If this parameter is specified, the command displays entropy stats only for the specified Volume.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Start Time

This parameter specifies the start time of entropy stats collection interval. If this parameter is specified, only rows that match the specified input for timestamp will be displayed.

[-total-data-written {<integer>[KB|MB|GB|TB|PB] }] - Total Data Blocks written

This parameter specifies the amount of data written in the interval. If this parameter is specified, only rows that match the specified input for total-data-written will be displayed.

[-encryption-percentage <percent>] - Encryption Percentage

This parameter specifies the encryption percentage of the interval. If this parameter is specified, only rows that match the specified input for encryption-percentage will be displayed.

[-duration <time_interval>] - Duration of the interval

This parameter specifies the duration of the interval. If this parameter is specified, only rows that match the specified input for duration will be displayed.

Examples

The following example displays the recent high encryption stat information of a volume.

```
cluster1::> security anti-ransomware volume entropy-stat show-recent-high-encryption-stat -vserver vs1 -volume vol1
```

Vserver	Volume	Start Time	Total	Encrypted	
			Duration	Data Written	Data%
vs0	vol1	1/21/2025 10:49:40	0h10m10s	3GB	55%
vs0	vol1	1/21/2025 11:10:43	0h10m58s	2GB	60%

security anti-ransomware volume entropy-stat show-recent-hourly-stat

Display the volume entropy recent hourly stats

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume entropy-stat show-recent-hourly-stat` command displays the percentage of data classified as encrypted using an entropy algorithm measured at hourly intervals, at the volume level.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume for which the entropy stats need to be displayed. If this parameter is specified, the command displays entropy stats only for the specified Vserver.

[-volume <volume name>] - Volume Name

This parameter specifies the anti-ransomware enabled volume for which the entropy stats need to be displayed. If this parameter is specified, the command displays entropy stats only for the specified Volume.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Start Time

This parameter specifies the start time of entropy stats collection interval. If this parameter is specified, only rows that match the specified input for timestamp will be displayed.

[`-total-data-written` {<integer>[KB|MB|GB|TB|PB]}] - Total Data Blocks written

This parameter specifies the amount of data written in the interval. If this parameter is specified, only rows that match the specified input for total-data-written will be displayed.

[`-encryption-percentage` <percent>] - Encryption Percentage

This parameter specifies the encryption percentage of the interval. If this parameter is specified, only rows that match the specified input for encryption-percentage will be displayed.

[`-duration` <time_interval>] - Duration of the interval

This parameter specifies the duration of the interval. If this parameter is specified, only rows that match the specified input for duration will be displayed.

Examples

The following example displays the recent hourly entropy stats information of a volume.

```
cluster1::> security anti-ransomware volume entropy-stat show-recent-  
hourly-stat -vserver vs1 -volume vol1
```

Vserver	Volume	Start Time	Total	Encrypted	Data%
			Duration	Data Written	
vs0	vol1	1/27/2025 19:49:39	0h59m8s	500MB	0%
vs0	vol1	1/27/2025 20:48:47	1h0m0s	200MB	0%
vs0	vol1	1/27/2025 21:48:47	1h0m0s	40MB	10%
vs0	vol1	1/27/2025 22:48:47	1h10m52s	1GB	20%
vs0	vol1	1/27/2025 23:59:39	0h59m8s	2GB	10%
vs0	vol1	1/28/2025 00:58:47	1h10m0s	350MB	0%
vs0	vol1	1/28/2025 02:08:47	1h0m0s	77.48MB	13%
vs0	vol1	1/28/2025 03:08:47	1h0m0s	44MB	0%
vs0	vol1	1/28/2025 04:08:47	1h0m54s	3GB	0%

security anti-ransomware volume entropy-stat show-recent-sub-hourly-stat

Display the volume entropy recent sub-hourly stats

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume entropy-stat show-recent-sub-hourly-stat` command displays the percentage of data classified as encrypted using an entropy algorithm measured at sub-hourly intervals, at the volume level.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `-fields ?` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume for which the entropy stats need to be displayed. If this parameter is specified, the command displays entropy stats only for the specified Vserver.

[-volume <volume name>] - Volume Name

This parameter specifies the anti-ransomware enabled volume for which the entropy stats need to be displayed. If this parameter is specified, the command displays entropy stats only for the specified Volume.

[-timestamp <MM/DD/YYYY HH:MM:SS>] - Start Time

This parameter specifies the start time of entropy stats collection interval. If this parameter is specified, only rows that match the specified input for timestamp will be displayed.

[-total-data-written {<integer>[KB|MB|GB|TB|PB] }] - Total Data Blocks written

This parameter specifies the amount of data written in the interval. If this parameter is specified, only rows that match the specified input for total-data-written will be displayed.

[-encryption-percentage <percent>] - Encryption Percentage

This parameter specifies the encryption percentage of the interval. If this parameter is specified, only rows that match the specified input for encryption-percentage will be displayed.

[-duration <time_interval>] - Duration of the interval

This parameter specifies the duration of the interval. If this parameter is specified, only rows that match the specified input for duration will be displayed.

Examples

The following example displays the recent sub-hourly entropy stats information of a volume.

```
cluster1::> security anti-ransomware volume entropy-stat show-recent-sub-
hourly-stat -vserver vs1 -volume vol1
```

Vserver	Volume	Start Time	Total	Encrypted	Data Written	Data%
			Duration	Data		
vs0	vol1	1/28/2025 10:49:40	0h10m0s	100MB		0%
vs0	vol1	1/28/2025 10:59:40	0h50m4s	150MB		10%
vs0	vol1	1/28/2025 11:49:44	0h9m57s	200MB		0%
vs0	vol1	1/28/2025 11:59:41	0h9m59s	400MB		0%
vs0	vol1	1/28/2025 12:09:40	0h10m1s	300MB		0%
vs0	vol1	1/28/2025 12:19:41	0h10m2s	10MB		0%
vs0	vol1	1/28/2025 12:29:43	0h9m58s	1MB		0%
vs0	vol1	1/28/2025 12:39:41	0h10m0s	50MB		0%

security anti-ransomware volume event-log modify

Modify anti-ransomware event-log for volumes

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume event-log` command.

Parameters

-vserver <vserver name> - Vserver Name

This parameter specifies the Vserver of anti-ransomware enabled volume.

-volume <volume name> - Volume Name

This parameter specifies the anti-ransomware enabled volume.

[-is-enabled-on-new-file-extension-seen {true|false}] - Is Enabled on New File Extension Seen

This parameter indicates whether an alert event should be created when files with new extensions are created.

[-is-enabled-on-snapshot-copy-creation {true|false}] - Is Enabled on Snapshot Copy Creation

This parameter indicates whether an alert event should be created when snapshots are created.

Examples

```

cluster1::> security anti-ransomware volume event-log modify -vserver vs1
-volume vol1 -is-enabled-on-new-file-extension-seen true -is-enabled-on
-snapshot-copy-creation true

cluster1::> security anti-ransomware volume event-log show -vserver vs1
-volume vol1
Vserver : vs1
          Volume : vol1
          Is Enabled on
New File Extension Seen : true
          Is Enabled on
Snapshot Copy Creation : true

```

security anti-ransomware volume event-log show

Show anti-ransomware event-log for volumes

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The security anti-ransomware volume event-log command.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

This parameter specifies the Vserver of anti-ransomware enabled volume.

[-volume <volume name>] - Volume Name

This parameter specifies the anti-ransomware enabled volume.

[-is-enabled-on-new-file-extension-seen {true|false}] - Is Enabled on New File Extension Seen

This parameter indicates whether an alert event is generated on creation of files with new extensions.

[-is-enabled-on-snapshot-copy-creation {true|false}] - Is Enabled on Snapshot Copy Creation

This parameter indicates whether an alert event is generated when a snapshot is created.

security anti-ransomware volume space show

Display the details of anti-ransomware space usage

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This `security anti-ransomware volume space show` displays the space usage by Anti-ransomware feature.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver Name

This parameter specifies the Vserver on which the volume is located.

[-volume <volume name>] - Volume Name

This parameter specifies the name of the volume whose space usage details are to be shown.

[-space-used-by-snapshot {<integer>[KB|MB|GB|TB|PB] }] - Space Used by snapshots

This parameter shows space usage by Anti-ransomware snapshots.

[-space-used-by-logs {<integer>[KB|MB|GB|TB|PB] }] - Space Used by logs

This parameter shows the space used by the Anti-ransomware logs.

[-total-space-used {<integer>[KB|MB|GB|TB|PB] }] - Total space used by anti-ransomware

This parameter shows the total space used by the Anti-ransomware feature.

[-no-of-snapshot <integer>] - Number of Anti-ransomware Snapshot Copies

This parameter shows the total count of the Anti-ransomware snapshots.

Examples

The following example shows a sample output for this command:


```
clus1::>> security anti-ransomware volume space show
```

Vserver	Volume	Space Used By Snapshot	Space Used By logs	Total Space Used	Snapshot Copies
vs1	vol1	308KB	8B	308.0KB	2

security anti-ransomware volume workload-behavior clear-surge

Clear the observed surge values on a volume

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume workload-behavior clear-surge` command clears the observed surge values.

Parameters

-vserver <vserver name> - Vserver Name

This parameter specifies the Vserver on which the volume is located.

-volume <volume name> - Volume Name

This parameter specifies the name of the volume on which anti-ransomware feature is enabled.

Examples

```
cluster1::> security anti-ransomware volume workload-behavior show
-vserver vs1 -volume vol1
```

```

Vserver: vs1
Volume: vol1
File Extensions Observed: .txt, .exe, .pdf, .img
Number of File Extensions Observed: 4
Historical Statistics
High Entropy Data Write Percentage: 50
High Entropy Data Write Peak Rate (KB/Minute): 50
File Create Peak Rate (per Minute): 100
File Delete Peak Rate (per Minute): 100
File Rename Peak Rate (per Minute): 100
Surge Observed
Surge Timeline: 09/05/2022 14:01:00
High Entropy Data Write Percentage: 100

```

```

    High Entropy Data Write Peak Rate (KB/Minute): 2000
        File Create Peak Rate (per Minute): 80
        File Delete Peak Rate (per Minute): -
        File Rename Peak Rate (per Minute): 200
            Newly Observed File Extensions: .dll, .exec, .js
        Number of Newly Observed File Extensions: 10, 4, 22

cluster1::> security anti-ransomware volume workload-behavior clear-surge
-vserver vs1 -volume voll

cluster1::> security anti-ransomware volume workload-behavior show
-vserver vs1 -volume voll

                                Vserver: vs1
                                Volume: voll
                                File Extensions Observed: .txt, .exe, .pdf, .img
                                Number of File Extensions Observed: 4
Historical Statistics
    High Entropy Data Write Percentage: 50
    High Entropy Data Write Peak Rate (KB/Minute): 50
        File Create Peak Rate (per Minute): 100
        File Delete Peak Rate (per Minute): 100
        File Rename Peak Rate (per Minute): 100
Surge Observed
                                Surge Timeline: -
                                High Entropy Data Write Percentage: -
    High Entropy Data Write Peak Rate (KB/Minute): -
        File Create Peak Rate (per Minute): -
        File Delete Peak Rate (per Minute): -
        File Rename Peak Rate (per Minute): -
            Newly Observed File Extensions: .dll, .exec, .js
        Number of Newly Observed File Extensions: 10, 4, 22

```

security anti-ransomware volume workload-behavior show

Display information about the volume's workload-behavior learnt by the analytics algorithm

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This `security anti-ransomware volume workload-behavior show` displays the workload characteristics observed during anti-ransomware monitoring.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `-fields ?` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

-vserver <Vserver Name> - Vserver Name

This parameter specifies the Vserver of the anti-ransomware enabled volume.

-volume <volume name> - Volume Name

This parameter specifies the anti-ransomware enabled volume for which the workload behavior details are displayed.

[-file-extensions-included <text>,...] - List of File Extensions Observed

This parameter displays the list of file extensions observed during anti-ransomware monitoring.

[-total-file-extensions-included <integer>] - Number of File Extensions Observed

This parameter displays the number of file extensions observed during anti-ransomware monitoring.

[-high-entropy-data-write-peak-percent <integer>] - High Entropy Data Write Peak Percentage

This parameter displays the peak historical high entropy data write percentage of the incoming data.

[-high-entropy-data-write-peak-rate <integer>] - High Entropy Data Write Peak Rate (KB/minute)

This parameter displays the peak historical high entropy data write rate.

[-file-create-peak-rate <integer>] - File Create Peak Rate per Minute

This parameter displays the peak historical rate of file create operations in the volume.

[-file-rename-peak-rate <integer>] - File Rename Peak Rate per Minute

This parameter displays the peak historical rate of file rename operations in the volume.

[-file-delete-peak-rate <integer>] - File Delete Peak Rate per Minute

This parameter displays the peak historical rate of file delete operations in the volume.

[-surge-timeline <MM/DD/YYYY HH:MM:SS>] - Surge Timeline

This parameter displays the timeline where a surge was observed in the workload characteristics compared to the historically learned characteristics.

[-surge-high-entropy-data-write-peak-percent <integer>] - High Entropy Data Write Percentage During Surge

This parameter displays the peak percentage value of high entropy data write in the incoming data when the surge was observed.

[-surge-high-entropy-data-write-peak-rate <integer>] - High Entropy Data-write Peak Rate Surge (KB/minute)

This parameter displays the peak rate of high entropy data write when the surge was observed.

[-surge-file-create-peak-rate <integer>] - File Create Peak Rate (per Minute) During Surge

This parameter displays the surge in the peak rate of file create operations.

[-surge-file-delete-peak-rate <integer>] - File Delete Peak Rate (per Minute) During Surge

This parameter displays the surge in the peak rate of file delete operations.

[-surge-file-rename-peak-rate <integer>] - File Rename Peak Rate (per Minute) During Surge

This parameter displays the surge in the peak rate of file rename operations.

[-attack-file-extensions-observed <text>,...] - File Extensions Observed During Attack

This parameter displays the list of file types observed during a suspected ransomware attack.

[-attack-file-extensions-observed-counts <integer>,...] - Number of File Extensions Observed During Attack

This parameter displays the count of various file types observed during a suspected ransomware attack.

Examples

The following example shows sample output for this command:

```
cluster1::> security anti-ransomware volume workload-behavior show
-vserver vs1 -volume vol1

                                Vserver: vs1
                                Volume: vol1
                                File Extensions Observed: .ext1, .ext2, .ext3
                                Number of File Extensions Observed: 3
Historical Statistics
    High Entropy Data Write Percentage: 40
    High Entropy Data Write Peak Rate (KB/Minute): 50
    File Create Peak Rate (per Minute): 100
    File Delete Peak Rate (per Minute): 100
    File Rename Peak Rate (per Minute): 100
Surge Observed
                                Surge Timeline: 1/1/2022 01:01:01
                                High Entropy Data Write Percentage: 95
    High Entropy Data Write Peak Rate (KB/Minute): 200
    File Create Peak Rate (per Minute): 200
    File Delete Peak Rate (per Minute): 200
    File Rename Peak Rate (per Minute): 200
                                Newly Observed File Extensions: .uk1,.uk2,.uk3
                                Number of Newly Observed File Extensions: 1, 2, 3
```

security anti-ransomware volume workload-behavior update-baseline-from-surge

Set the observed surge values as the new baseline on a volume

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware volume workload-behavior update-baseline-from-surge` command sets the observed surge value as new baseline.

Parameters

-vserver <vserver name> - Vserver Name

This parameter specifies the Vserver on which the volume is located.

-volume <volume name> - Volume Name

This parameter specifies the name of the volume on which anti-ransomware feature is enabled.

Examples

```
cluster1::> security anti-ransomware volume workload-behavior show
-vserver vs1 -volume vol1

                                Vserver: vs1
                                Volume: vol1
                                File Extensions Observed: .txt, .exe, .pdf, .img
                                Number of File Extensions Observed: 4
Historical Statistics
    High Entropy Data Write Percentage: 50
    High Entropy Data Write Peak Rate (KB/Minute): 50
    File Create Peak Rate (per Minute): 100
    File Delete Peak Rate (per Minute): 100
    File Rename Peak Rate (per Minute): 100
Surge Observed
                                Surge Timeline: 10/3/2021 14:01:00
                                High Entropy Data Write Percentage: 100
                                High Entropy Data Write Peak Rate (KB/Minute): 2000
                                File Create Peak Rate (per Minute): 80
                                File Delete Peak Rate (per Minute): -
                                File Rename Peak Rate (per Minute): 200
                                Newly Observed File Extensions: .dll, .exec, .js
                                Number of Newly Observed File Extensions: 10, 4, 22

cluster1::> security anti-ransomware volume workload-behavior update-
baseline-from-surge -vserver vs1 -volume vol1
```

```

cluster1::> security anti-ransomware volume workload-behavior show
-vserver vs1 -volume vol1

                                Vserver: vs1
                                Volume: vol1
                                File Extensions Observed: .txt, .exe, .pdf, .img
                                Number of File Extensions Observed: 4
Historical Statistics
    High Entropy Data Write Percentage: 100
    High Entropy Data Write Peak Rate (KB/Minute): 2000
    File Create Peak Rate (per Minute): 180
    File Delete Peak Rate (per Minute): 100
    File Rename Peak Rate (per Minute): 200
Surge Observed
    Surge Timeline: -
    High Entropy Data Write Percentage: -
    High Entropy Data Write Peak Rate (KB/Minute): -
    File Create Peak Rate (per Minute): -
    File Delete Peak Rate (per Minute): -
    File Rename Peak Rate (per Minute): -
    Newly Observed File Extensions: .dll, .exec, .js
    Number of Newly Observed File Extensions: 10, 4, 22

```

security anti-ransomware vserver event-log modify

Modify anti ransomware event log configuration for Vservers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware vserver event-log modify` command modifies the anti ransomware event log configuration of a specified Vserver

Parameters

-vserver <vserver name> -Vserver

Vserver whose anti ransomware event log configuration will be modified.

[-is-enabled-on-new-file-extension-seen {true|false}] - Is Enabled on New File Extension Seen

This parameter indicates whether an alert event should be created when files with new extensions are created.

[-is-enabled-on-snapshot-copy-creation {true|false}] - Is Enabled on Snapshot Copy Creation

This parameter indicates whether an alert event should be created when snapshots are created.

security anti-ransomware vsserver event-log show

Show anti ransomware event log configuration for Vservers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security anti-ransomware vsserver event-log show` command displays anti ransomware event log configuration for a Vserver.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If this parameter is specified, the command displays anti ransomware event log information about the specified Vserver.

[-is-enabled-on-new-file-extension-seen {true|false}] - Is Enabled on New File Extension Seen

If this parameter is specified, the command displays information only about the Vservers that match the specified value for new file extension seen event logging.

[-is-enabled-on-snapshot-copy-creation {true|false}] - Is Enabled on Snapshot Copy Creation

If this parameter is specified, the command displays information only about the Vservers that match the specified value for snapshot creation event logging.

Examples

The following example shows a sample output for this command:

```
cluster1:> security anti-ransomware vsserver event-log show
Vserver: vs_1
  Is Enabled on New File Extension Seen: true
  Is Enabled on Snapshot Copy Creation: false
```

Copyright information

Copyright © 2026 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.