vserver fpolicy commands

Command reference

NetApp
February 02, 2026

Table of Contents

vserver fpolicy commands

vserver fpolicy disable

Disable a policy

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

Description

The `vserver fpolicy disable` command disables an FPolicy policy for the specified Vserver.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to disable an FPolicy policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy you want to disable.

Examples

The following command disables an FPolicy policy.

```
cluster1::> vserver fpolicy show
Vserver                 Policy Name                    Sequence  Status
Engine
----------------------- ------------------------------ --------  ------
--------
vs1.example.com         vs1_pol                               -  off
native
vs2.example.com         vs2_pol                               5  on
external
2 entries were displayed.

cluster1::> vserver fpolicy disable -vserver vs2.example.com -policy-name
vs2_pol

cluster1::> vserver fpolicy show
Vserver                 Policy Name                    Sequence  Status
Engine
----------------------- ------------------------------ --------  -------
-------
vs1.example.com         vs1_pol                               -  off
native
vs2.example.com         vs2_pol                               -  off
external
2 entries were displayed.
```

vserver fpolicy enable

Enable a policy

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

Description

The `vserver fpolicy enable` command enables FPolicy policies for the specified Vserver and sets their sequence (priority). The sequence is used when multiple policies have subscribed to the same file access event. To modify the sequence number of a policy, the administrator must disable the policy (if it is enabled) and then use this command to enable it with the new sequence number. Policies that use the *`native`* engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them.

ⓘ Events on FlexGroup volumes do not notify the FPolicy server.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to enable an FPolicy policy. The

Vserver administrator can enable FPolicy policies created within the scope of the Vserver and can also enable an FPolicy policy created by the cluster administrator. The cluster administrator can enable FPolicy policies for any Vserver but cannot enable them with a scope of cluster. The scope is determined at a Vserver level.

`-policy-name <Policy name>` **- Policy**

This parameter specifies the name of the FPolicy policy you want to enable.

`-sequence-number <integer>` **- Policy Sequence Number**

This parameter specifies the sequence number that is assigned to the policy.

Examples

The following command enables an FPolicy policy:

```
cluster1::> vserver fpolicy show
Vserver                 Policy Name                    Sequence  Status
Engine
----------------------- ------------------------------ --------  ------
--------
vs1.example.com         vs1_pol                               -  off
native
vs2.example.com         vs2_pol                               -  off
external
2 entries were displayed.
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                 Policy Name                    Sequence  Status
Engine
----------------------- ------------------------------ --------  -------
-------
vs1.example.com         vs1_pol                               -  off
native
vs2.example.com         vs2_pol                               5  on
external
2 entries were displayed.
```

vserver fpolicy engine-connect

Establish a connection to FPolicy server

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

Description

The `vserver fpolicy engine-connect` command connects an FPolicy server to a specified node. Connecting the FPolicy server to a node enables FPolicy processing, providing the FPolicy configuration is complete. Before connecting an FPolicy server to a node, you must configure FPolicy by completing the following tasks:

- Create an FPolicy event
- Create an FPolicy external engine
- Create an FPolicy policy
- Create a scope for the FPolicy policy

ⓘ The FPolicy event and external engine must be attached to the FPolicy policy.

ⓘ The FPolicy policy should be enabled.

Parameters

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

This parameter specifies the node that you want to connect to the FPolicy server. The value local specifies the current node.

`-vserver <Vserver Name>` - Vserver

This parameter specifies the Vserver that you want to connect to the specified FPolicy server using the specified FPolicy policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy that is attached to an external engine.

`-server <IP Address>` - Server

This parameter specifies the FPolicy server to which you want to connect the node. The specified server must be present in the external engine configuration of the above specified policy.

Examples

The following example connects an FPolicy server.

```
cluster1::> vserver fpolicy engine-connect -node FPolicy-01 -vserver
vs1.example.com -policy-name p -server 1.1.1.1
cluster1::> vserver fpolicy show
  FPolicy                                                       Server-
Server-
  Vserver         Policy        Node          Server            status
type
  --------------- ------------- ------------ -----------------
-------------- -----------
  vs1.example.com p             FPolicy-01   1.1.1.1           connected
primary
```

vserver fpolicy engine-disconnect

Terminate connection to FPolicy server

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

Description

The `vserver fpolicy engine-disconnect` command disconnects an FPolicy server from a specified node.

Parameters

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

This parameter specifies the node that you want to disconnect from the FPolicy server. The value local specifies the current node.

`-vserver <Vserver Name>` - Vserver

This parameter specifies the Vserver that you want to disconnect from the specified FPolicy server with the specified attached FPolicy policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy that is attached with an external engine.

`-server <IP Address>` - Server

This parameter specifies the FPolicy server you want to disconnect. The specified server must be present in the external engine configuration of the above specified FPolicy policy.

Examples

The following example disconnects an FPolicy server.

```
cluster1::> vserver fpolicy engine-disconnect -node FPolicy-01 -vserver
vs1.example.com -policy-name p -server 1.1.1.1
cluster1::> vserver fpolicy show
 FPolicy                                                     Server-
Server-
 Vserver         Policy        Node         Server            status
type
 --------------- ------------- ------------ -----------------
-------------- -----------
 vs1.example.com p             FPolicy-01   1.1.1.1           disconnected
primary
```

vserver fpolicy show-enabled

Display all enabled policies

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

Description

The `vserver fpolicy show-enabled` command displays information about all enabled policies in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy policies:

- Vserver name
- Policy name
- Priority

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy policies.

You can specify the `-instance` parameter to display information for all FPolicy policies in a list format.

Parameters

{ `[-fields <fieldname>,…]`

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| `[-instance ]` }

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

`[-vserver <vserver>]` - Vserver

If you specify this parameter, the command displays information only about the FPolicy policies for the specified Vserver.

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

If you specify this parameter, the command displays information only about the FPolicy policy that you specify.

`[-priority <text>]` **- Policy Priority**

If you specify this parameter, the command displays information only about the FPolicy policies with the policy priority that you specify.

Examples

The following example displays the information about enabled FPolicy policies on the cluster.

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name                    Priority

----------------------- ------------------------------ ----------
vs1.example.com         pol_native                     native
vs1.example.com         pol_native2                    native
vs1.example.com         pol1                           2
vs1.example.com         pol2                           4
```

vserver fpolicy show-engine

Display FPolicy server status

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

Description

The `vserver fpolicy show-engine` command displays status information for all FPolicy external engines or displays status information only for FPolicy servers for a specified Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information for all FPolicy servers:

- Vserver name
- Node name
- FPolicy policy name
- FPolicy server IP Address
- FPolicy server status
- FPolicy server type

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy servers. You can specify specific parameters to display only information that matches those parameters. For instance, to display information only about all FPolicy servers (external engines) that are connected, run the command with the `-fields` parameter set to server and `-server-status ` parameter set to connected.

You can specify the `-instance` parameter to display all information for all policies in the list form.

Parameters

{ `[-fields <fieldname>,…]`

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| `[-instance ]` }

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

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

If you specify this parameter, the command displays information only about the FPolicy external engine attached to the specified node.

`[-vserver <Vserver Name>]` - Vserver

If you specify this parameter, the command displays information only about the FPolicy server for the specified Vserver.

`[-policy-name <Policy name>]` - Policy

If you specify this parameter, the command displays information only about the FPolicy servers that are attached with the specified policy.

`[-server <IP Address>]` - Server

If you specify this parameter, the command displays information only about the FPolicy servers that you specify.

`[-server-status <Status>]` - Server Status

If you specify this parameter, the command displays information only about the FPolicy servers that have the specified status.

`[-server-type <Server Type>]` - Server Type

If you specify this parameter, the command displays information only about the FPolicy servers that have the specified server type.

`[-connected-since <MM/DD/YYYY HH:MM:SS>]` - Time FPolicy Server was Connected

If you specify this parameter, the command displays information only about the FPolicy servers that have been connected since the specified time.

`[-disconnected-since <MM/DD/YYYY HH:MM:SS>]` - Time FPolicy Server was Disconnected

If you specify this parameter, the command displays information only about the FPolicy servers that have been disconnected since the specified time.

`[-disconnect-reason <text>]` - Reason for FPolicy Server Disconnection

If you specify this parameter, the command displays information only about the FPolicy servers that are disconnected because of the specified reason.

`[-disconnect-reason-id <integer>]` - ID for FPolicy Server Disconnection

If you specify this parameter, the command displays information about the FPolicy servers that are disconnected because of the specified disconnect reason ID. There is a unique ID associated with each disconnect reason, which can be used to identify the reason for FPolicy server disconnection.

`[-session-id <text>]` - Session ID

If you specify this parameter, the command displays information about the FPolicy server that is connected with the specified session ID. There is a unique session ID associated with each connection to FPolicy server, which can be used to identify the established connection.

Examples

This example displays information about all FPolicy servers (external engines).

```
cluster1::> vserver fpolicy show-engine
 FPolicy                                                      Server-
Server-
 Vserver         Policy        Node         Server            status
type
 --------------- ------------- ------------ -----------------
-------------- -----------
 vs2.example.com vs2_pol       FPolicy-01   9.9.9.9           connected
primary
 vs1.example.com vs1_pol       FPolicy-01   1.1.1.1           connected
primary
 2 entries were displayed.
```

This example displays information only about all connected FPolicy servers (external engines).

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
 node       vserver         policy-name server
 ---------- --------------- ----------- -------
 FPolicy-01 vs1.example.com vs1_pol     1.1.1.1
```

This example displays information about an FPolicy server.

```
cluster1::> vserver fpolicy show-engine -server 10.72.204.118 -instance
Node: fpol-01
                                Vserver: vserver_1.example.com
                                 Policy: pol_cifs
                                 Server: 10.72.204.118
                          Server Status: disconnected
                            Server Type: primary
      Time FPolicy Server was Connected: -
   Time FPolicy Server was Disconnected: 2/5/2013 05:06:22
Reason for FPolicy Server Disconnection: TCP Connection to FPolicy server
failed.
    ID for FPolicy Server Disconnection: 9307
                             Session ID:
```

vserver fpolicy show-passthrough-read-connection

Display connection status for FPolicy passthrough-read

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

Description

The `vserver fpolicy show-passthrough-read-connection` command displays the status of the passthrough-read connection from all FPolicy servers. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. If you do not specify any parameters, the command displays following information about the passthrough-read connection from FPolicy servers:

- Vserver name
- FPolicy policy name
- Node name
- FPolicy server IP address
- Passthrough-read connection status

You can specify the `-fields` parameter to specify which fields of information to display. In addition to the fields above, you can display the following fields.

- Session ID of the control channel
- Time passthrough-read channel was connected
- Time passthrough-read channel was disconnected
- Reason for passthrough-read channel disconnection

You can specify the `-instance` parameter to display information for all passthrough-read connections in the list form.

Parameters

{ `[-fields <fieldname>,…]`

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| `[-instance ]` }

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

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

If you specify this parameter, the command displays information only about the passthrough-read connections on the specified node.

`[-vserver <Vserver Name>]` - Vserver

If you specify this parameter, the command displays information only about the passthrough-read connections for the specified Vserver.

`[-policy-name <Policy name>]` - Policy

If you specify this parameter, the command displays information only about the passthrough-read connections that are attached with the specified FPolicy policy.

`[-server <IP Address>]` - Server

If you specify this parameter, the command displays information only about the passthrough-read connections from the specified FPolicy server.

`[-control-session-id <text>]` - Session ID of the Control Channel

If you specify this parameter, the command displays information only about the passthrough-read connections that are connected with the specified control session ID. The passthrough-read connection is attached to a control connection that has a unique control session ID.

`[-server-status <Status of fpolicy passthrough-read connection>]` - Server Status

If you specify this parameter, the command displays information only about the passthrough-read connections that have the specified status.

`[-connected-since <MM/DD/YYYY HH:MM:SS>]` - Time Channel Was Connected

If you specify this parameter, the command displays information only about the passthrough-read connections that have the specified connection time.

`[-disconnected-since <MM/DD/YYYY HH:MM:SS>]` - Time Channel Was Disconnected

If you specify this parameter, the command displays information only about the passthrough-read connections that have the specified disconnection time.

`[-disconnect-reason <Reason for fpolicy passthrough-read disconnection>]` - Reason for Disconnection

If you specify this parameter, the command displays information only about the passthrough-read connections that are disconnected because of the specified disconnect reason.

Examples

This example displays information about passthrough-read connections from all FPolicy servers.

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                            FPolicy           Server
Vserver          Policy Name   Node         Server            Status
---------------  ------------- ------------ -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
2 entries were displayed.
```

This example displays information about passthrough-read connections from all connected FPolicy servers.

```
cluster1::> vserver fpolicy show-passthrough-read-connection -server
-status connected
                                            FPolicy           Server
Vserver          Policy Name   Node         Server            Status
---------------  ------------- ------------ -----------------
--------------
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

This example displays information about passthrough-read connections from FPolicy servers configured in an FPolicy policy.

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance
Node: FPolicy-01
                                          Vserver: vserver_1.example.com
                                           Policy: pol_cifs_1
                                           Server: 2.2.2.2
                Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                    Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

vserver fpolicy show

Display all policies with status

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

Description

The `vserver fpolicy show` command displays status information about all FPolicy policies in the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy policies:

- Vserver name
- Policy name
- Sequence number
- Status

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy policies.

You can specify the `-instance` parameter to display information for all FPolicy policies in a list format.

Parameters

{ `[-fields <fieldname>,…]`

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| `[-instance ]` }

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

`[-vserver <Vserver Name>]` - Vserver

If you specify this parameter, the command displays information only about the FPolicy policies for the specified Vserver.

`[-policy-name <Policy name>]` - Policy

If you specify this parameter, the command displays information only about the FPolicy policy that you specify.

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

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified sequence-number.

`[-status {on|off}]` - Status

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified status.

`[-engine <Engine name>]` - FPolicy Engine

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified engine.

Examples

The following example displays the information about FPolicy policies on the cluster using the `vserver fpolicy show` command.

```
cluster1::> vserver fpolicy show
                                                               Sequence
            Vserver                 Policy Name                  Number
Status      Engine
            ----------------------- -------------------------- --------
---------   ---------
            FPolicy                 cserver_policy             -
off         eng1
            vs1.example.com         v1p1                       -
off         eng2
            vs1.example.com         v1p2                       -
off         native
            vs1.example.com         v1p3                       -
off         native
            vs1.example.com         cserver_policy             -
off         eng1
            vs2.example.com         v1p1                       3
on          native
            vs2.example.com         v1p2                       1
on          eng3
            vs2.example.com         cserver_policy             2
on          eng1
            8 entries were displayed.
```

vserver fpolicy persistent-store create

Create a Persist Store

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

Description

The `vserver fpolicy persistent-store create` command create an FPolicy Persistent Store entry for the Vserver. This can then be used for enabling the persistent mode for Fpolicy events by specifying the Fpolicy Persistent Store name for the parameter "persistent-store" when creating/modifying the Fpolicy policy. In persistent mode, when the Persistent Store is full, event notifications are dropped.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create FPolicy Persistent Store.

`-persistent-store <text>` - Persistent Store Name

This parameter specifies the name of the FPolicy Persistent Store that you want to create.

`-volume <text>` **- Volume name of the Persistent Store**

This parameter specifies volume name for the FPolicy Persistent Store.

`[-size {<integer>[KB|MB|GB|TB|PB]}]` **- Size of the Persistent Store**

This parameter specifies size of the FPolicy Persistent Store.

`[-autosize-mode {off|grow|grow_shrink}]` **- Autosize Mode for the Volume**

This parameter specifies autosize mode of the volume. The valid values are: *`off`* , *`grow`* , *`grow_shrink`* . The default value is *`off`* .

Examples

The following example creates an FPolicy persistent-store.

```
cluster1::> vserver fpolicy persistent-store create -vserver
vs1.example.com -persistent-store ps1 -volume psvol -size 1GB -autosize
-mode grow


cluster1::> vserver fpolicy persistent-store show -vserver vs1 -persistent
-store ps1
Vserver: vs1.example.com
                                             Persistent Store Name: ps1
                               Volume name of the Persistent store: psvol
                                      Size of the Persistent Store: 1GB
                                      Autosize Mode for the Volume: grow
```

vserver fpolicy persistent-store delete

Delete a Persist Store

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

Description

The `vserver fpolicy persistent-store delete` command deletes an FPolicy Persistent Store.

Parameters

`-vserver <Vserver Name>` **- Vserver**

This parameter specifies the name of the Vserver from which you want to delete the FPolicy Persistent Store.

`-persistent-store <text>` **- Persistent Store Name**

This parameter specifies the name of the FPolicy Persistent Store that you want to delete.

`[-delete-volume {true|false}]` - Delete the Persistent Store Volume

This parameter specifies if the associated volume for the FPolicy Persistent Store has to be deleted. By default, it will be false.

Examples

The following example deletes an FPolicy Persistent Store.

```
cluster1::> vserver fpolicy persistent-store delete -vserver
vs1.example.com -persistent-store ps1 -delete-volume true
```

vserver fpolicy persistent-store modify

Modify a Persist Store

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

Description

The `vserver fpolicy persistent-store modify` command modifies an FPolicy Persistent Store.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy Persistent Store.

`-persistent-store <text>` - Persistent Store Name

This parameter specifies name of the FPolicy Persistent Store that you want to modify.

`[-volume <text>]` - Volume name of the Persistent Store

This parameter specifies volume name for the FPolicy Persistent Store.

`[-size {<integer>[KB|MB|GB|TB|PB]}]` - Size of the Persistent Store

This parameter specifies size of the FPolicy Persistent Store.

`[-delete-volume {true|false}]` - Delete the previous Volume

This parameter specifies if the previously associated volume for the FPolicy Persistent Store has to be deleted. By default, it will be false.

Examples

The following example modifies an FPolicy Persistent Store.

```
cluster1::> vserver fpolicy persistent-store modify -vserver
vs1.example.com -persistent-store ps1 -volume psvol -size 1GB -delete
-volume true


cluster1::> vserver fpolicy persistent-store show -vserver vs1.example.com
-persistent-store ps1 -size 1GB
Vserver: vs1.example.com
                                             Persistent Store Name: ps1
                               Volume name of the Persistent Store: psvol
                                      Size of the Persistent Store: 1GB
```

vserver fpolicy persistent-store show

Display Persist Store details

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

Description

The `vserver fpolicy persistent-store show` command displays information about all FPolicy Persistent Store belonging to the Vserver. Any Vserver administrator can see FPolicy persistent store associated with their Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays information about all FPolicy persistent store:

- Vserver Name
- Persistent Store Name
- Persistent Store Volume name

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy persistent-store. You can specify additional parameters to display only information that matches those parameters. For example, to display information only about FPolicy Persistent Store where the FPolicy persistent store belong to particular Vserver vs1, run the command with the `-vserver` parameter set to vs1.

You can specify the `-instance` parameter to display all information for all policies in the list form.

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 you specify this parameter, the command displays information only about the FPolicy Persistent Store for the specified Vserver.

`[-persistent-store <text>]` - Persistent Store Name

If you specify this parameter, the command displays information only about the FPolicy Persistent Store that you specify.

`[-volume <text>]` - Volume name of the Persistent Store

If you specify this parameter, the command displays information only about the FPolicy Persistent Store that use the specified volume name.

`[-size {<integer>[KB|MB|GB|TB|PB]}]` - Size of the Persistent Store

If you specify this parameter, the command displays information only about the FPolicy Persistent Store that has the specified size.

`[-autosize-mode {off|grow|grow_shrink}]` - Autosize Mode for the Volume

If you specify this parameter, the command displays information only about the FPolicy Persistent Store that has the specified autosize mode.

Examples

The following example displays the information about FPolicy Persistent Store on the cluster using the `vserver fpolicy persistent-store show` command.

```
cluster1::> vserver fpolicy persistent-store show

Vserver         Persistent Store Volume Size
--------------- ---------------- ------ ----
vs1.example.com ps1              psvol  1GB
vs2.example.com ps2              psvol1 100MB
```

vserver fpolicy policy create

Create a policy

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

Description

The `vserver fpolicy policy create` command creates an FPolicy policy. You must create an FPolicy event name before creating an FPolicy policy. If you are using an external FPolicy server, you must also create an FPolicy engine before creating a policy.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create an FPolicy policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy that you want to create. An FPolicy policy name can be up to 256 characters long and is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_" and "." .

`-events <Event name>,…` - Events to Monitor

This parameter specifies a list of events to monitor for the FPolicy policy. All the events in the event list should be created by the administrator of the specified Vserver or the cluster administrator. The events must already exist. Create events using the `fpolicy policy event create` command.

`-engine <Engine name>` - FPolicy Engine

This parameter specifies an external engine for this FPolicy policy. An external engine contains information required by the node to send notifications to an FPolicy server. The Vserver administrator of the specified Vserver or the cluster administrator creates the external engine prior to creating the FPolicy policy. If this parameter is not specified, the default *`native`* external engine is used. The *`native`* external engine is internal to ONTAP and is used if you want to configure native file blocking and you do not want to use an external FPolicy server.

`[-is-mandatory {true|false}]` - Is Mandatory Screening Required

This parameter specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to *`true`* , file access events will be denied under these circumstances. To allow file access events under these circumstances, set this parameter to *`false`* . By default, it is *`true`* .

`[-allow-privileged-access {yes|no}]` - Allow Privileged Access

This parameter specifies privileged access for FPolicy servers. It is used to specify whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. With this option set to *`yes`* , FPolicy servers can access files on the cluster using a separate data channel with privileged access. By default, it is *`no`* .

`[-privileged-user-name <text>]` - User Name for Privileged Access

This parameter specifies the privileged user name. It is used to specify the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in *`"domain\user name"`* format. If `-allow-privileged-access` is set to *`no`* , any value set for this field is ignored.

`[-is-passthrough-read-enabled {true|false}]` - Is Passthrough Read Enabled

This parameter specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are the files which have been moved to secondary storage. If passthrough-read is enabled, the FPolicy server provides the data for the file over a separate channel instead of restoring the file to primary storage. By default, this parameter is *`false`* .

`[-persistent-store <text>]` - Persistent Store Name

This parameter specifies persistent storage name. This can then be used for enabling the Persistent mode for Fpolicy events.

Examples

The following example creates an FPolicy policy.

```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com -policy
-name vs1_pol -events cserver_evt,v1e1
          -engine native -is-mandatory true -allow-privileged-access no
-is-passthrough-read-enabled false

cluster1::> vserver fpolicy policy show -vserver vs1.example.com -policy
-name vs1_pol
Vserver: vs1.example.com
                    Policy Name: vs1_pol
              Events to Monitor: cserver_evt, v1e1
                 FPolicy Engine: native
Is Mandatory Screening Required: true
        Allow Privileged Access: no
User Name for Privileged Access: -
    Is Passthrough Read Enabled: false
          Persistent Store Name: -
```

vserver fpolicy policy delete

Delete a policy

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

Description

The `vserver fpolicy policy delete` command deletes an FPolicy policy.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver from which you want to delete the FPolicy policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy that you want to delete.

Examples

The following example deletes an FPolicy policy.

```
cluster1::> vserver fpolicy policy delete -vserver vs1.example.com -policy
-name vs1_pol
```

vserver fpolicy policy modify

Modify a policy

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

Description

The `vserver fpolicy policy modify` command modifies an FPolicy policy.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy policy.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy that you want to modify. An FPolicy policy name can be up to 256 characters long and is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_" and ".".

`[-events <Event name>,…]` - Events to Monitor

This parameter specifies a list of events to monitor for the FPolicy policy. All the events in the event list should be created by the administrator of the specified Vserver or the cluster administrator. The events must already exist. Create events using the `fpolicy policy event create` command.

`[-engine <Engine name>]` - FPolicy Engine

This parameter specifies an external engine for this FPolicy policy. An external engine contains information required by the node to send notifications to an FPolicy server. The Vserver administrator of the specified Vserver or the cluster administrator creates the external engine prior to modifying the FPolicy policy. If this parameter is not specified, the default *`native`* external engine is used. The *`native`* `_ external engine is internal to ONTAP and is used if you want to configure _native` file blocking and you do not want to use an external FPolicy server.

`[-is-mandatory {true|false}]` - Is Mandatory Screening Required

This parameter specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to *`true`* , file access events will be denied under these circumstances. To allow file access events under these circumstances, set this parameter to *`false`* . By default, it is *`true`* .

`[-allow-privileged-access {yes|no}]` - Allow Privileged Access

This parameter specifies privileged access for FPolicy servers. It is used to specify whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. With this option set to *`yes`* , FPolicy servers can access files on the cluster using a separate data channel with privileged access. By default, it is *`no`* .

`[-privileged-user-name <text>]` - User Name for Privileged Access

This parameter specifies the privileged user name. It is used to specify the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in *`"domain\user name"`* format. If `-allow-privileged-access` is set to *`no`* , any value set for this field is ignored.

`[-is-passthrough-read-enabled {true|false}]` - Is Passthrough Read Enabled

This parameter specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are the files which have been moved to secondary storage. If passthrough-read is enabled, the FPolicy server provides the data for the file over a separate channel instead of restoring the file to primary storage. By default, this parameter is `false` .

`[-persistent-store <text>]` - Persistent Store Name

This parameter specifies persistent storage name. This can then be used for enabling the Persistent mode for Fpolicy events.

Examples

The following example modifies an FPolicy policy.

```
cluster1::> vserver fpolicy policy modify -vserver vs1.example.com -policy
-name vs1_pol -events cserver_evt,v1e1
          -engine native -is-mandatory true -allow-privileged-access no
-is-passthrough-read-enabled false

cluster1::> vserver fpolicy policy show -vserver vs1.example.com -policy
-name vs1_pol
Vserver: vs1.example.com
                    Policy Name: vs1_pol
              Events to Monitor: cserver_evt, v1e1
                 FPolicy Engine: native
Is Mandatory Screening Required: true
        Allow Privileged Access: no
User Name for Privileged Access: -
    Is Passthrough Read Enabled: false
          Persistent Store Name: -
```

vserver fpolicy policy show

Display policy configuration

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

Description

The `vserver fpolicy policy show` command displays information about all FPolicy policies belonging to the Vserver. Any Vserver administrator can see FPolicy policies associated with their Vserver as well as policies created by the cluster administrator. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy policies:

- Vserver name

- Policy name
- Events to monitor
- FPolicy engine
- Is mandatory screening required
- Allow privileged access
- User name for privileged access

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy policies. You can specify additional parameters to display only information that matches those parameters. For example, to display information only about FPolicy policies where the FPolicy server requires privileged access, run the command with the `-fields` parameter set to policy-name (no "-") and `-allow-privileged -access` parameter set to *`yes`* .

You can specify the `-instance` parameter to display all information for all policies in the list form.

Parameters

`{ [-fields <fieldname>,…]`

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

`| [-instance ] }`

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

`[-vserver <Vserver Name>]` - Vserver

If you specify this parameter, the command displays information only about the FPolicy policies for the specified Vserver. FPolicy policies created by the cluster administrator are visible for all Vservers.

`[-policy-name <Policy name>]` - Policy

If you specify this parameter, the command displays information only about the FPolicy policy that you specify.

`[-events <Event name>,…]` - Events to Monitor

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified event or events.

`[-engine <Engine name>]` - FPolicy Engine

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified engine.

`[-is-mandatory {true|false}]` - Is Mandatory Screening Required

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified mandatory attribute.

`[-allow-privileged-access {yes|no}]` - Allow Privileged Access

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified privileged access.

`[-privileged-user-name <text>]` **- User Name for Privileged Access**

If you specify this parameter, the command displays information only about the FPolicy policy or policies that use the specified privileged user name.

`[-is-passthrough-read-enabled {true|false}]` **- Is Passthrough Read Enabled**

If you specify this parameter, the command displays information only about the FPolicy policies that use the specified passthrough-read setting.

`[-persistent-store <text>]` **- Persistent Store Name**

This parameter specifies persistent storage name. This can then be used for enabling the Persistent mode for Fpolicy events.

Examples

The following example displays the information about FPolicy policies on the cluster using the `vserver fpolicy policy show` command.

```
cluster1::> vserver fpolicy policy show
Vserver         Policy       Events     Engine         Is Mandatory
PrivAccess
--------------- -----------  ---------- -------------  ------------
----------
Cluster         cserver_pol  cserver_   cserver_eng    true          yes
                             evt
vs1.example.com p            r          n              true          no
vs1.example.com cserver_pol  cserver_   cserver_eng    true          yes
                             evt
vs2.example.com cserver_pol  cserver_   cserver_eng    true          yes
                             evt
4 entries were displayed.
```

The following example displays FPolicy policy name information about all Vserver FPolicy policies with the `-allow-privileged-access` parameter set to "yes".

```
cluster1::> vserver fpolicy policy show -fields policy-name -allow
-privileged-access yes
vserver         policy-name
--------------- -----------
Cluster         cserver_pol
vs1.example.com cserver_pol
vs2.example.com cserver_pol
3 entries were displayed.
```

vserver fpolicy policy event create

Create an event

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

Description

The `vserver fpolicy policy event create` command creates an FPolicy event. An event describes what to monitor. An event can contain protocol, file operations, filters, and volume operation event types. In the FPolicy configuration, an event is attached to an FPolicy policy. You can attach the same event to one or more policies.

> Three parameters have dependency rules: `-protocol` , `-files-operations` and `-filters` . The following combinations are supported:

- Both `-protocol` and `-file-operations`
- All of `-protocol` , `-file-operations` and `-filters`
- Specify none of three

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create an FPolicy event.

`-event-name <Event name>` - Event

This parameter specifies the name of the FPolicy event that you want to create. An event name can be up to 256 characters long. An event name value is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_" and ".".

`[-protocol <Protocol>]` - Protocol

This parameter specifies the protocol name for which the event will be created. By default, no protocol is selected. The value of this parameter must be one of the following:

- `_ cifs _` - This specifies that the event is for the CIFS protocol.
- `_ nfsv3_` - This specifies that the event is for the NFSv3 protocol.
- `_ nfsv4_` - This specifies that the event is for the NFSv4 protocol.

> If you specify `-protocol` , then you must also specify a valid value for the `-file -operations` parameter.

`[-file-operations <File Operation>,…]` - File Operations

This parameter specifies a list of file operations for the FPolicy event. The event will check the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. The list can include one or more of the following operations:

- `_close _` - File close operations.

- _create _ - File create operations.
- _create_dir _ - Directory create operations.
- _delete _ - File delete operations.
- _delete_dir _ - Directory delete operations.
- _getattr _ - Get attribute operations.
- _link _ - Link operations.
- _lookup _ - Lookup operations.
- _open _ - File open operations.
- _read _ - File read operations.
- _write _ - File write operations.
- _rename _ - File rename operations.
- _rename_dir _ - Directory rename operations.
- _setattr _ - Set attribute operations.
- _symlink _ - Symbolic link operations.

> If you specify `-file-operations` then you must specify a valid protocol in the `-protocol` parameter.

`[-filters <Filter>,…]` - Filters

This parameter specifies a list of filters of given file operation or operations for the protocol specified in the `-protocol` parameter. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:

- _ `monitor-ads` _ - Filter the client request for alternate data stream.
- _ `close-with-modification` _ - Filter the client request for close with modification.
- _ `close-without-modification`_ - Filter the client request for close without modification.
- _ `close-with-read` _ - Filter the client request for close with read.
- _ `first-read` _ - Filter the client requests for the first-read. When this filter is used for CIFS events, the first-read request within a CIFS session results in FPolicy processing. When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping -duration` configurations determine the first read-request for which FPolicy processing is done.
- _ `first-write` _ - Filter the client requests for the first-write. When this filter is used for CIFS events, the first-write request within a CIFS session results in FPolicy processing. When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io -grouping-duration` configurations determine the first-write request for which FPolicy processing is done.
- _ `offline-bit` _ - Filter the client request for offline bit set. Setting this filter, FPolicy server receives notification only when offline files are accessed.
- _ `open-with-delete-intent` _ - Filter the client request for open with delete intent. Setting this filter, FPolicy server receives notification only when an attempt is made to open a file with the intent to

delete it. This is used by file systems when the FILE_DELETE_ON_CLOSE flag is specified.

- _ `open-with-write-intent` _ - Filter the client request for open with write intent. Setting this filter, FPolicy server receives notification only when an attempt is made to open a file with the intent to write something in it.
- _ `write-with-size-change` _ - Filter the client request for write with size change.
- _ `setattr-with-owner-change` _ - Filter the client setattr requests for changing owner of a file or directory.
- _ `setattr-with-group-change` _ - Filter the client setattr requests for changing group of a file or directory.
- _ `setattr-with-sacl-change` _ - Filter the client setattr requests for changing sacl on a file or directory.
- _ `setattr-with-dacl-change` _ - Filter the client setattr requests for changing dacl on a file or directory.
- _ `setattr-with-modify-time-change` _ - Filter the client setattr requests for changing the modification time of a file or directory.
- _ `setattr-with-access-time-change` _ - Filter the client setattr requests for changing the access time of a file or directory.
- _ `setattr-with-creation-time-change` _ - Filter the client setattr requests for changing the creation time of a file or directory.
- _ `setattr-with-mode-change` _ - Filter the client setattr requests for changing the mode bits on a file or directory.
- _ `setattr-with-size-change` _ - Filter the client setattr requests for changing the size of a file.
- _ `setattr-with-allocation-size-change` _ - Filter the client setattr requests for changing the allocation size of a file.
- _ `exclude-directory` _ - Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.

> ⓘ If you specify a value for the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.

> ⓘ If the client sends multiple read/write requests simultaneously for the same file, then the first-read and first-write filters can result in more than one FPolicy notification.

`[-volume-operation {true|false}]` - Send Volume Operation Notifications

This parameter specifies whether volume operations generate notifications for the FPolicy event. If this field is set to *`true`* then FPolicy sends notifications when volumes are mounted or unmounted. By default, it is *`false`* .

`[-monitor-fileop-failure {true|false}]` - Send Failed File Operation Notifications

This parameter specifies whether failed file operations generate notifications for the FPolicy event. If field is set to *`true`* then FPolicy sends notifications when the file operations fail due to lack of permissions. By default, it is *`false`* .

Examples

The following example creates an FPolicy event.

```
cluster1::> vserver fpolicy policy event create -vserver vs1.example.com
-event-name cifs_event -protocol cifs
                                                            -file
-operations open,close,read,write -filters first-read,offline-bit
                                                            -volume
-operation true -monitor-fileop-failure false
cluster1::> vserver fpolicy policy event show -vserver vs1.example.com
-event-name cifs_event
Vserver: vs1.example.com
                                     Event Name: cifs_event
                                       Protocol: cifs
                                File Operations: open, close, read, write
                                        Filters: first-read, offline-bit
            Send Volume Operation Notifications: true
       Send Failed File Operation Notifications: false
```

The following is a list of supported `-file-operations` and `-filters` for the *`CIFS`* protocol.

```
     Supported |
          File |
    Operations | Supported Filters

==========================================================================
============

    close      : monitor-ads, close-with-modification, close-without-
modification,
                 offline-bit, close-with-read, exclude-directory
    create     : monitor-ads, offline-bit
    create_dir : none
    delete     : monitor-ads, offline-bit
    delete_dir : none
    getattr    : offline-bit, exclude-directory
    open       : monitor-ads, offline-bit, open-with-delete-intent, open-
with-write-intent,
                 exclude-directory
    read       : monitor-ads, first-read, offline-bit
    write      : monitor-ads, first-write, offline-bit, write-with-size-
change
    rename     : offline-bit, monitor-ads
    rename_dir : none
    setattr    : offline-bit, monitor-ads, setattr-with-owner-change,
                 setattr-with-group-change, setattr-with-sacl-change,
                 setattr-with-dacl-change, setattr-with-modify-time-
change,
                 setattr-with-access-time-change, setattr-with-creation-
time-change,
                 setattr-with-size-change, setattr-with-allocation-size-
change,
                 exclude-directory
```

The following is a list of supported `-file-operations` and `-filters` for the *`nfsv3`* protocol.

```
     Supported |
          File |
    Operations | Supported Filters

==========================================================================
============
     create     : offline-bit
     create_dir : none
     delete     : offline-bit
     delete_dir : none
     link       : offline-bit
     lookup     : offline-bit, exclude-directory
     read       : offline-bit, first-read
     write      : offline-bit, write-with-size-change, first-write
     rename     : offline-bit
     rename_dir : none
     setattr    : offline-bit, setattr-with-owner-change, setattr-with-
group-change,
                  setattr-with-modify-time-change, setattr-with-access-
time-change,
                  setattr-with-mode-change, setattr-with-size-change,
exclude-directory
     symlink    : offline-bit
```

The following is a list of supported `-file-operations` and `-filters` for the *`nfsv4`* protocol.

```
     Supported |
          File |
    Operations | Supported Filters

==========================================================================
============
     close      : offline-bit, exclude-directory
     create     : offline-bit
     create_dir : none
     delete     : offline-bit
     delete_dir : none
     getattr    : offline-bit, exclude-directory
     link       : offline-bit
     lookup     : offline-bit, exclude-directory
     open       : offline-bit, exclude-directory
     read       : offline-bit, first-read
     write      : offline-bit, write-with-size-change, first-write
     rename     : offline-bit
     rename_dir : none
     setattr    : offline-bit, setattr-with-owner-change, setattr-with-
group-change,
                  setattr-with-sacl-change, setattr-with-dacl-change,
                  setattr-with-modify-time-change, setattr-with-access-
time-change,
                  setattr-with-size-change, exclude-directory
     symlink    : offline-bit
```

The following is a list of supported `-file-operations` for supported protocol when `-monitor-fileop -failure` is set to true.

```
    Protocol  | Supported File Operations

==========================================================================
===============
     cifs     : open
     nfsv3    : create, create_dir, read, write, delete, delete_dir,
rename, rename_dir,
                setattr, link
     nfsv4    : open, create, create_dir, read, write, delete, delete_dir,
rename, rename_dir,
                setattr, link
```

vserver fpolicy policy event delete

Delete an event

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

Description

The `vserver fpolicy policy event delete` command deletes an FPolicy event.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the Vserver from which you want to delete an FPolicy event.

`-event-name <Event name>` - Event

This parameter specifies the name of the FPolicy event you want to delete.

Examples

The following example deletes an FPolicy event.

```
cluster1::> vserver fpolicy policy event delete  -vserver vs1.example.com
-event-name cifs_event
```

vserver fpolicy policy event modify

Modify an event

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

Description

The `vserver fpolicy policy event modify` command modifies an FPolicy event. An event describes what to monitor. An event can contain protocol, file operations, filters, and volume operation event types. In the FPolicy configuration, an event is attached to an FPolicy policy. You can attach the same event to one or more policies. You can modify an event while it is attached to an FPolicy policy. Any changes to the event take effect immediately.

> ⓘ Three parameters have dependency rules: `-protocol` , `-files-operations` and `-filters` . The following combinations are supported:

- Both `-protocol` and `-file-operations`
- All of `-protocol` , `-file-operations` and `-filters`
- Specify none of three

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy event.

`-event-name <Event name>` - Event

This parameter specifies the name of the FPolicy event that you want to modify. An event name can be up to 256 characters long. An event name value is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_" and "." .

`[-protocol <Protocol>]` - Protocol

This parameter specifies the protocol name for which the event will be modified. By default, no protocol is selected. The value of this parameter must be one of the following:

- _ `cifs` _ - This specifies that the event is for the CIFS protocol.
- _ `nfsv3`_ - This specifies that the event is for the NFSv3 protocol.
- _ `nfsv4`_ - This specifies that the event is for the NFSv4 protocol.

> If you specify `-protocol` , then you must also specify a valid value for the `-file -operations` parameter.

`[-file-operations <File Operation>,…]` - File Operations

This parameter specifies a list of file operations for the FPolicy event. The event will check the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. The list can include one or more of the following operations:

- _ `close` _ - File close operations.
- _ `create` _ - File create operations.
- _ `create_dir`_ - Directory create operations.
- _ `delete` _ - File delete operations.
- _ `delete_dir`_ - Directory delete operations.
- _ `getattr` _ - Get attribute operations.
- _ `link` _ - Link operations.
- _ `lookup` _ - Lookup operations.
- _ `open` _ - File open operations.
- _ `read` _ - File read operations.
- _ `write` _ - File write operations.
- _ `rename` _ - File rename operations.
- _ `rename_dir`_ - Directory rename operations.
- _ `setattr` _ - Set attribute operations.
- _ `symlink` _ - Symbolic link operations.

> If you specify `-file-operations` then you must specify a valid protocol in the `-protocol` parameter.

`[-filters <Filter>,…]` - Filters

This parameter specifies a list of filters of given file operation or operations for the protocol specified in the `-protocol` parameter. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:

- _ `monitor-ads` _ - Filter the client request for alternate data stream.
- _ `close-with-modification` _ - Filter the client request for close with modification.
- _ `close-without-modification`_ - Filter the client request for close without modification.
- _ `close-with-read` _ - Filter the client request for close with read.
- _ `first-read` _ - Filter the client requests for the first-read. When this filter is used for CIFS events, the first-read request within a CIFS session results in FPolicy processing. When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping -duration` configurations determine the first read-request for which FPolicy processing is done.
- _ `first-write` _ - Filter the client requests for the first-write. When this filter is used for CIFS events, the first-write request within a CIFS session results in FPolicy processing. When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io -grouping-duration` configurations determine the first-write request for which FPolicy processing is done.
- _ `offline-bit` _ - Filter the client request for offline bit set. Setting this filter, FPolicy server receives notification only when offline files are accessed.
- _ `open-with-delete-intent` _ - Filter the client request for open with delete intent. Setting this filter, FPolicy server receives notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the FILE_DELETE_ON_CLOSE flag is specified.
- _ `open-with-write-intent` _ - Filter the client request for open with write intent. Setting this filter, FPolicy server receives notification only when an attempt is made to open a file with the intent to write something in it.
- _ `write-with-size-change` _ - Filter the client request for write with size change.
- _ `setattr-with-owner-change` _ - Filter the client setattr requests for changing owner of a file or directory.
- _ `setattr-with-group-change` _ - Filter the client setattr requests for changing group of a file or directory.
- _ `setattr-with-sacl-change` _ - Filter the client setattr requests for changing sacl on a file or directory.
- _ `setattr-with-dacl-change` _ - Filter the client setattr requests for changing dacl on a file or directory.
- _ `setattr-with-modify-time-change` _ - Filter the client setattr requests for changing the modification time of a file or directory.
- _ `setattr-with-access-time-change` _ - Filter the client setattr requests for changing the access time of a file or directory.
- _ `setattr-with-creation-time-change` _ - Filter the client setattr requests for changing the

creation time of a file or directory.

- _ `setattr-with-mode-change` _ - Filter the client setattr requests for changing the mode bits on a file or directory.
- _ `setattr-with-size-change` _ - Filter the client setattr requests for changing the size of a file.
- _ `setattr-with-allocation-size-change` _ - Filter the client setattr requests for changing the allocation size of a file.
- _ `exclude-directory` _ - Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.

> ⓘ If you specify a value for the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.

> ⓘ If the client sends multiple read/write requests simultaneously for the same file, then the first-read and first-write filters can result in more than one FPolicy notification.

`[-volume-operation {true|false}]` - Send Volume Operation Notifications

This parameter specifies whether volume operations generate notifications for the FPolicy event. If this field is set to *`true`* then FPolicy sends notifications when volumes are mounted or unmounted. By default, it is *`false`* .

`[-monitor-fileop-failure {true|false}]` - Send Failed File Operation Notifications

This parameter specifies whether failed file operation generate notifications for the FPolicy event. If field is set to *`true`* then FPolicy sends notifications when the file operations fail due to lack of permissions. By default, it is *`false`* .

Examples

The following example modifies an FPolicy event.

```
cluster1::> vserver fpolicy policy event modify -vserver vs1.example.com
-event-name cifs_event -protocol cifs
                                                            -file
-operations open,close,read,write -filters first-read,offline-bit
                                                            -volume
-operation true -monitor-fileop-failure false
cluster1::> vserver fpolicy policy event show -vserver vs1.example.com
-event-name cifs_event
Vserver: vs1.example.com
                                     Event Name: cifs_event
                                       Protocol: cifs
                                File Operations: open, close, read, write
                                        Filters: first-read, offline-bit
            Send Volume Operation Notifications: true
       Send Failed File Operation Notifications: false
```

The following is a list of supported `-file-operations` and `-filters` for the *`CIFS`* protocol.

```
     Supported |
          File |
    Operations | Supported Filters

==========================================================================
============

    close      : monitor-ads, close-with-modification, close-without-
modification,
                 offline-bit, close-with-read, exclude-directory
    create     : monitor-ads, offline-bit
    create_dir : none
    delete     : monitor-ads, offline-bit
    delete_dir : none
    getattr    : offline-bit, exclude-directory
    open       : monitor-ads, offline-bit, open-with-delete-intent, open-
with-write-intent,
                 exclude-directory
    read       : monitor-ads, first-read, offline-bit
    write      : monitor-ads, first-write, offline-bit, write-with-size-
change
    rename     : offline-bit, monitor-ads
    rename_dir : none
    setattr    : offline-bit, monitor-ads, setattr-with-owner-change,
                 setattr-with-group-change, setattr-with-sacl-change,
                 setattr-with-dacl-change, setattr-with-modify-time-
change,
                 setattr-with-access-time-change, setattr-with-creation-
time-change,
                 setattr-with-size-change, setattr-with-allocation-size-
change,
                 exclude-directory
```

The following is a list of supported `-file-operations` and `-filters` for the *`nfsv3`* protocol.

```
     Supported |
          File |
    Operations | Supported Filters

==========================================================================
============
     create     : offline-bit
     create_dir : none
     delete     : offline-bit
     delete_dir : none
     link       : offline-bit
     lookup     : offline-bit, exclude-directory
     read       : offline-bit, first-read
     write      : offline-bit, write-with-size-change, first-write
     rename     : offline-bit
     rename_dir : none
     setattr    : offline-bit, setattr-with-owner-change, setattr-with-
group-change,
                  setattr-with-modify-time-change, setattr-with-access-
time-change,
                  setattr-with-mode-change, setattr-with-size-change,
exclude-directory
     symlink    : offline-bit
```

The following is a list of supported `-file-operations` and `-filters` for the *`nfsv4`* protocol.

```
     Supported |
          File |
    Operations | Supported Filters

==========================================================================
============
     close      : offline-bit, exclude-directory
     create     : offline-bit
     create_dir : none
     delete     : offline-bit
     delete_dir : none
     getattr    : offline-bit, exclude-directory
     link       : offline-bit
     lookup     : offline-bit, exclude-directory
     open       : offline-bit, exclude-directory
     read       : offline-bit, first-read
     write      : offline-bit, write-with-size-change, first-write
     rename     : offline-bit
     rename_dir : none
     setattr    : offline-bit, setattr-with-owner-change, setattr-with-
group-change,
                  setattr-with-sacl-change, setattr-with-dacl-change,
                  setattr-with-modify-time-change, setattr-with-access-
time-change,
                  setattr-with-size-change, exclude-directory
     symlink    : offline-bit
```

The following is a list of supported `-file-operations` for supported protocol when `-monitor-fileop -failure` is set to true.

```
    Protocol  | Supported File Operations

==========================================================================
===============
     cifs     : open
     nfsv3    : create, create_dir, read, write, delete, delete_dir,
rename, rename_dir,
                setattr, link
     nfsv4    : open, create, create_dir, read, write, delete, delete_dir,
rename, rename_dir,
                setattr, link
```

vserver fpolicy policy event show

Display events

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

Description

The `vserver fpolicy policy event show` command displays information about all FPolicy events belonging to the Vserver. Any Vserver administrator can see FPolicy events associated with their Vserver as well as FPolicy events created by the cluster administrator. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy events:

- Vserver name
- FPolicy event name
- Protocol name
- List of file operations
- List of filters
- Volume operation
- Monitor failed file operation

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy events. You can specify additional parameters to display only information that matches those parameters. For example, to display information only about all CIFS events configured with the `-volume-operation` field set, run the command with the `-fields` parameter set to `-event-name` event-name `-protocol` *`cifs`*`-volume -operation` *`yes`* .

You can specify the `-instance` parameter to display all information for all policies in a list format.

Parameters

{ `[-fields <fieldname>,…]`

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| `[-instance ]` }

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

`[-vserver <Vserver Name>]` - Vserver

If you specify this parameter, the command displays information only about the FPolicy events for the specified Vserver. Events created on the admin Vserver by the cluster administrator are visible in all Vservers.

`[-event-name <Event name>]` - Event

If you specify this parameter, the command displays information only about the FPolicy event that matches the specified event name.

`[-protocol <Protocol>]` - Protocol

If you specify this parameter, the command displays information only about the FPolicy event or events that use the specified protocol.

`[-file-operations <File Operation>,…]` - File Operations

If you specify this parameter, the command displays information only about the FPolicy event or events that use the specified file operation or operations.

`[-filters <Filter>,…]` - Filters

If you specify this parameter, the command displays information only about the FPolicy event or events that use the specified filter or filters.

`[-volume-operation {true|false}]` - Send Volume Operation Notifications

If this field is set to *`true`* , then FPolicy displays information about those events for which it sends notifications when volumes are mounted or unmounted. If you set this parameter to *`true`* , the command displays information about events where the `-volume-operation` parameter is set *`true`* and volume operations such as mount and unmount are monitored. If you set this parameter to *`false`* , the command displays information about events where volume operations are not monitored.

`[-monitor-fileop-failure {true|false}]` - Send Failed File Operation Notifications

If you specify this parameter, the command displays information only about the FPolicy event or events that has `-monitor-fileop-failure` parameter set to the specified value.

Examples

The following example displays the information about all Vserver FPolicy policy events.

```
cluster1::> vserver fpolicy policy event show
                                Event                        File
Volume
                Vserver         Name               Protocols Operations
Filters      Operation
                --------------- ------------------ --------- -------------
------------ ------------
                Cluster         cserver_evt        cifs      open, close,
first-write, true
                                                             read, write
first-read
                vs1.example.com cserver_evt        cifs      open, close,
first-write, true
                                                             read, write
first-read
                vs1.example.com v1e1               cifs      open, read
first-read   -
                vs1.example.com v1e2               cifs      open
-            false
                vs1.example.com v1e3               nfsv4     open
-            true
                vs2.example.com cserver_evt        cifs      open, close,
first-write, true
                                                             read, write
first-read
                6 entries were displayed.
```

The following example displays event name information about all Vserver FPolicy policy events with CIFS as a protocol and with false as volume operation.

```
cluster1::> vserver fpolicy policy event show -fields event-name -protocol
cifs -volume-operation false
               vserver         event-name
               --------------- ----------
               vs1.example.com v1e2
```

vserver fpolicy policy external-engine create

Create an external engine

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

Description

The `vserver fpolicy policy external-engine create` command creates an FPolicy external engine. The cluster uses the external engine to hold configuration information that it needs in order to send notification information to the FPolicy servers. It specifies the primary servers and secondary servers to which the cluster will send notifications. It also specifies FPolicy server related configuration information.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create an FPolicy external engine.

`-engine-name <Engine name>` - Engine

This parameter specifies the name of the FPolicy external engine that you want to create. An external engine name can be up to 256 characters long. An external engine name is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_", and "." .

`-primary-servers <IP Address>,…` - Primary FPolicy Servers

This parameter specifies a list of IP addresses for the primary FPolicy servers to which you want the external engine you create to apply. The `-primary-servers` parameter is used to specify a list of servers to which to send file access events for a given FPolicy policy. When an administrator configures multiple servers as primary servers, notifications are sent to the FPolicy servers in a round-robin fashion.

`-port <integer>` - Port Number of FPolicy Service

This parameter specifies the port number for the FPolicy service.

`[-secondary-servers <IP Address>,…]` - Secondary FPolicy Servers

This parameter specifies a list of IP addresses for the secondary FPolicy servers to which you want the external engine you create to apply. Secondary servers will be used only when all the primary servers are not reachable. When an administrator configures multiple servers as secondary servers, notifications are sent to FPolicy server in a round-robin fashion. By default, no secondary server is selected.

`[-extern-engine-type <External Engine Type>]` - External Engine Type

This parameter specifies the type of the external engine. This specifies how the FPolicy server should behave, synchronously or asynchronously. By default, it is *`synchronous`* in nature. When set to *`synchronous`* , after sending a notification to the external FPolicy server, request processing does not continue until after receiving a response from the FPolicy server. At that point request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action. When set to *`asynchronous`* , after sending a notification to the external FPolicy server, file request processing continues.

`-ssl-option {no-auth|server-auth|mutual-auth}` - SSL Option for External Communication

This parameter specifies the SSL option for external communication with the FPolicy server. Possible values include the following:

- no-auth : When set to no-auth, no authentication takes place. The communication link is established over the TCP protocol.
- server-auth : When set to server-auth, only the FPolicy server is authenticated by the Vserver. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.
- mutual-auth : When set to mutual-auth, mutual authentication takes place between the Vserver and the

FPolicy server, i.e. authentication of the FPolicy server by the Vserver along with authentication of the Vserver by the FPolicy server. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate along with the public certificate and key file for authentication of the Vserver.

The public certificate of certificate authority (CA) that is used to sign the FPolicy server certificate is installed using the security certificate install command with `-type` set to *`client_ca`* . The private key and public certificate required for authentication of the Vserver is installed using the security certificate install command with `-type` set to *`server`* .

`[-reqs-cancel-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Canceling a Request (privilege: advanced)

This parameter specifies the timeout for canceling a request. It is used to specify the time interval in which the node waits for a response from the FPolicy server. Beyond this timeout, a cancel request is sent to the FPolicy server to cancel the pending request. The request is then sent to an alternate FPolicy server that is registered for the policy. This timeout helps in handling a FPolicy server that is not responding, which can improve CIFS/NFS client response. Also, this feature can help in releasing of system resources since the request is moved from a down/bad FPolicy server to an alternate FPolicy server. The value for this field must be between 0s and 100s. By default, it is 20s.

`[-reqs-abort-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Aborting a Request (privilege: advanced)

This parameter specifies the timeout for aborting a request. The value for this field must be between 0s and 200s. By default, it is 40s.

`[-status-req-interval <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Interval for Sending Status Requests (privilege: advanced)

This parameter specifies the interval for sending status requests. It is used to specify the interval after which a status request will be send to the FPolicy server. The value for this field must be between 0s and 50s. By default, it is 10s.

`[-max-connection-retries <integer>]` - Max Reconnect Attempt (privilege: advanced)

This parameter specifies the maximum number of attempts to reconnect to the FPolicy server from a Vserver. It is used to specify the number of times a broken connection will be retried. The value for this field must be between 0 and 20. By default, it is 5.

`[-max-server-reqs <integer>]` - Maximum Outstanding Requests for FPolicy Server (privilege: advanced)

This parameter specifies the maximum number of outstanding requests for the FPolicy server. It is used to specify maximum outstanding requests that will be queued up for the FPolicy server. The value for this field must be between 1 and 10000. The default values are 500, 1000 or 2000 for Low-end(< 64 GB memory), Mid-end(>=64 GB memory) and High-end(>=128 GB memory) Platforms respectively.

`[-server-progress-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Disconnecting Non-responsive Server (privilege: advanced)

This parameter specifies the timeout for disconnecting non-responsive FPolicy servers. It is used to specify the time interval after which the connection to the FPolicy server is terminated. This happens only when the FPolicy server's queue contains the maximum allowed number of requests that it can hold in its queue and no response is received within this timeout. The maximum allowed number of requests is either 50 (the default) or the number specified by the `-max-server-reqs` parameter. The value for this field must be between 1s and 100s. By default, it is 60s.

`[-keep-alive-interval <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Interval for Sending Keep-Alive Messages (privilege: advanced)

This parameter specifies the interval in hours (h), minutes (m), or seconds (s) at which keep-alive messages are sent to the FPolicy server. Keep-alive messages are used to detect half-open connections. The range of supported values for this field is 10 through 600 (h, m, or s). Alternatively, the value can be set to 0, which disables keep-alive messages and prevents them from being sent to the FPolicy servers. The default value for this field is 120s.

`[-certificate-common-name <FQDN or Custom Common Name>]` - FQDN or Custom Common Name

This parameter specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the Vserver and the FPolicy server is configured.

`[-certificate-serial <text>]` - Serial Number of Certificate

This parameter specifies the serial number of the certificate used for authentication if SSL authentication between the Vserver and the FPolicy server is configured.

`[-certificate-ca <text>]` - Certificate Authority

This parameter specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the Vserver and the FPolicy server is configured.

`[-recv-buffer-size <integer>]` - Receive Buffer Size (privilege: advanced)

This parameter specifies the receive buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the receive buffer is set to a value defined by the system. For example, if the default receive buffer size of the socket is 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the receive buffer.

`[-send-buffer-size <integer>]` - Send Buffer Size (privilege: advanced)

This parameter specifies the send buffer size of the connected socket for the FPolicy server. The default value is set to 1 Mb. When the value is set to 0, the size of the send buffer is set to a value defined by the system. For example, if the default send buffer size of the socket is set to 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the send buffer.

`[-session-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Session ID Purge Timeout During Reconnection (privilege: advanced)

This parameter specifies the interval after which a new session ID is sent to the FPolicy server during reconnection attempts. The value for this field must be between 0s and 200s. The default value is set to 10 seconds. If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the `-session-timeout` interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications.

`[-is-resiliency-enabled {true|false}]` - Is Resiliency Feature Enabled

This parameter specifies whether the resiliency feature is enabled. When this parameter is set to *`true`* and all the primary and secondary servers are down, or no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified `-resiliency-directory -path` . To deny the file access events from being stored under these circumstances, set this parameter to *`false`* . By default, it is *`false`* .

`[-resiliency-max-retention-duration <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Maximum Notification Retention Duration

This parameter specifies the duration for which the notifications are written to files inside the storage controller during network outage. The value for this field must be between 0s and 600s. By default, it is set to 180s.

`[-resiliency-directory-path <text>]` - Directory for Notification Storage

This parameter specifies the directory path under the `-vserver` namespace, where notifications are stored in the files whenever network outage happens.

`[-extern-engine-format {xml|protobuf}]` - External Engine Format

This parameter specifies the format of the Fpolicy notification messages sent to the external engine. Valid values: *`xml`* or *`protobuf`* . Default value for this parameter is *`xml`* . When set to *`protobuf`* , the notification messages are encoded in binary form using Google Protobuf. Before setting this to *`protobuf`* , ensure that the Fpolicy server also supports Protobuf deserialization.

Examples

The following example creates an FPolicy external engine.

```
cluster1::> vserver fpolicy policy external-engine create -vserver
vs1.example.com -engine-name new_engine -primary-servers 1.1.1.1 -port 10
-secondary-servers 2.2.2.2 -ssl-option mutual-auth -extern-engine-type
synchronous -extern-engine-format xml -certificate-serial 8DDE112A114D1FBC
-certificate-common-name Sample1-FPolicy-Client -certificate-ca TASample1

cluster1::> vserver fpolicy policy external-engine show -vserver
vs1.example.com -engine-name new_engine
Vserver: vs1.example.com
                               Engine: new_engine
               Primary FPolicy Servers: 1.1.1.1
        Port Number of FPolicy Service: 10
             Secondary FPolicy Servers: 2.2.2.2
                  External Engine Type: synchronous
                External Engine Format: xml
SSL Option for External Communication: mutual-auth
           FQDN or Custom Common Name: Sample1-FPolicy-Client
                        Serial Number: 8DDE112A114D1FBC
                Certificate Authority: TASample1
```

Related Links

- security certificate install

vserver fpolicy policy external-engine delete

Delete an external engine

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

Description

The `vserver fpolicy policy external-engine delete` command deletes an FPolicy external engine.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the Vserver from which you want to delete an FPolicy external engine.

`-engine-name <Engine name>` - Engine

This parameter specifies the name of the FPolicy external engine you want to delete.

Examples

The following example deletes an FPolicy external engine.

```
cluster1::> vserver fpolicy policy external-engine show -vserver
vs1.example.com -engine-name new_engine
Vserver: vs1.example.com
                               Engine: new_engine
               Primary FPolicy Servers: 1.1.1.1
        Port Number of FPolicy Service: 10
             Secondary FPolicy Servers: 2.2.2.2
                  External Engine Type: synchronous
SSL Option for External Communication: mutual-auth
            FQDN or Custom Common Name: Sample1-FPolicy-Client
                         Serial Number: 8DDE112A114D1FBC
                 Certificate Authority: TASample1

cluster1::> vserver fpolicy policy external-engine delete -vserver
vs1.example.com -engine-name new_engine
```

vserver fpolicy policy external-engine modify

Modify an external engine

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

Description

The `vserver fpolicy policy external-engine modify` command modifies an FPolicy external engine. The cluster uses the external engine to hold configuration information that it needs in order to send notification information to the FPolicy servers. It specifies the primary servers and secondary servers to which the cluster will send notifications. It also specifies FPolicy server related configuration information.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy external engine.

`-engine-name <Engine name>` - Engine

This parameter specifies the name of the FPolicy external engine that you want to modify. An external engine name can be up to 256 characters long. An external engine name is a string that can only contain any combination of ASCII-range alphanumeric characters (a-z, A-Z, 0-9), "_", and "." .

`[-primary-servers <IP Address>,…]` - Primary FPolicy Servers

This parameter specifies a list of IP addresses for the primary FPolicy servers to which you want the external engine you modify to apply. The `-primary-servers` parameter is used to specify a list of servers to which to send file access events for a given FPolicy policy. When an administrator configures multiple servers as primary servers, notifications are sent to the FPolicy servers in a round-robin fashion.

`[-port <integer>]` - Port Number of FPolicy Service

This parameter specifies the port number for the FPolicy service.

`[-secondary-servers <IP Address>,…]` - Secondary FPolicy Servers

This parameter specifies a list of IP addresses for the secondary FPolicy servers to which you want the external engine you modify to apply. Secondary servers will be used only when all the primary servers are not reachable. When an administrator configures multiple servers as secondary servers, notifications are sent to FPolicy server in a round-robin fashion. By default, no secondary server is selected.

`[-extern-engine-type <External Engine Type>]` - External Engine Type

This parameter specifies the type of the external engine. This specifies how the FPolicy server should behave, synchronously or asynchronously. By default, it is synchronous in nature. When set to synchronous, after sending a notification to the external FPolicy server, request processing does not continue until after receiving a response from the FPolicy server. At that point request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action. When set to asynchronous, after sending a notification to the external FPolicy server, file request processing continues.

`[-ssl-option {no-auth|server-auth|mutual-auth}]` - SSL Option for External Communication

This parameter specifies the SSL option for external communication with the FPolicy server. Possible values include the following:

- no-auth : When set to no-auth, no authentication takes place. The communication link is established over the TCP protocol.
- server-auth : When set to server-auth, only the FPolicy server is authenticated by the Vserver. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.
- mutual-auth : When set to mutual-auth, mutual authentication takes place between the Vserver and the

FPolicy server, i.e. authentication of the FPolicy server by the Vserver along with authentication of the Vserver by the FPolicy server. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate along with the public certificate and key file for authentication of the Vserver.

The public certificate of certificate authority (CA) that is used to sign the FPolicy server certificate is installed using the security certificate install command with `-type` set to *`client_ca`* . The private key and public certificate required for authentication of the Vserver is installed using the security certificate install command with `-type` set to *`server`* .

`[-reqs-cancel-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Canceling a Request (privilege: advanced)

This parameter specifies the timeout for canceling a request. It is used to specify the time interval in which the node waits for a response from the FPolicy server. Beyond this timeout, a cancel request is sent to the FPolicy server to cancel the pending request. The request is then sent to an alternate FPolicy server that is registered for the policy. This timeout helps in handling a FPolicy server that is not responding, which can improve CIFS/NFS client response. Also, this feature can help in releasing of system resources since the request is moved from a down/bad FPolicy server to an alternate FPolicy server. The value for this field must be between 0s and 100s. By default, it is 20s.

`[-reqs-abort-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Aborting a Request (privilege: advanced)

This parameter specifies the timeout for aborting a request. The value for this field must be between 0s and 200s. By default, it is 40s.

`[-status-req-interval <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Interval for Sending Status Requests (privilege: advanced)

This parameter specifies the interval for sending status requests. It is used to specify the interval after which a status request will be send to the FPolicy server. The value for this field must be between 0s and 50s. By default, it is 10s.

`[-max-connection-retries <integer>]` - Max Reconnect Attempt (privilege: advanced)

This parameter specifies the maximum number of attempts to reconnect to the FPolicy server from a Vserver. It is used to specify the number of times a broken connection will be retried. The value for this field must be between 0 and 20. By default, it is 5.

`[-max-server-reqs <integer>]` - Maximum Outstanding Requests for FPolicy Server (privilege: advanced)

This parameter specifies the maximum number of outstanding requests for the FPolicy server. It is used to specify the maximum outstanding requests that will be queued up for the FPolicy server. The value for this field must be between 1 and 10000. The default values are 500, 1000 or 2000 for Low-end(< 64 GB memory), Mid-end(>=64 GB memory) and High-end(>=128 GB memory) Platforms respectively.

`[-server-progress-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Disconnecting Non-responsive Server (privilege: advanced)

This parameter specifies the timeout for disconnecting non-responsive FPolicy servers. It is used to specify the time interval after which the connection to the FPolicy server is terminated. This happens only when the FPolicy server's queue contains the maximum allowed number of requests that it can hold in its queue and no response is received within this timeout. The maximum allowed number of requests is either 50 (the default) or the number specified by the `-max-server-reqs` parameter. The value for this field must be between 1s and 100s. By default, it is 60s.

`[-keep-alive-interval <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Interval for Sending Keep-Alive Messages (privilege: advanced)

This parameter specifies the interval in hours (h), minutes (m), or seconds (s) at which keep-alive messages are sent to the FPolicy server. Keep-alive messages are used to detect half-open connections. The range of supported values for this field is 10 through 600 (h, m, or s). Alternatively, the value can be set to 0, which disables keep-alive messages and prevents them from being sent to the FPolicy servers. The default value for this field is 120s.

`[-certificate-common-name <FQDN or Custom Common Name>]` - FQDN or Custom Common Name

This parameter specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the Vserver and the FPolicy server is configured.

`[-certificate-serial <text>]` - Serial Number of Certificate

This parameter specifies the serial number of the certificate used for authentication if SSL authentication between the Vserver and the FPolicy server is configured.

`[-certificate-ca <text>]` - Certificate Authority

This parameter specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the Vserver and the FPolicy server is configured.

`[-recv-buffer-size <integer>]` - Receive Buffer Size (privilege: advanced)

This parameter specifies the receive buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the receive buffer is set to a value defined by the system. For example, if the default receive buffer size of the socket is 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the receive buffer.

`[-send-buffer-size <integer>]` - Send Buffer Size (privilege: advanced)

This parameter specifies the send buffer size of the connected socket for the FPolicy server. The default value is set to 1 Mb. When the value is set to 0, the size of the send buffer is set to a value defined by the system. For example, if the default send buffer size of the socket is set to 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the send buffer.

`[-session-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Session ID Purge Timeout During Reconnection (privilege: advanced)

This parameter specifies the interval after which a new session ID is sent to the FPolicy server during reconnection attempts. The value for this field must be between 0s and 200s. The default value is set to 10 seconds. If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the `-session-timeout` interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications.

`[-is-resiliency-enabled {true|false}]` - Is Resiliency Feature Enabled

This parameter specifies whether the resiliency feature is enabled. When this parameter is set to *`true`* and all the primary and secondary servers are down, or no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified `-resiliency-directory -path` . To deny the file access events from being stored under these circumstances, set this parameter to *`false`* . By default, it is *`false`* .

[-resiliency-max-retention-duration <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Maximum Notification Retention Duration

This parameter specifies the duration for which the notifications are written to files inside the storage controller during network outage. The value for this field must be between 0s and 600s. By default, it is set to 180s.

[-resiliency-directory-path <text>] - Directory for Notification Storage

This parameter specifies the directory path under the `-vserver` namespace, where notifications are stored in the files whenever network outage happens.

[-extern-engine-format {xml|protobuf}] - External Engine Format

This parameter specifies the format of the Fpolicy notification messages sent to the external engine. Valid values: *xml* or *protobuf* . Default value for this parameter is *xml* . When set to *protobuf* , the notification messages are encoded in binary form using Google Protobuf. Before setting this to *protobuf* , ensure that the Fpolicy server also supports Protobuf deserialization.

Examples

The following example modifies an FPolicy external engine.

```
cluster1::> vserver fpolicy policy external-engine modify -vserver
vs1.example.com -engine-name new_engine -primary-servers 1.1.1.1 -port 10
-secondary-servers 2.2.2.2

cluster1::> vserver fpolicy policy external-engine show -vserver
vs1.example.com -engine-name new_engine
Vserver: vs1.example.com
                               Engine: new_engine
               Primary FPolicy Servers: 1.1.1.1
        Port Number of FPolicy Service: 10
             Secondary FPolicy Servers: 2.2.2.2
                  External Engine Type: synchronous
                External Engine Format: xml
SSL Option for External Communication: mutual-auth
           FQDN or Custom Common Name: Sample1-FPolicy-Client
                         Serial Number: 8DDE112A114D1FBC
                 Certificate Authority: TASample1
```

The following example shows how to modify `-recv-buffer-size` and `-send-buffer-size` to a non-default value of 0.

```
cluster1::*> vserver fpolicy policy external-engine modify -vserver
vs1.example.com -engine-name new_engine -recv-buffer-size 0 -send-buffer
-size 0
```

Related Links

- security certificate install

vserver fpolicy policy external-engine show

Display external engines

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

Description

The `vserver fpolicy policy external-engine show` command displays information about all FPolicy external engines belonging to the Vserver. Any Vserver administrator can see FPolicy external engines associated to their Vserver as well as external engines created by cluster administrator. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy external engines:

- Vserver name
- FPolicy external engine name
- List of primary FPolicy servers
- List of secondary FPolicy servers
- Port number for FPolicy service
- FPolicy external engine type
- FPolicy external engine format

You can specify the `-fields` parameter to specify which fields of information to display about FPolicy external engines. You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about all external engines where the `-port` parameter is set to *9* , run the command with the `-field` parameter set to engine-name and `-port` parameter set to *9* .

You can specify the `-instance` parameter to display all information for all policies in a list format.

Parameters

{ [-fields <fieldname>,…]

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| [-instance] }

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

[-vserver <Vserver Name>] - Vserver

If you specify this parameter, the command displays information only about the FPolicy external engines for the specified Vserver. FPolicy external engines that the cluster administrator creates are visible in all Vservers.

[-engine-name <Engine name>] - Engine

If you specify this parameter, the command displays information only about the FPolicy external engine that you specify.

`[-primary-servers <IP Address>,…]` - Primary FPolicy Servers

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified IP addresses as primary FPolicy servers.

`[-port <integer>]` - Port Number of FPolicy Service

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified port for the FPolicy service.

`[-secondary-servers <IP Address>,…]` - Secondary FPolicy Servers

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified IP addresses as secondary FPolicy servers.

`[-extern-engine-type <External Engine Type>]` - External Engine Type

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified external engine type.

`[-ssl-option {no-auth|server-auth|mutual-auth}]` - SSL Option for External Communication

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified SSL option.

`[-reqs-cancel-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Canceling a Request (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified timeout for canceling a request.

`[-reqs-abort-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Aborting a Request (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified timeout for aborting a request.

`[-status-req-interval <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Interval for Sending Status Requests (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified interval for sending status requests.

`[-max-connection-retries <integer>]` - Max Reconnect Attempt (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified maximum reconnect attempts.

`[-max-server-reqs <integer>]` - Maximum Outstanding Requests for FPolicy Server (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified FPolicy server maximum outstanding requests.

`[-server-progress-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Timeout for Disconnecting Non-responsive Server (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified timeout for disconnecting non-responsive server.

`[-keep-alive-interval <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Interval for Sending Keep-Alive Messages (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified keep-alive interval.

`[-certificate-common-name <FQDN or Custom Common Name>]` - FQDN or Custom Common Name

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified certificate common name.

`[-certificate-serial <text>]` - Serial Number of Certificate

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified certificate serial number.

`[-certificate-ca <text>]` - Certificate Authority

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified certificate authority name.

`[-recv-buffer-size <integer>]` - Receive Buffer Size (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified receive buffer size.

`[-send-buffer-size <integer>]` - Send Buffer Size (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified send buffer size.

`[-session-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Session ID Purge Timeout During Reconnection (privilege: advanced)

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified session timeout.

`[-is-resiliency-enabled {true|false}]` - Is Resiliency Feature Enabled

If you specify this parameter set to *`true`* , the command displays information only about the FPolicy external engine or engines that has the resiliency feature enabled.

`[-resiliency-max-retention-duration <[<integer>d][<integer>h][<integer>m][<integer>s]>]` - Maximum Notification Retention Duration

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified network outage duration.

`[-resiliency-directory-path <text>]` - Directory for Notification Storage

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified directory path.

`[-extern-engine-format {xml|protobuf}]` - External Engine Format

If you specify this parameter, the command displays information only about the FPolicy external engine or engines that use the specified engine format.

Examples

The following example displays the information about the configured external engines using the `vserver fpolicy policy external-engine show` command.

```
cluster1::> vserver fpolicy policy external-engine show
                              Primary           Secondary        External
External
 Vserver         Engine       Servers           Servers    Port  Engine
Type Engine Format
 --------------- -----------  ----------------- ---------- -----
----------- ------------
 Cluster         cserver_eng  9.9.9.9           -              9
synchronous xml
 vs1.example.com cserver_eng  9.9.9.9           -              9
synchronous protobuf
 vs1.example.com v1n1         1.1.1.1           2.2.2.2        1
synchronous protobuf
 vs2.example.com cserver_eng  9.9.9.9           -              9
synchronous xml
 vs2.example.com v2n1         3.3.3.3           5.5.5.5        2
synchronous xml
 5 entries were displayed.
```

The following example displays the information about all Vserver FPolicy external engines with the -port parameter set to 9.

```
cluster1::> vserver fpolicy policy external-engine show -fields engine-
name -port 9
 vserver         engine-name
 --------------- -----------
 Cluster         cserver_eng
 vs1.example.com cserver_eng
 vs2.example.com cserver_eng
 3 entries were displayed.
```

The following example displays the values of all the advanced-level parameters for the external engine v1n1 in Vserver vs1.example.com.

```
cluster1::*> vserver fpolicy policy external-engine show -vserver
vs1.example.com -engine-name v1n1 -instance
   (vserver fpolicy policy external-engine show)
Vserver: vs1.example.com
                                          Engine: v1n1
                         Primary FPolicy Servers: 1.1.1.1
                  Port Number of FPolicy Service: 1
                       Secondary FPolicy Servers: 2.2.2.2
                            External Engine Type: synchronous
                          External Engine Format: protobuf
           SSL Option for External Communication: no-auth
                 Timeout for Canceling a Request: 20s
                  Timeout for Aborting a Request: 40s
            Interval for Sending Status Requests: 10s
                           Max Reconnect Attempt: 5
 Maximum Outstanding Requests for FPolicy Server: 50
 Timeout for Disconnecting Non-responsive Server: 1m
        Interval for Sending Keep-Alive Messages: 2m
                      FQDN or Custom Common Name: -
                    Serial Number of Certificate: -
                           Certificate Authority: -
                             Receive Buffer Size: 0
                                Send Buffer Size: 0
    Session ID Purge Timeout During Reconnection: 10s
                   Is Resiliency Feature Enabled: true
         Maximum Notification Retention Duration: 3m
              Directory for Notification Storage: /fpolicy
```

vserver fpolicy policy scope create

Create scope

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

Description

The `vserver fpolicy policy scope create` command creates an FPolicy scope for an FPolicy policy. A scope defines the boundaries on which the FPolicy policy will apply. The Vserver is the basic scope boundary. When you create a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply and you must designate to which Vserver you want to apply the scope. There are a number of parameters that further restrict the scope within the specified Vserver. You can restrict the scope by specifying what to include in the scope. Or you can restrict the scope by specifying what to exclude from the scope. For example, you can restrict the scope by specifying which volumes to include using the `-volumes-to-include` parameter or which volumes to exclude using the `-volumes-to-exclude` parameter. Once you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

> ⓘ There are special considerations for the scope for a cluster FPolicy policy. The cluster FPolicy policy is a policy that the cluster administrator creates for the admin Vserver. If the cluster administrator also creates the scope for that cluster FPolicy policy, a Vserver administrator cannot create a scope for that same policy. However, if the cluster administrator does not create a scope for the cluster FPolicy policy, then any Vserver administrator can create the scope for that cluster policy. In the event that the Vserver administrator creates a scope for that cluster FPolicy policy, the cluster administrator cannot subsequently create a cluster scope for that same cluster policy. This is because the cluster administrator cannot override the scope for the same cluster policy.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to create an FPolicy policy scope.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy for which you want to create the scope.

`[-shares-to-include <Share name>,…]` - Shares to Include

This parameter specifies a list of shares for file access monitoring. With this option, the administrator provides a list of shares, separated by commas. For file access events relative to the specified shares and file operations monitored by the FPolicy policy, a notification is generated. The `-shares-to-include ` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

> ⓘ When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include` .

`[-shares-to-exclude <Share name>,…]` - Shares to Exclude

This parameter specifies a list of shares to exclude from file access monitoring. With this option, the administrator provides a list of shares, separated by commas. When a share is specified in the `-shares-to-exclude` parameter, no notification is sent for files accessed relative to that share. The `-shares-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

`[-volumes-to-include <volume name>,…]` - Volumes to Include

This parameter specifies a list of volumes for file access monitoring. With this option, the administrator provides a list of volumes, separated by commas. For file access events within the volume and file operations monitored by the FPolicy policy, a notification is generated. The `-volumes-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

`[-volumes-to-exclude <volume name>,…]` - Volumes to Exclude

This parameter specifies a list of volumes to exclude from file access monitoring. With this option, the administrator provides a list of volumes, separated by commas, for which no file access notifications are generated. The `-volumes-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

> When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include` . Similarly, when an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export-policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include` .

`[-export-policies-to-include <FPolicy export policy>,…]` - Export Policies to Include

This parameter specifies a list of export policies for file access monitoring. With this option, the administrator provides a list of export policies, separated by commas. For file access events within an export policy and file operations monitored by the FPolicy policy, a notification is generated. The `-export-policies-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

> When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include` .

`[-export-policies-to-exclude <FPolicy export policy>,…]` - Export Policies to Exclude

This parameter specifies a list of export policies to exclude from file access monitoring. With this option, the administrator provides a list of export policies, separated by commas, for which no file access notification is sent. The `-export-policies-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and *.

`[-file-extensions-to-include <File extension>,…]` - File Extensions to Include

This parameter specifies a list of file extensions, separated by commas, for a given FPolicy policy for which FPolicy processing is required. Any file access to files with the same extensions included in the `-file-extensions-to-include` parameter generates a notification. The `-file-extensions-to-include` parameter can contain regular expressions and can include metacharacters such as "?".

`[-file-extensions-to-exclude <File extension>,…]` - File Extensions to Exclude

This parameter specifies a list of file extensions, separated by commas, for a given FPolicy policy for which FPolicy processing will be excluded. Using the exclude list, the administrator can request notification for all extensions except those in the excluded list. Any file access to files with the same extensions included in the `-file-extensions-to-exclude` parameter does not generate a notification. The `-file-extensions-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?".

> An administrator can specify both `-file-extensions-to-include` and `-file-extensions-to-exclude` lists. The `-file-extensions-to-exclude` parameter is checked first before the `-file-extensions-to-include` parameter is checked.

`[-is-file-extension-check-on-directories-enabled {true|false}]` - Is File Extension Check on Directories Enabled (privilege: advanced)

This parameter specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to true, the directory objects are subjected to same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications would be sent for directories even if their name extensions do not match. By default, it is *`true`* .

`[-is-monitoring-of-objects-with-no-extension-enabled {true|false}]` - Is Monitoring of Objects with No Extension Enabled (privilege: advanced)

This parameter specifies whether the extension checks apply to objects with no extension as well. If this parameter is set to true, the objects with no extension are also monitored along with the objects with extension. By default, it is *`false`* .

> This parameter is ignored when file-extensions-to-include and file-extensions-to-exclude lists are empty.

Examples

The following example creates an FPolicy policy scope.

```
cluster1::> vserver fpolicy policy scope create   -vserver vs1.example.com
                                                            -policy-name
vs1_pol
                                                            -file
-extensions-to-include flv,wmv,mp3,mp4
                                                            -file
-extensions-to-exclude cpp,c,h,txt
cluster1::> vserver fpolicy policy scope show
            Vserver           Policy              Extensions
Extensions
            Name              Name                Included
Excluded
            ----------------- ------------------- --------------------
-------------------
            Cluster           cserver_pol         txt
mp3, wmv
            vs1.example.com   vs1_pol             flv, wmv, mp3, mp4
cpp, c, h, txt
            2 entries were displayed.
```

vserver fpolicy policy scope delete

Delete scope

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

Description

The `vserver fpolicy policy scope delete` command deletes an FPolicy policy scope.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver from which you want to delete the FPolicy policy scope.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy for which you want to delete the scope.

Examples

The following example deletes a scope of an FPolicy policy.

```
cluster1::> vserver fpolicy policy scope delete -vserver vs1.example.com
-policy-name vs1_pol
```

vserver fpolicy policy scope modify

Modify scope

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

Description

The `vserver fpolicy policy scope modify` command modifies an FPolicy scope for an FPolicy policy. A scope defines the boundaries on which the FPolicy policy will apply. The Vserver is the basic scope boundary. When you modify a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply and you must designate to which Vserver you want to apply the scope. There are a number of parameters that further restrict the scope within the specified Vserver. You can restrict the scope by specifying what to include in the scope. Or you can restrict the scope by specifying what to exclude from the scope. For example, you can restrict the scope by specifying which volumes to include using the `-volumes-to-include` parameter or which volumes to exclude using the `-volumes-to-exclude` parameter. Once you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the name of the Vserver on which you want to modify an FPolicy policy scope.

`-policy-name <Policy name>` - Policy

This parameter specifies the name of the FPolicy policy for which you want to modify the scope.

`[-shares-to-include <Share name>,…]` - Shares to Include

This parameter specifies a list of shares for file access monitoring. With this option, the administrator provides a list of shares, separated by commas. For file access events relative to the specified shares and file operations monitored by the FPolicy policy, a notification is generated. The `-shares-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

> ⓘ When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include` .

`[-shares-to-exclude <Share name>,…]` **- Shares to Exclude**

This parameter specifies a list of shares to exclude from file access monitoring. With this option, the administrator provides a list of shares, separated by commas. When a share is specified in the `-shares-to-exclude` parameter, no notification is sent for files accessed relative to that share. The `-shares-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

`[-volumes-to-include <volume name>,…]` **- Volumes to Include**

This parameter specifies a list of volumes for file access monitoring. With this option, the administrator provides a list of volumes, separated by commas. For file access events within the volume and file operations monitored by the FPolicy policy, a notification is generated. The `-volumes-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

`[-volumes-to-exclude <volume name>,…]` **- Volumes to Exclude**

This parameter specifies a list of volumes to exclude from file access monitoring. With this option, the administrator provides a list of volumes, separated by commas, for which no file access notifications are generated. The `-volumes-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

> ⓘ When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include` . Similarly, when an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export-policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include` .

`[-export-policies-to-include <FPolicy export policy>,…]` **- Export Policies to Include**

This parameter specifies a list of export policies for file access monitoring. With this option, the administrator provides a list of export policies, separated by commas. For file access events within an export policy and file operations monitored by the FPolicy policy, a notification is generated. The `-export-policies-to-include` parameter can contain regular expressions and can include metacharacters such as "?" and "*".

> ⓘ When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include` .

`[-export-policies-to-exclude <FPolicy export policy>,…]` **- Export Policies to Exclude**

This parameter specifies a list of export policies to exclude from file access monitoring. With this option, the administrator provides a list of export policies, separated by commas, for which no file access notification is sent. The `-export-policies-exclude` parameter can contain regular expressions and can include metacharacters such as "?" and *.

`[-file-extensions-to-include <File extension>,…]` **- File Extensions to Include**

This parameter specifies a list of file extensions, separated by commas, for a given FPolicy policy for which FPolicy processing is required. Any file access to files with the same extensions included in the `-file-extensions-to-include` parameter generates a notification. The `-file-extensions-to-include` parameter can contain regular expressions and can include metacharacters such as "?".

`[-file-extensions-to-exclude <File extension>,…]` - File Extensions to Exclude

This parameter specifies a list of file extensions, separated by commas, for a given FPolicy policy for which FPolicy processing will be excluded. Using the exclude list, the administrator can request notification for all extensions except those in the excluded list. Any file access to files with the same extensions included in the `-file-extensions-to-exclude` parameter does not generate a notification. The `-file -extensions-to-exclude` parameter can contain regular expressions and can include metacharacters such as "?".

ⓘ An administrator can specify both `-file-extensions-to-include` and `-file -extensions-to-exclude` lists. The `-file-extensions-to-exclude` parameter is checked first before the `-file-extensions-to-include` parameter is checked.

`[-is-file-extension-check-on-directories-enabled {true|false}]` - Is File Extension Check on Directories Enabled (privilege: advanced)

This parameter specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to true, the directory objects are subjected to same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications would be sent for directories even if their name extensions do not match. By default, it is *`true`* .

`[-is-monitoring-of-objects-with-no-extension-enabled {true|false}]` - Is Monitoring of Objects with No Extension Enabled (privilege: advanced)

This parameter specifies whether the extension checks apply to objects with no extension as well. If this parameter is set to true, the objects with no extension are also monitored along with the objects with extension. By default, it is *`false`* .

ⓘ This parameter is ignored when file-extensions-to-include and file-extensions-to-exclude lists are empty.

Examples

The following example modifies an FPolicy policy scope.

```
cluster1::> vserver fpolicy policy scope modify   -vserver vs1.example.com
                                                            -policy-name
vs1_pol
                                                            -file
-extensions-to-include flv,wmv,mp3,mp4
                                                            -file
-extensions-to-exclude cpp,c,h,txt
cluster1::> vserver fpolicy policy scope show
            Vserver           Policy              Extensions
Extensions
            Name              Name                Included
Excluded
            ----------------- ------------------- --------------------
-------------------
            Cluster           cserver_pol         txt
mp3, wmv
            vs1.example.com   vs1_pol             flv, wmv, mp3, mp4
cpp, c, h, txt
            2 entries were displayed.
```

vserver fpolicy policy scope show

Display scope

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

Description

The `vserver fpolicy policy scope show` command displays scope information about all FPolicy policies belonging to the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all FPolicy scopes:

- Vserver name
- Policy name
- The file extensions to include
- The file extensions to exclude

You can use the `-fields` parameter to specify which fields of information to display about FPolicy scopes. In addition to the fields above, you can display the following fields:

- The shares to include
- The shares to exclude
- The volumes to include
- The volumes to exclude

- The export policies to include
- The export policies to exclude
- Whether file extension check on directories is enabled
- Whether monitoring of objects with no extension is enabled

You can specify specific parameters to display only information that matches those parameters. For example, to display scope information only about all FPolicy policies where the `-file-extensions-to-include` parameter is set to txt, run the command with the `-fields` parameter set to policy-name and `-file-extensions-to-include` parameter set to txt.

You can specify the `-instance` parameter to display scope information for all FPolicy policies in a list format.

Parameters

{ `[-fields <fieldname>,…]`

If you specify the -fields <fieldname>, … parameter, the command only displays the fields that you specify.

| `[-instance ]` }

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

`[-vserver <Vserver Name>]` - Vserver

If you specify this parameter, the command displays scope information only about the FPolicy policies for the specified Vserver.

`[-policy-name <Policy name>]` - Policy

If you specify this parameter, the command displays information only about the specified FPolicy policy.

`[-shares-to-include <Share name>,…]` - Shares to Include

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified share or shares in the include list.

`[-shares-to-exclude <Share name>,…]` - Shares to Exclude

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified share or shares in the exclude list.

`[-volumes-to-include <volume name>,…]` - Volumes to Include

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified volume or volumes in the include list.

`[-volumes-to-exclude <volume name>,…]` - Volumes to Exclude

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified volume or volumes in the exclude list.

`[-export-policies-to-include <FPolicy export policy>,…]` - Export Policies to Include

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified export policy or policies in the include list.

`[-export-policies-to-exclude <FPolicy export policy>,…]` - Export Policies to Exclude

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified export policy or policies in the exclude list.

`[-file-extensions-to-include <File extension>,…]` - File Extensions to Include

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified file extension or extensions in the include list.

`[-file-extensions-to-exclude <File extension>,…]` - File Extensions to Exclude

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified file extension or extensions in exclude list.

`[-is-file-extension-check-on-directories-enabled {true|false}]` - Is File Extension Check on Directories Enabled (privilege: advanced)

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified file extension check on directories. If set to true, the command displays information about scopes where file extension checks on directories is enabled. If set to false, the command displays information about scopes where file extension checks on directories is disabled.

`[-is-monitoring-of-objects-with-no-extension-enabled {true|false}]` - Is Monitoring of Objects with No Extension Enabled (privilege: advanced)

If you specify this parameter, the command displays scope information only about the FPolicy policy or policies that use the specified monitoring of objects with no extension setting. If set to true, the command displays information about scope of policy or policies for which monitoring of objects with no extension is enabled.

Examples

The following example displays scope information about FPolicy policies.

```
cluster1::> vserver fpolicy policy scope show
         Vserver           Policy              Extensions
Extensions
         Name              Name                Included
Excluded
         ----------------- ------------------- --------------------
-------------------
         Cluster           cserver_pol         -                     -
         vs1.example.com   p                   -                     -
         vs1.example.com   vs1_pol             mp3                   -
         3 entries were displayed.
```

Copyright information

Trademark information