security anti-ransomware commands

ONTAP 9.11.1 commands

NetApp
May 23, 2023

Table of Contents

security anti-ransomware commands

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.

Examples

security anti-ransomware volume dry-run

Dry-run 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 dry-run` command starts anti-ransomware monitoring in the evaluation mode on a volume.

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.

`-volume <volume name>` - Volume Name

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

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.

| `[-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 Vservee.

[-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.

[-dry-run-start-time <MM/DD/YYYY HH:MM:SS>] - Dry Run Start Time

If this parameter is specified, the command displays the dry run start time of the volumes that have the state dry-run or dry-run-paused.

[-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.

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.

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 genrated 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 folowing 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.

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 <[vserver:]volume/path/to/filename>` - Destination path under the volume to copy the file

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

Examples

The following example displays command output:

```
node::*> security anti-ransomware volume attack generate-report -volume
vol1 -dest-path vs1:vol1/
Report "report_file_vs1vol1_30-03-2021_16-11-38" available at path
"vs1:vol1/".
```

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 ransomwares 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 -notifiy-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 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

cluster1::> security anti-ransomware volume attack-detection-parameters
modify -vserver vs1 -volume vol1 -file-delete-rate-surge-notify-percentage
25

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 : 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 ransomwares 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 -notifiy-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 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 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 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 Snapshot copies.

[-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 Snapshot copies.

Examples

The folowing example shows a sample output for this command:

```
clus1::>> security anti-ransomware volume space show
                        Space Used By Space Used By Total Space Snapshot
Vserver    Volume       Snapshot      logs          Used        Copies
---------- ----------- ----------    ----------    ----------
---------------
vs1        vol1             308KB            8B       308.0KB
2
```

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 learnt 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 Statstics
  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                                : 1/1/2022 01:01:01
  High Entropy Data Write Percentage            : 200
  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 Statstics
  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 Statstics
  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
```

Copyright information

Trademark information