snaplock commands

ONTAP commands

NetApp
February 04, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-97/snaplock-compliance-clock-initialize.html on February 04, 2026. Always check docs.netapp.com for the latest.

Table of Contents

snaplock commands . . . 1
- snaplock compliance-clock commands . . . 1
  - snaplock compliance-clock initialize . . . 1
  - snaplock compliance-clock show . . . 1
  - snaplock compliance-clock ntp modify . . . 2
  - snaplock compliance-clock ntp show . . . 3
- snaplock event-retention commands . . . 3
  - snaplock event-retention abort . . . 3
  - snaplock event-retention apply . . . 4
  - snaplock event-retention show-vservers . . . 5
  - snaplock event-retention show . . . 5
  - snaplock event-retention policy create . . . 7
  - snaplock event-retention policy delete . . . 8
  - snaplock event-retention policy modify . . . 9
  - snaplock event-retention policy show . . . 9
- snaplock legal-hold commands . . . 10
  - snaplock legal-hold abort . . . 10
  - snaplock legal-hold begin . . . 11
  - snaplock legal-hold dump-files . . . 12
  - snaplock legal-hold dump-litigations . . . 13
  - snaplock legal-hold end . . . 14
  - snaplock legal-hold show . . . 15
- snaplock log commands . . . 17
  - snaplock log create . . . 17
  - snaplock log delete . . . 18
  - snaplock log modify . . . 19
  - snaplock log show . . . 19
  - snaplock log file archive . . . 20
  - snaplock log file show . . . 21

snaplock commands

snaplock compliance-clock commands

snaplock compliance-clock initialize

Initializes the node ComplianceClock

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

Description

` snaplock compliance-clock initialize` command is used to initialize System ComplianceClock from the system clock. System ComplianceClock can be initialized only once by the user. Once initialized, user cannot make any changes to the System ComplianceClock. Hence, user should ensure that system clock is correct before initializing the System ComplianceClock.

Parameters

`-node {<nodename>|local}` - Node

Specifies the name of the node on which System ComplianceClock needs to be initialized.

`[-force <true>]` - Forces Initialization

If you use this paramter, it will suppress the warning message during `snaplock compliance-clock initialize` operation.

Examples

```
cluster-1::> snaplock compliance-clock initialize -node node1

Warning: You are about to initialize the secure ComplianceClock of the
node
         node1 to the current value of the node's system clock. This
         procedure can be performed only once on a given node, so you
should
         ensure that the system time is set correctly before proceeding.
         The current node's system clock is: Wed Nov 26 16:18:30 IST 2014

Do you want to continue? {y|n}: y

cluster-1::>
```

snaplock compliance-clock show

Displays the node ComplianceClock

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

Description

The ` snaplock compliance-clock show ` command will display System ComplianeClock of the nodes in the cluster. It will display the following information:

- Node name
- ComplianceClock Time

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

If this parameter is specified, the command will display ComplianceClock for that particular node only.

[-time <text>] - ComplianceClock Time of the Node

If this parameter is specified, the command will display nodes having the same `-time` value.

Examples

```
cluster1::> snaplock compliance-clock show
        Node                ComplianceClock Time
        ------------------- ----------------------------------
        node1               Mon Jan 12 11:34:15 IST 2015 +05:30
        node2               Mon Jan 12 11:34:10 IST 2015 +05:30
        2 entries were displayed.
```

```
cluster1::> snaplock compliance-clock show -node node1
        Node                ComplianceClock Time
        ------------------- ----------------------------------
        node1               Mon Jan 12 11:34:45 IST 2015 +05:30
```

snaplock compliance-clock ntp modify

Modify SnapLock ComplianceClock synchronization setting

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

Description

The `snaplock compliance-clock ntp modify` command modifies the option to enable or disable the SnapLock ComplianceClock synchronization with the system time. The ComplianceClock is synchronized only

when an NTP server has been configured so that the system time follows the NTP time and the skew between the ComplianceClock time and the system time is greater than 1 day.

Parameters

`[-is-sync-enabled {true|false}]` - Enable ComplianceClock sync to NTP system time (privilege: advanced)

Specifies whether synchronization should be enabled or not. This is a cluster wide option.

Examples

```
cluster1::> snaplock compliance-clock ntp modify -is-sync-enabled true
```

snaplock compliance-clock ntp show

Display SnapLock ComplianceClock synchronization setting

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

Description

The ` snaplock compliance-clock ntp show ` command will display ComplianceClock synchronization setting. It will display the following information:

- is-sync-enabled - Displays if the option to synchronize the ComplianceClock with system time has been enabled or not.

Examples

```
cluster1::> snaplock compliance-clock ntp show
Enable clock sync to NTP system time: true
```

snaplock event-retention commands

snaplock event-retention abort

Abort an Event Based Retention policy operation.

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

Description

The `snaplock event-retention abort` is used to abort an ongoing Event Based Retention (EBR) operation. This command only aborts the operations that have not yet completed. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

Parameters

`-vserver <vserver name>` - Vserver Name

Specifies the vserver on which the EBR operation is running.

`-operation-id <integer>` - Operation ID

Specifies the operation ID of the EBR operation that needs to be aborted.

Examples

The following example aborts an ongoing EBR operation with operation-id *16842754*:

```
vs1::> snaplock event-retention abort -operation-id 16842754
            vs1::>
```

snaplock event-retention apply

Apply an Event Based Retention policy on all files within a user specified path.

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

Description

The `snaplock event-retention apply` command starts a new operation to apply the specified Event Based Retention (EBR) policy to all files in the specified path. If a file is a regular file, it will be made a WORM file and retained for a retention-period as defined by the specified policy name. If a file is already WORM, its retention time will be extended to a retention-period as defined by the specified policy name, starting from the current time. The retention time of a file will be extended only if the file's current retention time is less than the new retention time value to be set. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

Parameters

`-vserver <vserver name>` - Vserver Name

Specifies the name of the Vserver which has the EBR policy defined to be applied on one or more files.

`-policy-name <text>` - Policy Name

Specifies the name of the EBR policy to be applied on one or more files.

`-volume <volume name>` - Volume

Specifies the name of the SnapLock volume containing a file path or a directory path as specified by the path parameter. The specified EBR policy is applied to one or more files depending on the value of path.

`-path <text>` - Path

Specifies the path relative to the output volume root, of the form "/path". The path can be path to a file or a directory. The EBR policy is applied to all files under the specified path. To apply the EBR policy to all files in a volume, specify the path as "/".

Examples

The following example starts an EBR operation to apply a policy on files for specified volume:

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
                SnapLock event based retention operation is queued. Run
"snaplock event-retention show -operation-id 16842754 -instance" to view
the operation status.
```

snaplock event-retention show-vservers

Show Vservers with SnapLock Event Based Retention policies

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

Description

The `snaplock event-retention show-vservers` command is used to display the Vservers that have SnapLock Event Based Retention (EBR) policies created.

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.

Examples

The following example displays all Vservers that have SnapLock EBR policies:

```
cluster-1::*> snaplock event-retention show-vservers
        Vserver
        -----------------
        vs1
```

snaplock event-retention show

Show status of Event Based Retention operation

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

Description

The `snaplock event-retention show` command displays the status of an Event Based Retention (EBR) operation. Information about completed operations will be cleaned up after an hour after completion. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

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

If this parameter is specified, the command displays all EBR operations that match the specified Vserver.

[-operation-id <integer>] - Operation ID

If this parameter is specified, the command displays all EBR operations that match the specified operation ID.

[-volume <volume name>] - Volume Name

If this parameter is specified, the command displays all EBR operations that match the specified volume. The parameter specifies the volume on which EBR operation is running or has completed.

[-path <text>] - Path

If this parameter is specified, the command displays all EBR operations that match the specified path. The parameter specifies the path on which EBR operation is running or has completed.

[-policy-name <text>] - Policy Name

If this parameter is specified, the command displays all EBR operations that match the specified policy name. The parameter specifies the EBR policy name.

[-retention-period {{<integer> seconds|minutes|hours|days|months|years} | infinite}] - Retention Period

If this parameter is specified, the command displays all EBR operations that match the specified retention period. The parameter specifies the retention period of the EBR policy.

[-num-files-processed <integer>] - Number of Files Processed

If this parameter is specified, the command displays all EBR operations that match the specified number of processed files. The parameter specifies the number of files on which EBR policy was applied successfully.

[-num-files-failed <integer>] - Number of Files Failed

If this parameter is specified, the command displays all EBR operations that match the specified number of failed files. The parameter specifies the number of files on which the application of EBR policy failed.

[-num-files-skipped <integer>] - Number of Files Skipped

If this parameter is specified, the command displays all EBR operations that match the specified number of skipped files. The parameter specifies the number of files on which the application of EBR policy was skipped. A file that is under legal-hold will be skipped. If the retention time of a file is being shortened as a result of applying the EBR policy, that file will also be skipped.

[-num-inodes-ignored <integer>] - Number of Inodes Ignored

If this parameter is specified, the command displays all EBR operations that match the specified number of ignored inodes. The parameter specifies the number of inodes on which the application of EBR policy was

not attempted because they were not regular files.

[-operation-status {Unknown|In-Progress|Failed|Aborting|Completed}] - Operation Status

If this parameter is specified, the command displays all EBR operations that match the specified operation status. The parameter specifies the operation status of an EBR operation.

[-status-details <text>] - Status Details

If this parameter is specified, the command displays all EBR operations that match the specified status details. The parameter specifies the status details of an EBR operation.

Examples

The following examples show the status of EBR operations for Vserver "vs1" and volume "slc" and the status of event-retention operation for operation ID *16842753* respectively.

```
vs1::*> snaplock event-retention operation show -volume slc
            Operation ID   Vserver         Volume          Operation
Status
            -------------- --------------- ---------------
----------------
            16842753       vs1             slc             Completed
            16842754       vs1             slc             In-progress
vs1::*> snaplock event-retention operation show -operation-id 16842753
Operation ID: 16842753
                    Vserver: vs1
                     Volume: slc
                       Path: /vol/slc/d1
                Policy Name: p1
           Retention Period: 10 years
  Number of Files Processed: 50
     Number of Files Failed: 0
   Number of Inodes Ignored: 2
           Operation Status: Completed
             Status Details: No error
```

snaplock event-retention policy create

Create SnapLock Event Based Retention policies for a Vserver

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

Description

The `snaplock event-retention policy create` command is used to create Event Based Retention (EBR) policies for a Vserver. A policy consists of a *policy-name* and a *retention-period*. Only a user with security login role *vsadmin-snaplock* is allowed to perform this operation.

Parameters

-vserver <vserver name> - Vserver Name

Specifies the name of the Vserver for which a policy needs to be created.

-name <text> - Policy Name

Specifies the name of the EBR policy to be created.

-retention-period {{<integer> seconds|minutes|hours|days|months|years} | infinite} - Event Retention Period

Specifies the retention period for an EBR policy.

Examples

The following example creates a new EBR policy "p1" for Vserver "vs1" with a retention period of *"10 years"* :

```
vs1::> snaplock event-retention policy create -name p1 -retention-period
"10 years"
```

snaplock event-retention policy delete

Delete SnapLock Event Based Retention policies for a Vserver

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

Description

The `snaplock event-retention policy delete` command is used to delete Event Based Retention (EBR) policies for a Vserver. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

Parameters

-vserver <vserver name> - Vserver Name

If this parameter is specified, the command deletes all EBR policies that match the specified Vserver.

-name <text> - Policy Name

If this parameter is specified, the command deletes all EBR policies that match the specified *`name`* .

Examples

The following example deletes retention policy "p1" for Vserver "vs1":

```
vs1::> snaplock event-retention policy delete -name p1
```

snaplock event-retention policy modify

Modify SnapLock Event Based Retention policies for a Vserver

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

Description

The `snaplock event-retention policy modify` command is used to modify the retention period of an Event Based Retention (EBR) policy for a Vserver. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

Parameters

`-vserver <vserver name>` - Vserver Name

Specifies the name of the Vserver for which retention period of a policy needs to be modified.

`-name <text>` - Policy Name

Specifies the name of the EBR policy for which the retention period needs to be modified.

`[-retention-period {{<integer> seconds|minutes|hours|days|months|years} | infinite}]` - Event Retention Period

Specifies the new value of retention period.

Examples

The following example modifies the retention period of policy "p1" for Vserver "vs1" to *`"5 years"`* :

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period
"5 years"
```

snaplock event-retention policy show

Show SnapLock Event Based Retention policies for a Vserver

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

Description

The `snaplock event-retention policy show` command is used to show Event Based Retention (EBR) policies for a Vserver. A policy consists of a *`policy-name`* and a *`retention-period`* . The command output depends on the parameter or parameters specified. If no parameters are specified, all policies for all vservers will be displayed. If one or more parameters are specified, only those entries matching the specified values will be displayed. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

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

If this parameter is specified, the command displays all EBR policies that match the specified Vserver.

[-name <text>] - Policy Name

If this parameter is specified, the command displays all EBR policies that match the specified *name* .

[-retention-period {{<integer> seconds|minutes|hours|days|months|years} | infinite}] - Event Retention Period

If this parameter is specified, the command displays all EBR policies that match the specified *retention-period* .

Examples

The following example displays all event-retention policies for vserver "vs1":

```
vs1::> snaplock event-retention policy show
            Vserver           Name                Retention Period
            ----------------- ------------------- --------------------
            vs1               p1                  10 years
            vs1               p2                  5 years
```

snaplock legal-hold commands

snaplock legal-hold abort

Abort Snaplock legal-hold operation.

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

Description

The `snaplock legal-hold abort` is used to abort an ongoing legal-hold operation. The type of legal-hold operations that can be aborted using this command are begin, end and dump-files. This command only aborts operations that have not yet completed. Only a user with security login role *vsadmin-snaplock* is allowed to perform this operation.

Parameters

-vserver <vserver name> - Vserver Name

Specifies the vserver on which the legal-hold operation is running.

-operation-id <integer> - Operation ID

Specifies the operation ID of the legal-hold operation to be aborted.

Examples

The following example aborts an ongoing legal-hold operation with operation-id *16842754* :

```
vs1::> snaplock legal-hold abort -operation-id 16842754
            vs1::>
```

snaplock legal-hold begin

Starts an operation to place files under legal-hold in the user specified path on a SnapLock compliance volume.

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

Description

The `snaplock legal-hold begin` command is used to place specified file or files under legal-hold for a given litigation. Only a user with security login role *vsadmin-snaplock* is allowed to perform this operation.

Parameters

-vserver <vserver name> - Vserver Name

Specifies the name of the Vserver which owns the volume. The specified file or files to be placed under legal-hold reside on this volume.

-litigation-name <text> - Litigation Name

Specifies the name of the litigation for which the file or files have to be placed under legal-hold.

-volume <volume name> - Volume

Specifies the name of the SnapLock compliance volume on which the file or files to be placed under legal-hold reside.

-path <text> - Path

Specifies a path relative to the volume root. The path can be either a file path of the single file to be placed under legal-hold or a directory path where all regular files under it must be placed under legal-hold.

Examples

The following example starts a legal-hold begin operation on file *file1* in volume *slc_vol1* :

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume
slc_vol1 -path /file1
SnapLock legal-hold begin operation is queued. Run "snaplock legal-hold
show -operation-id 16842773 -instance" to view the operation status.
```

The following example starts a legal-hold begin operation on all files in the volume *slc_vol1* :

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume
slc_vol1 -path /
SnapLock legal-hold begin operation is queued. Run "snaplock legal-hold
show -operation-id 16842775 -instance" to view the operation status.
```

snaplock legal-hold dump-files

Dump list of files under legal-hold to specified output path.

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

Description

The `snaplock legal-hold dump-files` is used to dump the list of files under legal-hold for a given vserver, volume and litigation to an auto-generated file in the user specified path. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

Parameters

`-vserver <vserver name>` - Vserver Name

Specifies the name of the Vserver for which the list of files under legal-hold is to be dumped.

`-litigation-name <text>` - Litigation Name

Specifies the name of the litigation for which the list of files under legal-hold is to be dumped.

`-volume <volume name>` - Volume Name

Specifies the name of the SnapLock compliance volume for which the list of files under legal-hold is to be dumped.

`-output-volume <volume name>` - Output Volume Name

Specifies the name of the output volume containing the output directory path where the list of files under legal-hold is to be dumped. The output volume must be a regular read-write volume.

`-output-directory-path <text>` - Path Relative to Output Volume Root

Specifies the output directory path relative to the output volume root, where the list of files under legal-hold is to be dumped. The output directory path should be of the form "/directory-path". If output needs to be dumped on the volume root, specify the path as "/".

Examples

The following example starts a legal-hold dump-files operation:

```
vs1::> snaplock legal-hold dump-files -volume vol1_slc -litigation-name
lit1 -output-volume vol1 -output-directory-path /d1
            SnapLock legal-hold dump-files operation is queued. Run
"snaplock legal-hold show -operation-id 16842754 -instance" to view the
operation status.
            vs1::>
```

snaplock legal-hold dump-litigations

Dump list of litigations for a given Vserver to specified output path.

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

Description

The `snaplock legal-hold dump-litigations` is used to dump the list of litigations for a given vserver to a user specified path. Under the user specified path, we create a directory with a unique name. Under the user specified path, a directory with an auto-generated name is created. Under this directory, multiple files are created. Each file represents a unique litigation name that was found in the given vserver. Each file contains a list of volume names that have files under legal-hold for that given litigation. For example, if the file name is "lit1" and the contents of the file are "volume1" and "volume2", then it indicates that both these volumes have files under legal-hold for litigation "lit1". Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

Parameters

`-vserver <vserver name>` - Vserver Name

Specifies the name of the Vserver for which the list of litigations is to be dumped.

`[-volume <volume name>]` - Volume Name

If this parameter is specified, the command displays the list of litigations for volume that matches the specified value. The volume must be of type SnapLock compliance.

`-output-volume <volume name>` - Output Volume Vame

Specifies the name of the output volume containing the output directory path where the list of litigations is to be dumped. The output volume must be a regular read-write volume.

`-output-directory-path <text>` - Path Relative to Output Volume Root

Specifies the output directory path relative to the volume root, where the list of litigations is to be dumped. The output directory path should be of the form "/directory-path". If output needs to be dumped to the volume root, specify the path as "/".

Examples

The following example starts a legal-hold dump-litigations job:

```
vs1::> snaplock legal-hold dump-litigations -output-volume vol1 -output
-directory-path /d1
            Dump Litigations job for Vserver "vs1" has been queued. Run
"job show -id 22 -instance" to view the status.
            vs1::>
```

snaplock legal-hold end

Starts an operation to release legal-hold on files in the user specified path on a SnapLock compliance volume.

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

Description

The `snaplock legal-hold end` command is used to release legal-hold on specified file or files for a given litigation. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

Parameters

`-vserver <vserver name>` - Vserver Name

Specifies the name of the Vserver which owns the volume. The specified file or files to be released from legal-hold reside on this volume.

`-litigation-name <text>` - Litigation Name

Specifies the name of the litigation for which the file or files have to release from legal-hold.

`-volume <volume name>` - Volume

Specifies the name of the SnapLock compliance volume on which the file or files to be released from legal-hold reside.

`-path <text>` - Path

Specifies a path relative to the volume root. The path can be either a file path of the single file to be released from legal-hold or a directory path where all regular files under it must be released from legal-hold.

Examples

The following example starts a legal-hold end operation on file *`file1`* in volume *`slc_vol1`* :

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume
slc_vol1 -path /file1
SnapLock legal-hold end operation is queued. Run "snaplock legal-hold show
-operation-id 16842773 -instance" to view the operation status.
```

The following example starts a legal-hold end operation on all files in the volume *`slc_vol1`* :

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume
slc_vol1 -path /
SnapLock legal-hold end operation is queued. Run "snaplock legal-hold show
-operation-id 16842775 -instance" to view the operation status.
```

snaplock legal-hold show

Show status of a legal-hold operation.

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

Description

The `snaplock legal-hold show` command displays the status of a legal-hold operation. Information about completed operations will be cleaned up after an hour of completion. Only a user with security login role *`vsadmin-snaplock`* is allowed to perform this operation.

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

If this parameter is specified, the command displays all legal-hold operations that match the specified Vserver.

[-operation-id <integer>] - Operation ID

If this parameter is specified, the command displays all legal-hold operations that match the specified operation ID.

[-volume <volume name>] - Volume Name

If this parameter is specified, the command displays all legal-hold operations that match the specified volume. The parameter specifies the volume on which legal-hold operation is running or has completed.

[-path <text>] - Path

If this parameter is specified, the command displays all legal-hold operations that match the specified path. The parameter specifies the path on which legal-hold operation is running or has completed.

[-litigation-name <text>] - Litigation Name

If this parameter is specified, the command displays all legal-hold operations that match the specified litigation name. The parameter specifies the legal-hold litigation name.

[-operation-type {unknown|begin|end|dump-files}] - Operation Type

If this parameter is specified, the command displays all legal-hold operations that match the specified

operation type. The parameter specifies the type of legal-hold operation.

[-operation-status {Unknown|In-Progress|Failed|Aborting|Completed}] - Operation Status

If this parameter is specified, the command displays all legal-hold operations that match the specified operation status. The parameter specifies the status of legal-hold operation.

[-num-files-processed <integer>] - Number of Files Processed

If this parameter is specified, the command displays all legal-hold operations that match the specified number of files processed. The parameter specifies the number of files on which legal-hold operation was successful.

[-num-files-failed <integer>] - Number of Files Failed

If this parameter is specified, the command displays all legal-hold operations that match the specified number of files failed. The parameter specifies the number of files on which legal-hold operation failed.

[-num-files-skipped <integer>] - Number of Files Skipped

If this parameter is specified, the command displays all legal-hold operations that match the specified number of files skipped.

The parameter specifies the number of files on which legal-hold begin operation was skipped. The legal-hold begin operation is skipped on a file if it is already under hold for a given litigation or if it is a hard link to a file that is already under hold for a given litigation.

[-num-inodes-ignored <integer>] - Number of Inodes Ignored

If this parameter is specified, the command displays all legal-hold operations that match the specified number of inodes ignored. The parameter specifies the number of inodes on which the legal-hold operation was not attempted because they were not regular files.

[-status-details <text>] - Status Details

If this parameter is specified, the command displays all legal-hold operations that match the specified status details. The parameter specifies the status details of an legal-hold operation.

Examples

The following examples show the status of legal-hold operations for Vserver *vs1* and volume *slc_vol1* and the status of legal-hold operation for operation ID *16842786* respectively:

```
vs1::> snaplock legal-hold show -volume slc_vol1
                                                    Operation
Operation     Operation ID    Vserver   Volume      Status
------------- --------------- --------- ----------- ---------
begin         16842784        vs1       slc_vol1
                                                    Completed
begin         16842786        vs1       slc_vol1
                                                    Completed
begin         16842788        vs1       slc_vol1
                                                    In-Progress
dump-files    16842790        vs1       slc_vol1
                                                    Completed
end           16842794        vs1       slc_vol1
                                                    Completed
5 entries were displayed.

vs1::> snaplock legal-hold show -operation-id 16842786
Vserver: vs1
                      Volume: slc_vol1
                Operation ID: 16842786
             Litigation Name: litigation1
                        Path: /
              Operation Type: begin
                      Status: Completed
   Number of Files Processed: 100
      Number of Files Failed: 15
     Number of Files Skipped: 20
    Number of Inodes Ignored: 0
              Status Details: No error
```

snaplock log commands

snaplock log create

Create audit log configuration for a Vserver.

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

Description

```
The `snaplock log create` command is used to create a SnapLock log
configuration for the Vserver. A SnapLock log configuration consists of
volume to store the log, the maximum size of the log file, and the default
period of time for which the log file should be retained.
```

Parameters

-vserver <vserver name> - Vserver Name

Specifies the name of the Vserver for which the configuration needs to be created.

-volume <volume name> - Log Volume Name

Specifies the name of the volume that is used for logging. This must be a SnapLock Compliance volume.

[-max-log-size {<integer>[KB|MB|GB|TB|PB]}] - Maximum Size of Log File

Specifies the maximum size of the log file. Once a log file reaches this limit, it is archived and a new log file is created. This parameter is optional. The default value is *10MB* .

[-default-retention-period {{<integer> seconds|minutes|hours|days|months|years} | infinite}] - Default Log Record Retention Period

Specifies the default period of time a record (which is logged) is retained. This parameter is optional. The default value is *"6 months"* .

Examples

```
cluster1::> snaplock log create -volume vol1 -max-log-size 50MB -default
-retention-period "1 year" -vserver vs1
        [Job 47] Job succeeded: SnapLock log created for Vserver "vs1".
```

snaplock log delete

Delete audit log configuration for a Vserver.

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

Description

The `snaplock log delete` command deletes the SnapLock log configuration associated with the Vserver. This command closes all the active log files in the log volume and mark the volume as disabled for SnapLock logging.

Parameters

-vserver <vserver name> - Vserver Name

Specifies the name of the Vserver whose SnapLock log configuration is deleted.

Examples

```
cluster1::> snaplock log delete -vserver vs1
        [Job 47] Job succeeded: SnapLock log deleted for Vserver "vs1".
```

snaplock log modify

Modify audit log configuration for a Vserver.

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

Description

The `snaplock log modify` command modifies the SnapLock log configuration of the Vserver. Log volume, maximum size of log file, and default retention period can be modfied. If the log volume is modified, then the active log files in the existing log volume is closed and the log volume is marked as disabled for logging. The new log volume is enabled for logging.

Parameters

`-vserver <vserver name>` - Vserver Name

Specifies the name of the Vserver for which the SnapLock log configuration needs to be modified.

`[-volume <volume name>]` - Log Volume Name

Specifies the new log volume that is configured for this Vserver for logging.

`[-max-log-size {<integer>[KB|MB|GB|TB|PB]}]` - Maximum Size of Log File

Specifies the new value for maximum log file size.

`[-default-retention-period {{<integer> seconds|minutes|hours|days|months|years} | infinite}]` - Default Log Record Retention Period

Specifies the new value for default retention period.

Examples

```
cluster1::> snaplock log modify -volume vol1 -vserver vs1 -max-log-size
15MB
        [Job 48] Job succeeded: SnapLock log modified for Vserver "vs1".
```

snaplock log show

Display audit log configuration.

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

Description

The `snaplock log show` command displays the following information about the SnapLock log infrastructure:

- Vserver name
- Volume name
- Maximum log size
- Default retention period

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

If this parameter is specified, the command displays the log information for Vserveers that match the specified value.

[-volume <volume name>] - Log Volume Name

If this parameter is specified, the command displays the log configuration for volumes that match the specified value.

[-max-log-size {<integer>[KB|MB|GB|TB|PB]}] - Maximum Size of Log File

If this parameter is specified, the command displays the log configuration with a matching `-max-log-size` value.

[-default-retention-period {{<integer> seconds|minutes|hours|days|months|years} | infinite}] - Default Log Record Retention Period

If this parameter is specified, the command displays the log configuration with a matching `-default-retention-period` value.

Examples

```
cluster1::> snaplock log show -vserver vs1
Vserver Name                          : vs1
      Log Volume Name                      : 15MB
      Maximum Size of Log File             : 15MB
      Default Log Record Retention Period : 6 months
```

```
cluster1::> snaplock log show
        Vserver           Volume              Maximum Size
Retention Period
        ----------------- ------------------- --------------------
--------------------
        vs1               vol1                15MB                 6 months
```

snaplock log file archive

Archive Active Log Files in Log Volume

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

Description

The `snaplock log file archive` command archives the currently active log file by closing it and creating a new active log file. If base-name is not provided, the command archives all active log files associated with the Vserver. Otherwise, the command archives the active log file associated with the base-name provided.

Parameters

`-vserver <vserver name>` - Vserver Name

Specifies the name of the Vserver for which active log files need to be archived.

`[-base-name {privileged-delete | system | legal-hold}]` - Base Name of Log File

Specifies the log base-name, whose active log file needs to be archived. The base-name is the name of the source of log records. Valid base-names are *`system`* , *`privileged-delete`* and *`legal-hold`* . Each base-name has its own directory in which log files containing log records generated by base-name are stored.

Examples

```
cluster1::> snaplock log archive -vserver vs1
        [Job 48] Job succeeded: SnapLock log archived for Vserver "vs1".
```

snaplock log file show

Display audit log file information.

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

Description

The `snaplock log file show` command displays the following information about the log files:

- Vserver name
- Volume name
- File path
- Expiry time of the file
- File size

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

If this parameter is specified, then log files in the Vserver that match the specified value is displayed.

[-base-name {privileged-delete | system | legal-hold}] - Base Name of Log File

If this parameter is specified, then the log files having a matching `-base-name` is displayed.

[-volume <volume name>] - Log Volume Name

If this parameter is specified, then the log files in volumes that match the specified value are shown.

[-file-path <text>] - Log File Path

If this parameter is specified, then the log files that match the specified value are displayed.

[-expiry-time <text>] - Log File Expiry Time

If this parameter is specified, then the log files having a matching `-expiry-time` value are displayed.

[-file-size {<integer>[KB|MB|GB|TB|PB]}] - File Size

If this parameter is specified, then the log files having a matching `-file-size` value are displayed.

Examples

```
cluster1::> snaplock log file show
        Vserver           Volume              Base Name           File
Path
        ----------------- ------------------- -------------------
--------------------
        vs1               vol1                system
/vol/vol1/snaplock_log/system_logs/20160120_183756_GMT-present
```

```
cluster1::> snaplock log file show -vserver vs1 -base-name system
Vserver     : vs1
        Volume      : vol1
        Base Name   : system
        File Path   :
/vol/vol1/snaplock_log/system_logs/20160120_183756_GMT-present
        Expiry Time : Wed Jul 20 18:37:56 GMT 2016
        File Size   : 560B
```

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.