



# **Plan the FPolicy configuration**

## **ONTAP 9**

NetApp  
June 04, 2024

# Table of Contents

- Plan the FPolicy configuration ..... 1
  - Requirements, considerations, and best practices for configuring FPolicy ..... 1
  - What the steps for setting up an FPolicy configuration are ..... 6
- Plan the FPolicy external engine configuration ..... 8
- Plan the FPolicy event configuration ..... 17
- Plan the FPolicy policy configuration ..... 27
- Plan the FPolicy scope configuration ..... 32

# Plan the FPolicy configuration

## Requirements, considerations, and best practices for configuring FPolicy

Before you create and configure FPolicy configurations on your storage virtual machines (SVMs), you need to be aware of certain requirements, considerations, and best practices for configuring FPolicy.

FPolicy features are configured either through the command line interface (CLI) or through REST APIs.

### Requirements for setting up FPolicy

Before you configure and enable FPolicy on your storage virtual machine (SVM), you need to be aware of certain requirements.

- All nodes in the cluster must be running a version of ONTAP that supports FPolicy.
- If you are not using the ONTAP native FPolicy engine, you must have external FPolicy servers (FPolicy servers) installed.
- The FPolicy servers must be installed on a server accessible from the data LIFs of the SVM where FPolicy policies are enabled.



Beginning with ONTAP 9.8, ONTAP provides a client LIF service for outbound FPolicy connections with the addition of the `data-fpolicy-client` service. [Learn more about LIFs and service policies.](#)

- The IP address of the FPolicy server must be configured as a primary or secondary server in the FPolicy policy external engine configuration.
- If the FPolicy servers access data over a privileged data channel, the following additional requirements must be met:
  - SMB must be licensed on the cluster.

Privileged data access is accomplished using SMB connections.

- A user credential must be configured for accessing files over the privileged data channel.
- The FPolicy server must run under the credentials configured in the FPolicy configuration.
- All data LIFs used to communicate with the FPolicy servers must be configured to have `cifs` as one of the allowed protocols.

This includes the LIFs used for passthrough-read connections.

### Best practices and recommendations when setting up FPolicy

When setting up FPolicy on storage virtual machines (SVMs), get familiar with the general configuration best practices and recommendations to ensure that your FPolicy configuration provides robust monitoring performance and results that meet your requirements.

For specific guidelines related to performance, sizing, and configuration, work with your FPolicy partner

application.

## Persistent stores

Beginning with ONTAP 9.14.1, FPolicy allows you to set up a persistent store to capture file access events for asynchronous non-mandatory policies in the SVM. Persistent stores can help decouple client I/O processing from FPolicy notification processing to reduce client latency. Synchronous (either mandatory or non-mandatory) and asynchronous mandatory configurations are not supported.

- Before using the persistent store functionality, ensure your partner applications support this configuration.
- You need one persistent store for each SVM where FPolicy is enabled.
  - Only one persistent store can be set up on each SVM. This single persistent store needs to be used for all FPolicy configurations on that SVM, even if the policies are from different partners.
- ONTAP 9.15.1 or later:
  - The persistent store, its volume, and its volume configuration is handled automatically when you create the persistent store.
- ONTAP 9.14.1:
  - The persistent store, its volume, and its volume configuration is handled manually.
- Create the persistent store volume on the node with LIFs that expect maximum traffic to be monitored by FPolicy.
  - ONTAP 9.15.1 or later: Volumes are automatically created and configured during persistent store creation.
  - ONTAP 9.14.1: Cluster administrators need to create and configure a volume for the persistent store on each SVM where FPolicy is enabled.
- If the notifications accumulated in the persistent store exceed the size of the volume provisioned, FPolicy starts dropping the incoming notification with appropriate EMS messages.
  - ONTAP 9.15.1 or later: In addition to the `size` parameter, the `autosize-mode` parameter can help the volume grow or shrink in response to the amount of used space.
  - ONTAP 9.14.1: The `size` parameter is configured during volume creation to provide a maximum limit.
- Set the snapshot policy to `none` for the persistent store volume instead of `default`. This is to ensure that there is no accidental restore of the snapshot leading to loss of current events and to prevent possible duplicate event processing.
  - ONTAP 9.15.1 or later: The `snapshot-policy` parameter is automatically configured to `none` during persistent store creation.
  - ONTAP 9.14.1: The `snapshot-policy` parameter is configured to `none` during volume creation.
- Make the persistent store volume inaccessible for external user protocol access (CIFS/NFS) to avoid accidental corruption or deletion of the persisted event records.
  - ONTAP 9.15.1 or later: ONTAP automatically blocks the volume from external user protocol access (CIFS/NFS) during persistent store creation.
  - ONTAP 9.14.1: After enabling FPolicy, unmount the volume in ONTAP to remove the junction path. This makes it inaccessible for external user protocol access (CIFS/NFS).

For more information, refer to [FPolicy persistent stores](#) and [Create persistent stores](#).

## Persistent store failover and giveback

The persistent store remains as it was when the last event was received, when there is an unexpected reboot, or FPolicy is disabled and enabled again. After a takeover operation, new events are stored and processed by the partner node. After a giveback operation, the persistent store resumes processing any unprocessed events that might remain from when the node takeover occurred. Live events would be given priority over unprocessed events.

If the persistent store volume moves from one node to another in the same SVM, the notifications that are yet to be processed also move to the new node. You need to re-run the `fpolicy persistent-store create` command on either node after the volume is moved to ensure the pending notifications are delivered to the external server.

## Policy configuration

Configuration of the FPolicy external engine, events, and scope for SVMs can improve your overall experience and security.

- Configuration of the FPolicy external engine for SVMs:
  - Providing additional security comes with a performance cost. Enabling Secure Sockets Layer (SSL) communication has a performance effect on accessing shares.
  - The FPolicy external engine should be configured with more than one FPolicy server to provide resiliency and high availability of FPolicy server notification processing.
- Configuration of FPolicy events for SVMs:

Monitoring file operations influences your overall experience. For example, filtering unwanted file operations on the storage side improves your experience. NetApp recommends setting up the following configuration:

- Monitoring the minimum types of file operations and enabling the maximum number of filters without breaking the use case.
- Using filters for `getattr`, `read`, `write`, `open`, and `close` operations. The SMB and NFS home directory environments have a high percentage of these operations.
- Configuration of FPolicy scope for SVMs:

Restrict the scope of the policies to the relevant storage objects, such as shares, volumes, and exports, instead of enabling them across the entire SVM. NetApp recommends checking the directory extensions. If the `is-file-extension-check-on-directories-enabled` parameter is set to `true`, directory objects are subjected to the same extension checks as regular files.

## Network configuration

Network connectivity between the FPolicy server and the controller should be of low latency. NetApp recommends separating FPolicy traffic from client traffic by using a private network.

In addition, you should place external FPolicy servers (FPolicy servers) in close proximity to the cluster with high-bandwidth connectivity to provide minimal latency and high-bandwidth connectivity.



For a scenario in which the LIF for FPolicy traffic is configured on a different port to the LIF for client traffic, the FPolicy LIF might fail over to the other node because of a port failure. As a result, the FPolicy server becomes unreachable from the node which causes the FPolicy notifications for file operations on the node to fail. To avoid this issue, verify that the FPolicy server can be reached through at least one LIF on the node to process FPolicy requests for the file operations performed on that node.

## Hardware configuration

You can have the FPolicy server on either a physical server or a virtual server. If the FPolicy server is in a virtual environment, you should allocate dedicated resources (CPU, network, and memory) to the virtual server.

The cluster node-to-FPolicy server ratio should be optimized to ensure that FPolicy servers are not overloaded, which can introduce latencies when the SVM responds to client requests. The optimal ratio depends on the partner application for which the FPolicy server is being used. NetApp recommends working with partners to determine the appropriate value.

## Multiple-policy configuration

The FPolicy policy for native blocking has the highest priority, irrespective of the sequence number, and decision-altering policies have a higher priority than others. Policy priority depends on the use case. NetApp recommends working with partners to determine the appropriate priority.

## Size considerations

FPolicy performs in-line monitoring of SMB and NFS operations, sends notifications to the external server, and waits for a response, depending on the mode of external engine communication (synchronous or asynchronous). This process affects the performance of SMB and NFS access and CPU resources.

To mitigate any issues, NetApp recommends working with partners to assess and size the environment before enabling FPolicy. Performance is affected by several factors including the number of users, workload characteristics, such as operations per user and data size, network latency, and failure or server slowness.

## Monitor performance

FPolicy is a notification-based system. Notifications are sent to an external server for processing and to generate a response back to ONTAP. This round-trip process increases latency for client access.

Monitoring the performance counters on the FPolicy server and in ONTAP gives you the capability to identify bottlenecks in the solution and to tune the parameters as necessary for an optimal solution. For example, an increase in FPolicy latency has a cascading effect on SMB and NFS access latency. Therefore, you should monitor both workload (SMB and NFS) and FPolicy latency. In addition, you can use quality-of-service policies in ONTAP to set up a workload for each volume or SVM that is enabled for FPolicy.

NetApp recommends running the `statistics show -object workload` command to display workload statistics. In addition, you should monitor the following parameters:

- Average, read, and write latencies
- Total number of operations
- Read and write counters

You can monitor the performance of FPolicy subsystems by using the following FPolicy counters.



You must be in diagnostic mode to collect statistics related to FPolicy.

## Steps

### 1. Collect FPolicy counters:

- `statistics start -object fpolicy -instance instance_name -sample-id ID`
- `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

### 2. Display FPolicy counters:

- `statistics show -object fpolicy -instance instance_name -sample-id ID`
- `statistics show -object fpolicy_server -instance instance_name -sample-id ID`

The `fpolicy` and `fpolicy_server` counters give you information on several performance parameters which are described in the following table.

Counters	Description
<b>“fpolicy” counters</b>	
<code>aborted_requests</code>	Number of screen requests for which processing is aborted on the SVM
<code>event_count</code>	List of events resulting in notification
<code>max_request_latency</code>	Maximum screen requests latency
<code>outstanding_requests</code>	Total number of screen requests in process
<code>processed_requests</code>	Total number of screen requests that went through fpolicy processing on the SVM
<code>request_latency_hist</code>	Histogram of latency for screen requests
<code>requests_dispatched_rate</code>	Number of screen requests dispatched per second
<code>requests_received_rate</code>	Number of screen requests received per second
<b>“fpolicy_server” counters</b>	
<code>max_request_latency</code>	Maximum latency for a screen request
<code>outstanding_requests</code>	Total number of screen requests waiting for response
<code>request_latency</code>	Average latency for screen request
<code>request_latency_hist</code>	Histogram of latency for screen requests
<code>request_sent_rate</code>	Number of screen requests sent to FPolicy server per second
<code>response_received_rate</code>	Number of screen responses received from FPolicy server per second

## Manage FPolicy workflow and dependency on other technologies

NetApp recommends disabling an FPolicy policy before making any configuration changes. For example, if you want to add or modify an IP address in the external engine configured for the enabled policy, first disable the policy.

If you configure FPolicy to monitor NetApp FlexCache volumes, NetApp recommends that you not configure FPolicy to monitor read and getattr file operations. Monitoring these operations in ONTAP requires the retrieval of inode-to-path (I2P) data. Because I2P data cannot be retrieved from FlexCache volumes, it must be retrieved from the origin volume. Therefore, monitoring these operations eliminates the performance benefits that FlexCache can provide.

When both FPolicy and an off-box antivirus solution are deployed, the antivirus solution receives notifications first. FPolicy processing starts only after antivirus scanning is complete. It is important that you size antivirus solutions correctly because a slow antivirus scanner can affect overall performance.

## Passthrough-read upgrade and revert considerations

There are certain upgrade and revert considerations that you must know about before upgrading to an ONTAP release that supports passthrough-read or before reverting to a release that does not support passthrough-read.

### Upgrading

After all nodes are upgraded to a version of ONTAP that supports FPolicy passthrough-read, the cluster is capable of using the passthrough-read functionality; however, passthrough-read is disabled by default on existing FPolicy configurations. To use passthrough-read on existing FPolicy configurations, you must disable the FPolicy policy and modify the configuration, and then reenabling the configuration.

### Reverting

Before reverting to a version of ONTAP that does not support FPolicy passthrough-read, you must meet the following conditions:

- Disable all the policies using passthrough-read, and then modify the affected configurations so that they do not use passthrough-read.
- Disable FPolicy functionality on the cluster by disabling every FPolicy policy on the cluster.

Before reverting to a version of ONTAP that does not support persistent stores, ensure that none of the FPolicy policies have a configured persistent store. If a persistent store is configured, the revert will fail.

## What the steps for setting up an FPolicy configuration are

Before FPolicy can monitor file access, an FPolicy configuration must be created and enabled on the storage virtual machine (SVM) for which FPolicy services are required.

The steps for setting up and enabling an FPolicy configuration on the SVM are as follows:

1. Create an FPolicy external engine.

The FPolicy external engine identifies the external FPolicy servers (FPolicy servers) that are associated with a specific FPolicy configuration. If the internal “native” FPolicy engine is used to create a native file-blocking configuration, you do not need to create an FPolicy external engine.

Beginning with ONTAP 9.15.1, you can use the `protobuf` engine format. When set to `protobuf`, the notification messages are encoded in binary form using Google Protobuf. Before setting the engine format to `protobuf`, ensure that the FPolicy server also supports `protobuf` deserialization. For more information, see [Plan the FPolicy external engine configuration](#)



## 2. Create an FPolicy event.

An FPolicy event describes what the FPolicy policy should monitor. Events consist of the protocols and file operations to monitor, and can contain a list of filters. Events use filters to narrow the list of monitored events for which the FPolicy external engine must send notifications. Events also specify whether the policy monitors volume operations.

## 3. Create an FPolicy persistent store (optional).

Beginning with ONTAP 9.14.1, FPolicy allows you to set up [persistent stores](#) to capture file access events for asynchronous non-mandatory policies in the SVM. Synchronous (either mandatory or non-mandatory) and asynchronous mandatory configurations are not supported.

Persistent stores can help decouple client I/O processing from FPolicy notification processing to reduce client latency.

Beginning with ONTAP 9.15.1, FPolicy persistent store configuration is simplified. The `persistent-store-create` command automates volume creation for the SVM and configures the volume for the persistent store.

## 4. Create an FPolicy policy.

The FPolicy policy is responsible for associating, with the appropriate scope, the set of events that need to be monitored and for which of the monitored events notifications must be sent to the designated FPolicy server (or to the native engine if no FPolicy servers are configured). The policy also defines whether the FPolicy server is allowed privileged access to the data for which it receives notifications. An FPolicy server needs privileged access if the server needs to access the data. Typical use cases where privileged access is needed include file blocking, quota management, and hierarchical storage management. The policy is where you specify whether the configuration for this policy uses an FPolicy server or the internal “native” FPolicy server.

A policy specifies whether screening is mandatory. If screening is mandatory and all FPolicy servers are down or no response is received from the FPolicy servers within a defined timeout period, then file access is denied.

A policy’s boundaries are the SVM. A policy cannot apply to more than one SVM. However, a specific SVM can have multiple FPolicy policies, each with the same or different combination of scope, event, and external server configurations.

## 5. Configure the policy scope.

The FPolicy scope determines which volumes, shares, or export-policies the policy acts on or excludes from monitoring. A scope also determines which file extensions should be included or excluded from FPolicy monitoring.



Exclude lists take precedence over include lists.

## 6. Enable the FPolicy policy.

When the policy is enabled, the control channels and, optionally, the privileged data channels are connected. The FPolicy process on the nodes on which the SVM participates begin monitoring file and folder access and, for events that match configured criteria, sends notifications to the FPolicy servers (or to the native engine if no FPolicy servers are configured).



If the policy uses native file blocking, an external engine is not configured or associated with the policy.

## Plan the FPolicy external engine configuration

### Plan the FPolicy external engine configuration

Before you configure the FPolicy external engine, you must understand what it means to create an external engine and which configuration parameters are available. This information helps you to determine which values to set for each parameter.

#### Information that is defined when creating the FPolicy external engine

The external engine configuration defines the information that FPolicy needs to make and manage connections to the external FPolicy servers, including the following:

- SVM name
- Engine name
- The IP addresses of the primary and secondary FPolicy servers and the TCP port number to use when making the connection to the FPolicy servers
- Whether the engine type is asynchronous or synchronous
- Whether the engine format is `xml` or `protobuf`

Beginning with ONTAP 9.15.1, you can use the `protobuf` engine format. When set to `protobuf`, the notification messages are encoded in binary form using Google Protobuf. Before setting the engine format to `protobuf`, ensure that the FPolicy server also supports `protobuf` deserialization.

Since the `protobuf` format is supported beginning with ONTAP 9.15.1, you must consider external engine format before reverting to an earlier release of ONTAP. If you revert to an earlier release than ONTAP 9.15.1, work with your FPolicy partner to either:

- Change each engine format from `protobuf` to `xml`
- Delete the engines with an engine format of `protobuf`
- How to authenticate the connection between the node and the FPolicy server

If you choose to configure mutual SSL authentication, then you must also configure parameters that provide SSL certificate information.


- How to manage the connection using various advanced privilege settings

This includes parameters that define such things as timeout values, retry values, keep-alive values, maximum request values, sent and receive buffer size values, and session timeout values.

The `vserver fpolicy policy external-engine create` command is used to create an FPolicy external engine.

## What the basic external engine parameters are

You can use the following table of basic FPolicy configuration parameters to help you plan your configuration:

Type of information	Option
<p><b>SVM</b></p> <p>Specifies the SVM name that you want to associate with this external engine.</p> <p>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p><b>Engine name</b></p> <p>Specifies the name to assign to the external engine configuration. You must specify the external engine name later when you create the FPolicy policy. This associates the external engine with the policy.</p> <p>The name can be up to 256 characters long.</p> <div><p>The name should be up to 200 characters long if configuring the external engine name in a MetroCluster or SVM disaster recovery configuration.</p></div> <p>The name can contain any combination of the following ASCII-range characters:</p> <ul style="list-style-type: none"><li>• a through z</li><li>• A through Z</li><li>• 0 through 9</li><li>• “_”, “-”, and “.”</li></ul>	<p><code>-engine-name engine_name</code></p>

<p><i>Primary FPolicy servers</i></p> <p>Specifies the primary FPolicy servers to which the node sends notifications for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses.</p> <p>If more than one primary server IP address is specified, every node on which the SVM participates creates a control connection to every specified primary FPolicy server at the time the policy is enabled. If you configure multiple primary FPolicy servers, notifications are sent to the FPolicy servers in a round-robin fashion.</p> <p>If the external engine is used in a MetroCluster or SVM disaster recovery configuration, you should specify the IP addresses of the FPolicy servers at the source site as primary servers. The IP addresses of the FPolicy servers at the destination site should be specified as secondary servers.</p>	<p>-primary-servers IP_address,...</p>
<p><i>Port number</i></p> <p>Specifies the port number of the FPolicy service.</p>	<p>-port integer</p>
<p><i>Secondary FPolicy servers</i></p> <p>Specifies the secondary FPolicy servers to which to send file access events for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses.</p> <p>Secondary servers are used only when none of the primary servers are reachable. Connections to secondary servers are established when the policy is enabled, but notifications are sent to secondary servers only if none of the primary servers are reachable. If you configure multiple secondary servers, notifications are sent to the FPolicy servers in a round-robin fashion.</p>	<p>-secondary-servers IP_address,...</p>
<p><i>External engine type</i></p> <p>Specifies whether the external engine operates in synchronous or asynchronous mode. By default, FPolicy operates in synchronous mode.</p> <p>When set to <code>synchronous</code>, file request processing sends a notification to the FPolicy server, but then 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.</p> <p>When set to <code>asynchronous</code>, file request processing sends a notification to the FPolicy server, and then continues.</p>	<p>-extern-engine-type external_engine_type The value for this parameter can be one of the following:</p> <ul style="list-style-type: none"> <li>• synchronous</li> <li>• asynchronous</li> </ul>

<p><i>External engine format</i></p> <p>Specify whether the external engine format is xml or protobuf.</p> <p>Beginning with ONTAP 9.15.1, you can use the protobuf engine format. When set to protobuf, the notification messages are encoded in binary form using Google Protobuf. Before setting the engine format to protobuf, ensure that the FPolicy server also supports protobuf deserialization.</p>	<pre>- extern-engine-format {protobuf or xml}</pre>
<p><i>SSL option for communication with FPolicy server</i></p> <p>Specifies the SSL option for communication with the FPolicy server. This is a required parameter. You can choose one of the options based on the following information:</p> <ul style="list-style-type: none"> <li>• When set to <code>no-auth</code>, no authentication takes place.</li> </ul> <p>The communication link is established over TCP.</p> <ul style="list-style-type: none"> <li>• When set to <code>server-auth</code>, the SVM authenticates the FPolicy server using SSL server authentication.</li> <li>• When set to <code>mutual-auth</code>, mutual authentication takes place between the SVM and the FPolicy server; the SVM authenticates the FPolicy server, and the FPolicy server authenticates the SVM.</li> </ul> <p>If you choose to configure mutual SSL authentication, then you must also configure the <code>-certificate-common-name</code>, <code>-certificate-serial</code>, and <code>-certificate-ca</code> parameters.</p>	<pre>-ssl-option {no-auth  server-auth mutual-auth}</pre>
<p><i>Certificate FQDN or custom common name</i></p> <p>Specifies the certificate name used if SSL authentication between the SVM and the FPolicy server is configured. You can specify the certificate name as an FQDN or as a custom common name.</p> <p>If you specify <code>mutual-auth</code> for the <code>-ssl-option</code> parameter, you must specify a value for the <code>-certificate-common-name</code> parameter.</p>	<pre>-certificate-common -name text</pre>
<p><i>Certificate serial number</i></p> <p>Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.</p> <p>If you specify <code>mutual-auth</code> for the <code>-ssl-option</code> parameter, you must specify a value for the <code>-certificate-serial</code> parameter.</p>	<pre>-certificate-serial text</pre>

<p><b>Certificate authority</b></p> <p>Specifies the CA name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.</p> <p>If you specify <code>mutual-auth</code> for the <code>-ssl-option</code> parameter, you must specify a value for the <code>-certificate-ca</code> parameter.</p>	<p><code>-certificate-ca text</code></p>
---	--

## What the advanced external engine options are

You can use the following table of advanced FPolicy configuration parameters as you plan whether to customize your configuration with advanced parameters. You use these parameters to modify communication behavior between the cluster nodes and the FPolicy servers:

Type of information	Option
<p><b>Timeout for canceling a request</b></p> <p>Specifies the time interval in hours (h), minutes (m), or seconds (s) that the node waits for a response from the FPolicy server.</p> <p>If the timeout interval passes, the node sends a cancel request to the FPolicy server. The node then sends the notification to an alternate FPolicy server. This timeout helps in handling an FPolicy server that is not responding, which can improve SMB/NFS client response. Also, canceling requests after a timeout period can help in releasing system resources because the notification request is moved from a down/bad FPolicy server to an alternate FPolicy server.</p> <p>The range for this value is 0 through 100. If the value is set to 0, the option is disabled and cancel request messages are not sent to the FPolicy server. The default is 20s.</p>	<p><code>-reqs-cancel-timeout integer[h m s]</code></p>
<p><b>Timeout for aborting a request</b></p> <p>Specifies the timeout in hours (h), minutes (m), or seconds (s) for aborting a request.</p> <p>The range for this value is 0 through 200.</p>	<p><code>-reqs-abort-timeout `integer[h m s]</code></p>
<p><b>Interval for sending status requests</b></p> <p>Specifies the interval in hours (h), minutes (m), or seconds (s) after which a status request is sent to the FPolicy server.</p> <p>The range for this value is 0 through 50. If the value is set to 0, the option is disabled and status request messages are not sent to the FPolicy server. The default is 10s.</p>	<p><code>-status-req-interval integer[h m s]</code></p>

<p><i>Maximum outstanding requests on the FPolicy server</i></p> <p>Specifies the maximum number of outstanding requests that can be queued on the FPolicy server.</p> <p>The range for this value is 1 through 10000. The default is 500.</p>	<p>-max-server-reqs integer</p>
<p><i>Timeout for disconnecting a nonresponsive FPolicy server</i></p> <p>Specifies the time interval in hours (h), minutes (m), or seconds (s) after which the connection to the FPolicy server is terminated.</p> <p>The connection is terminated after the timeout period only if the FPolicy server's queue contains the maximum allowed requests and no response is received within the timeout period. The maximum allowed number of requests is either 50 (the default) or the number specified by the max-server-reqs- parameter.</p> <p>The range for this value is 1 through 100. The default is 60s.</p>	<p>-server-progress -timeout integer[h m s]</p>
<p><i>Interval for sending keep-alive messages to the FPolicy server</i></p> <p>Specifies the time interval in hours (h), minutes (m), or seconds (s) at which keep-alive messages are sent to the FPolicy server.</p> <p>Keep-alive messages detect half-open connections.</p> <p>The range for this value is 10 through 600. If the value is set to 0, the option is disabled and keep-alive messages are prevented from being sent to the FPolicy servers. The default is 120s.</p>	<p>-keep-alive-interval-integer[h m s]</p>
<p><i>Maximum reconnect attempts</i></p> <p>Specifies the maximum number of times the SVM attempts to reconnect to the FPolicy server after the connection has been broken.</p> <p>The range for this value is 0 through 20. The default is 5.</p>	<p>-max-connection-retries integer</p>
<p><i>Receive buffer size</i></p> <p>Specifies the receive buffer size of the connected socket for the FPolicy server.</p> <p>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.</p> <p>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.</p>	<p>-recv-buffer-size integer</p>

<p><i>Send buffer size</i></p> <p>Specifies the send buffer size of the connected socket for the FPolicy server.</p> <p>The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the send buffer is set to a value defined by the system.</p> <p>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.</p>	<p><code>-send-buffer-size</code> integer</p>
<p><i>Timeout for purging a session ID during reconnection</i></p> <p>Specifies the interval in hours (h), minutes (m), or seconds (s) after which a new session ID is sent to the FPolicy server during reconnection attempts.</p> <p>If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the <code>-session-timeout</code> interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications.</p> <p>The default value is set to 10 seconds.</p>	<p><code>-session-timeout</code> [integerh][integerm][integer s]</p>

## Additional information about configuring FPolicy external engines to use SSL authenticated connections

You need to know some additional information if you want to configure the FPolicy external engine to use SSL when connecting to FPolicy servers.

### SSL server authentication

If you choose to configure the FPolicy external engine for SSL server authentication, before creating the external engine, you must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.

### Mutual authentication

If you configure FPolicy external engines to use SSL mutual authentication when connecting storage virtual machine (SVM) data LIFs to external FPolicy servers, before creating the external engine, you must install the public certificate of the CA that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM. You must not delete this certificate while any FPolicy policies are using the installed certificate.

If the certificate is deleted while FPolicy is using it for mutual authentication when connecting to an external FPolicy server, you cannot reenabling a disabled FPolicy policy that uses that certificate. The FPolicy policy cannot be reenabled in this situation even if a new certificate with the same settings is created and installed on the SVM.

If the certificate has been deleted, you need to install a new certificate, create new FPolicy external engines that use the new certificate, and associate the new external engines with the FPolicy policy that you want to



reenable by modifying the FPolicy policy.

## Install certificates for SSL

The public certificate of the CA that is used to sign the FPolicy server certificate is installed by using the `security certificate install` command with the `-type` parameter set to `client-ca`. The private key and public certificate required for authentication of the SVM is installed by using the `security certificate install` command with the `-type` parameter set to `server`.

## Certificates do not replicate in SVM disaster recovery relationships with a non-ID-preserve configuration

Security certificates used for SSL authentication when making connections to FPolicy servers do not replicate to SVM disaster recovery destinations with non-ID-preserve configurations. Although the FPolicy external-engine configuration on the SVM is replicated, security certificates are not replicated. You must manually install the security certificates on the destination.

When you set up the SVM disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), all of the FPolicy configuration details are replicated, including the security certificate information. You must install the security certificates on the destination only if you set the option to `false` (non-ID-preserve).

## Restrictions for cluster-scoped FPolicy external engines with MetroCluster and SVM disaster recovery configurations

You can create a cluster-scoped FPolicy external engine by assigning the cluster storage virtual machine (SVM) to the external engine. However, when creating a cluster-scoped external engine in a MetroCluster or SVM disaster recovery configuration, there are certain restrictions when choosing the authentication method that the SVM uses for external communication with the FPolicy server.

There are three authentication options that you can choose when creating external FPolicy servers: no authentication, SSL server authentication, and SSL mutual authentication. Although there are no restrictions when choosing the authentication option if the external FPolicy server is assigned to a data SVM, there are restrictions when creating a cluster-scoped FPolicy external engine:

Configuration	Permitted?
MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with no authentication (SSL is not configured)	Yes
MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with SSL server or SSL mutual authentication	No

- If a cluster-scoped FPolicy external engine with SSL authentication exists and you want to create a MetroCluster or SVM disaster recovery configuration, you must modify this external engine to use no

authentication or remove the external engine before you can create the MetroCluster or SVM disaster recovery configuration.

- If the MetroCluster or SVM disaster recovery configuration already exists, ONTAP prevents you from creating a cluster-scoped FPolicy external engine with SSL authentication.

## Complete the FPolicy external engine configuration worksheet

You can use this worksheet to record the values that you need during the FPolicy external engine configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the external engine.

### Information for a basic external engine configuration

You should record whether you want to include each parameter setting in the external engine configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage virtual machine (SVM) name	Yes	Yes	
Engine name	Yes	Yes	
Primary FPolicy servers	Yes	Yes	
Port number	Yes	Yes	
Secondary FPolicy servers	No		
External engine type	No		
SSL option for communication with external FPolicy server	Yes	Yes	
Certificate FQDN or custom common name	No		
Certificate serial number	No		
Certificate authority	No		

### Information for advanced external engine parameters

To configure an external engine with advanced parameters, you must enter the configuration command while in advanced privilege mode.

Type of information	Required	Include	Your values
Timeout for canceling a request	No		

Timeout for aborting a request	No		
Interval for sending status requests	No		
Maximum outstanding requests on the FPolicy server	No		
Timeout for disconnecting a nonresponsive FPolicy server	No		
Interval for sending keep-alive messages to the FPolicy server	No		
Maximum reconnect attempts	No		
Receive buffer size	No		
Send buffer size	No		
Timeout for purging a session ID during reconnection	No		

## Plan the FPolicy event configuration

### Plan the FPolicy event configuration overview

Before you configure FPolicy events, you must understand what it means to create an FPolicy event. You must determine which protocols you want the event to monitor, which events to monitor, and which event filters to use. This information helps you plan the values that you want to set.

#### What it means to create an FPolicy event

Creating the FPolicy event means defining information that the FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server. The FPolicy event configuration defines the following configuration information:

- Storage virtual machine (SVM) name
- Event name
- Which protocols to monitor

FPolicy can monitor SMB, NFSv3, NFSv4, and, beginning in ONTAP 9.15.1, NFSv4.1 file access operations.

- Which file operations to monitor

Not all file operations are valid for each protocol.

- Which file filters to configure

Only certain combinations of file operations and filters are valid. Each protocol has its own set of supported combinations.

- Whether to monitor volume mount and unmount operations





There is a dependency with three of the parameters (`-protocol`, `-file-operations`, `-filters`). The following combinations are valid for the three parameters:

- You can specify the `-protocol` and `-file-operations` parameters.
- You can specify all three of the parameters.
- You can specify none of the parameters.

## What the FPolicy event configuration contains

You can use the following list of available FPolicy event configuration parameters to help you plan your configuration:

Type of information	Option
<p><b>SVM</b></p> <p>Specifies the SVM name that you want to associate with this FPolicy event.</p> <p>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p><b>Event name</b></p> <p>Specifies the name to assign to the FPolicy event. When you create the FPolicy policy you associate the FPolicy event with the policy using the event name.</p> <p>The name can be up to 256 characters long.</p> <div> <p>The name should be up to 200 characters long if configuring the event in a MetroCluster or SVM disaster recovery configuration.</p> </div> <p>The name can contain any combination of the following ASCII-range characters:</p> <ul style="list-style-type: none"> <li>• a through z</li> <li>• A through Z</li> <li>• 0 through 9</li> <li>• " _ ", "-", and "."</li> </ul>	<p><code>-event-name event_name</code></p>

<p><i>Protocol</i></p> <p>Specifies which protocol to configure for the FPolicy event. The list for <code>-protocol</code> can include one of the following values:</p> <ul style="list-style-type: none"> <li>• <code>cifs</code></li> <li>• <code>nfsv3</code></li> <li>• <code>nfsv4</code></li> </ul> <div data-bbox="167 489 220 546">  </div> <p>If you specify <code>-protocol</code>, then you must specify a valid value in the <code>-file-operations</code> parameter. As the protocol version changes, the valid values might change.</p> <div data-bbox="167 632 220 688">  </div> <p>Beginning in ONTAP 9.15.1, <code>nfsv4</code> allows you to capture NFSv4.0 and NFSv4.1 events.</p>	<p><code>-protocol protocol</code></p>
--	--

### *File operations*

Specifies the list of file operations for the FPolicy event.

The event checks the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. You can list one or more file operations by using a comma-delimited list. The list for `-file-operations` can include one or more of the following values:

- `close` for file close operations
- `create` for file create operations
- `create-dir` for directory create operations
- `delete` for file delete operations
- `delete_dir` for directory delete operations
- `getattr` for get attribute operations
- `link` for link operations
- `lookup` for lookup operations
- `open` for file open operations
- `read` for file read operations
- `write` for file write operations
- `rename` for file rename operations
- `rename_dir` for directory rename operations
- `setattr` for set attribute operations
- `symlink` for symbolic link operations



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

`-file-operations`  
`file_operations,...`

## Filters

`-filters filter, ...`

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



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

- `monitor-ads` option to filter the client request for alternate data stream.
- `close-with-modification` option to filter the client request for close with modification.
- `close-without-modification` option to filter the client request for close without modification.
- `first-read` option to filter the client request for first read.
- `first-write` option to filter the client request for first write.
- `offline-bit` option to filter the client request for offline bit set.

Setting this filter results in the FPolicy server receiving notification only when offline files are accessed.

- `open-with-delete-intent` option to filter the client request for open with delete intent.

Setting this filter results in the FPolicy server receiving 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` option to filter client request for open with write intent.

Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to write something in it.

- `write-with-size-change` option to filter the client request for write with size change.
- `setattr-with-owner-change` option to filter the client setattr requests for changing owner of a file or a directory.
- `setattr-with-group-change` option to filter the client setattr requests for changing the group of a file or a directory.
- `setattr-with-sacl-change` option to filter the client setattr requests for changing the SAcl on a file or a directory.

This filter is available only for the SMB and NFSv4 protocols.

`setattr-with-dacl-change` option to filter the client setattr requests for changing the DACL on a file or a directory.

<p><i>Is volume operation required</i></p> <p>Specifies whether monitoring is required for volume mount and unmount operations. The default is <code>false</code>.</p>	<pre>-volume-operation {true false}</pre> <pre>-filters filter, ...</pre>
<p><i>FPolicy access denied notifications</i></p> <p>Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. These notifications are valuable for security, ransomware protection, and governance. Notifications will be generated for file operation failed due to lack of permission, which includes:</p> <ul style="list-style-type: none"> <li>• Failures due to NTFS permissions.</li> <li>• Failures due to Unix mode bits.</li> <li>• Failures due to NFSv4 ACLs.</li> </ul>	<pre>-monitor-fileop-failure {true false}</pre>

This option is available only for the SMB protocol.

## Supported file operation and filter combinations that FPolicy can monitor for SMB

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring SMB file access operations. When this filter is specified, the directory operations are not monitored.

The list of supported file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

Supported file operations	Supported filters
close	monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, exclude-directory
create	monitor-ads, offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	monitor-ads, offline-bit
delete_dir	Currently no filter is supported for this file operation.
getattr	offline-bit, exclude-dir
open	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
read	monitor-ads, offline-bit, first-read
write	monitor-ads, offline-bit, first-write, write-with-size-change



rename	monitor-ads, offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_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

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

Supported access denied file operation	Supported filters
open	NA

## Supported file operation and filter combinations that FPolicy can monitor for NFSv3

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv3 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

Supported file operations	Supported filters
create	offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	offline-bit
delete_dir	Currently no filter is supported for this file operation.
link	offline-bit
lookup	offline-bit, exclude-dir
read	offline-bit, first-read
write	offline-bit, first-write, write-with-size-change

rename	offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	offline-bit

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

Supported access denied file operation	Supported filters
access	NA
create	NA
create_dir	NA
delete	NA
delete_dir	NA
link	NA
read	NA
rename	NA
rename_dir	NA
setattr	NA
write	NA

## Supported file operation and filter combinations that FPolicy can monitor for NFSv4

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv4 file access operations.

Beginning with ONTAP 9.15.1, FPolicy supports the NFSv4.1 protocol.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv4 or NFSv4.1 file access events is provided in the following table:

Supported file operations	Supported filters
close	offline-bit, exclude-directory
create	offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	offline-bit
delete_dir	Currently no filter is supported for this file operation.
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, first-write, write-with-size-change
rename	offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_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

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of NFSv4 or NFSv4.1 file access events is provided in the following table:

Supported access denied file operation	Supported filters
--	-------------------

access	NA
create	NA
create_dir	NA
delete	NA
delete_dir	NA
link	NA
open	NA
read	NA
rename	NA
rename_dir	NA
setattr	NA
write	NA

## Complete the FPolicy event configuration worksheet

You can use this worksheet to record the values that you need during the FPolicy event configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy event.

You should record whether you want to include each parameter setting in the FPolicy event configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage virtual machine (SVM) name	Yes	Yes	
Event name	Yes	Yes	
Protocol	No		
File operations	No		
Filters	No		

Volume operation	No		
Access denied events (support beginning with ONTAP 9.13)	No		

## Plan the FPolicy policy configuration

### Plan the FPolicy policy configuration overview

Before you configure the FPolicy policy, you must understand which parameters are required when creating the policy as well as why you might want to configure certain optional parameters. This information helps you to determine which values to set for each parameter.

When creating an FPolicy policy you associate the policy with the following:

- The storage virtual machine (SVM)
- One or more FPolicy events
- An FPolicy external engine

You can also configure several optional policy settings.

### What the FPolicy policy configuration contains

You can use the following list of available FPolicy policy required and optional parameters to help you plan your configuration:

Type of information	Option	Required	Default
<p><i>SVM name</i></p> <p>Specifies the name of the SVM on which you want to create an FPolicy policy.</p>	<p><code>-vserver</code> <code>vserver_name</code></p>	Yes	None

<p><b>Policy name</b></p> <p>Specifies the name of the FPolicy policy.</p> <p>The name can be up to 256 characters long.</p> <div data-bbox="167 422 220 474"> </div> <p>The name should be up to 200 characters long if configuring the policy in a MetroCluster or SVM disaster recovery configuration.</p> <p>The name can contain any combination of the following ASCII-range characters:</p> <ul style="list-style-type: none"> <li>• a through z</li> <li>• A through Z</li> <li>• 0 through 9</li> <li>• “_”, “-”, and “.”</li> </ul>	<p>-policy-name policy_name</p>	<p>Yes</p>	<p>None</p>
<p><b>Event names</b></p> <p>Specifies a comma-delimited list of events to associate with the FPolicy policy.</p> <ul style="list-style-type: none"> <li>• You can associate more than one event to a policy.</li> <li>• An event is specific to a protocol.</li> <li>• You can use a single policy to monitor file access events for more than one protocol by creating an event for each protocol that you want the policy to monitor, and then associating the events to the policy.</li> <li>• The events must already exist.</li> </ul>	<p>-events event_name, ...</p>	<p>Yes</p>	<p>None</p>
<p><b>Persistent store</b></p> <p>Beginning with ONTAP 9.14.1, this parameter specifies the persistent store to capture file access events for asynchronous non-mandatory policies in the SVM.</p>	<p>-persistent -store persistent_store_name</p>	<p>No</p>	<p>None</p>

<p><i>External engine name</i></p> <p>Specifies the name of the external engine to associate with the FPolicy policy.</p> <ul style="list-style-type: none"> <li>• An external engine contains information required by the node to send notifications to an FPolicy server.</li> <li>• You can configure FPolicy to use the ONTAP native external engine for simple file blocking or to use an external engine that is configured to use external FPolicy servers (FPolicy servers) for more sophisticated file blocking and file management.</li> <li>• If you want to use the native external engine, you can either not specify a value for this parameter or you can specify <code>native</code> as the value.</li> <li>• If you want to use FPolicy servers, the configuration for the external engine must already exist.</li> </ul>	<p><code>-engine engine_name</code></p>	<p>Yes (unless the policy uses the internal ONTAP native engine)</p>	<p><code>native</code></p>
<p><i>Is mandatory screening required</i></p> <p>Specifies whether mandatory file access screening is required.</p> <ul style="list-style-type: none"> <li>• The mandatory screening setting determines what action is taken 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.</li> <li>• When set to <code>true</code>, file access events are denied.</li> <li>• When set to <code>false</code>, file access events are allowed.</li> </ul>	<p><code>-is-mandatory {true false}</code></p>	<p>No</p>	<p><code>true</code></p>

<p><i>Allow privileged access</i></p> <p>Specifies whether you want the FPolicy server to have privileged access to the monitored files and folders by using a privileged data connection.</p> <p>If configured, FPolicy servers can access files from the root of the SVM containing the monitored data using the privileged data connection.</p> <p>For privileged data access, SMB must be licensed on the cluster and all the data LIFs used to connect to the FPolicy servers must be configured to have <code>cifs</code> as one of the allowed protocols.</p> <p>If you want to configure the policy to allow privileged access, you must also specify the user name for the account that you want the FPolicy server to use for privileged access.</p>	<p>-allow -privileged -access {yes no}</p>	<p>No (unless passthrough-read is enabled)</p>	<p>no</p>
<p><i>Privileged user name</i></p> <p>Specifies the user name of the account the FPolicy servers use for privileged data access.</p> <ul style="list-style-type: none"> <li>• The value for this parameter should use the “domain\user name” format.</li> <li>• If <code>-allow-privileged-access</code> is set to <code>no</code>, any value set for this parameter is ignored.</li> </ul>	<p>-privileged -user-name user_name</p>	<p>No (unless privileged access is enabled)</p>	<p>None</p>



<p><i>Allow passthrough-read</i></p> <p>Specifies whether the FPolicy servers can provide passthrough-read services for files that have been archived to secondary storage (offline files) by the FPolicy servers:</p> <ul style="list-style-type: none"> <li>• Passthrough-read is a way to read data for offline files without restoring the data to the primary storage.</li> </ul> <p>Passthrough-read reduces response latencies because there is no need to recall files back to primary storage before responding to the read request. Additionally, passthrough-read optimizes storage efficiency by eliminating the need to consume primary storage space with files that are recalled solely to satisfy read requests.</p> <ul style="list-style-type: none"> <li>• When enabled, the FPolicy servers provide the data for the file over a separate privileged data channel opened specifically for passthrough-reads.</li> <li>• If you want to configure passthrough-read, the policy must also be configured to allow privileged access.</li> </ul>	<p><code>-is-passthrough</code>  <code>-read-enabled</code>  <code>{true false}</code></p>	<p>No</p>	<p>false</p>
--	--	-----------	--------------

## Requirement for FPolicy scope configurations if the FPolicy policy uses the native engine

If you configure the FPolicy policy to use the native engine, there is a specific requirement for how you define the FPolicy scope configured for the policy.

The FPolicy scope defines the boundaries on which the FPolicy policy applies, for example whether the FPolicy applies to specified volumes or shares. There are a number of parameters that further restrict the scope to which the FPolicy policy applies. One of these parameters, `-is-file-extension-check-on-directories-enabled`, specifies whether to check file extensions on directories. The default value is `false`, which means that file extensions on directories are not checked.

When an FPolicy policy that uses the native engine is enabled on a share or volume and the `-is-file-extension-check-on-directories-enabled` parameter is set to `false` for the scope of the policy, directory access is denied. With this configuration, because the file extensions are not checked for directories, any directory operation is denied if it falls under the scope of the policy.

To ensure that directory access succeeds when using the native engine, you must set the `-is-file-extension-check-on-directories-enabled` parameter to `true` when creating the scope.

With this parameter set to `true`, extension checks happen for directory operations and the decision whether to allow or deny access is taken based on the extensions included or excluded in the FPolicy scope configuration.

## Complete the FPolicy policy worksheet

You can use this worksheet to record the values that you need during the FPolicy policy configuration process. You should record whether you want to include each parameter setting in the FPolicy policy configuration and then record the value for the parameters that you want to include.

Type of information	Include	Your values
Storage virtual machine (SVM) name	Yes	
Policy name	Yes	
Event names	Yes	
Persistent store		
External engine name		
Is mandatory screening required?		
Allow privileged access		
Privileged user name		
Is passthrough-read enabled?		

## Plan the FPolicy scope configuration

### Plan the FPolicy scope configuration overview

Before you configure the FPolicy scope, you must understand what it means to create a scope. You must understand what the scope configuration contains. You also need to understand what the scope rules of precedence are. This information can help you plan the values that you want to set.

#### What it means to create an FPolicy scope

Creating the FPolicy scope means defining the boundaries on which the FPolicy policy applies. The storage virtual machine (SVM) is the basic 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 SVM you want to apply the scope.

There are a number of parameters that further restrict the scope within the specified SVM. You can restrict the scope by specifying what to include in the scope or by specifying what to exclude from the scope. After you

apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Notifications are generated for file access events where matches are found in the “include” options. Notifications are not generated for file access events where matches are found in the “exclude” options.

The FPolicy scope configuration defines the following configuration information:

- SVM name
- Policy name
- The shares to include or exclude from what gets monitored
- The export policies to include or exclude from what gets monitored
- The volumes to include or exclude from what gets monitored
- The file extensions to include or exclude from what gets monitored
- Whether to do file extension checks on directory objects



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 SVM. If the cluster administrator also creates the scope for that cluster FPolicy policy, the SVM 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 SVM administrator can create the scope for that cluster policy. If the SVM 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.

### What the scope rules of precedence are

The following rules of precedence apply to scope configurations:

- 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`.
- 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`.
- An administrator can specify both `-file-extensions-to-include` and `-file-extensions-to-exclude` lists.

The `-file-extensions-to-exclude` parameter is checked before the `-file-extensions-to-include` parameter is checked.

### What the FPolicy scope configuration contains

You can use the following list of available FPolicy scope configuration parameters to help you plan your configuration:



When configuring what shares, export policies, volumes, and file extensions to include or exclude from the scope, the include and exclude parameters can include metacharacters such as “?” and “\*”. The use of regular expressions is not supported.

Type of information	Option
<p><b>SVM</b></p> <p>Specifies the SVM name on which you want to create an FPolicy scope.</p> <p>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p><b>Policy name</b></p> <p>Specifies the name of the FPolicy policy to which you want to attach the scope. The FPolicy policy must already exist.</p>	<p><code>-policy-name policy_name</code></p>
<p><b>Shares to include</b></p> <p>Specifies a comma-delimited list of shares to monitor for the FPolicy policy to which the scope is applied.</p>	<p><code>-shares-to-include share_name, ...</code></p>
<p><b>Shares to exclude</b></p> <p>Specifies a comma-delimited list of shares to exclude from monitoring for the FPolicy policy to which the scope is applied.</p>	<p><code>-shares-to-exclude share_name, ...</code></p>
<p><b>Volumes to include</b> Specifies a comma-delimited list of volumes to monitor for the FPolicy policy to which the scope is applied.</p>	<p><code>-volumes-to-include volume_name, ...</code></p>
<p><b>Volumes to exclude</b></p> <p>Specifies a comma-delimited list of volumes to exclude from monitoring for the FPolicy policy to which the scope is applied.</p>	<p><code>-volumes-to-exclude volume_name, ...</code></p>
<p><b>Export policies to include</b></p> <p>Specifies a comma-delimited list of export policies to monitor for the FPolicy policy to which the scope is applied.</p>	<p><code>-export-policies-to -include export_policy_name, ...</code></p>
<p><b>Export policies to exclude</b></p> <p>Specifies a comma-delimited list of export policies to exclude from monitoring for the FPolicy policy to which the scope is applied.</p>	<p><code>-export-policies-to -exclude export_policy_name, ...</code></p>
<p><b>File extensions to include</b></p> <p>Specifies a comma-delimited list of file extensions to monitor for the FPolicy policy to which the scope is applied.</p>	<p><code>-file-extensions-to -include file_extensions, ...</code></p>

<p><i>File extension to exclude</i></p> <p>Specifies a comma-delimited list of file extensions to exclude from monitoring for the FPolicy policy to which the scope is applied.</p>	<pre>-file-extensions-to-exclude file_extensions, ...</pre>
<p><i>Is file extension check on directory enabled ?</i></p> <p>Specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to <code>true</code>, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to <code>false</code>, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match.</p> <p>If the FPolicy policy to which the scope is assigned is configured to use the native engine, this parameter must be set to <code>true</code>.</p>	<pre>-is-file-extension-check-on-directories-enabled {true  false}</pre>

## Complete the FPolicy scope worksheet

You can use this worksheet to record the values that you need during the FPolicy scope configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy scope.

You should record whether you want to include each parameter setting in the FPolicy scope configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage virtual machine (SVM) name	Yes	Yes	
Policy name	Yes	Yes	
Shares to include	No		
Shares to exclude	No		
Volumes to include	No		
Volumes to exclude	No		
Export policies to include	No		
Export policies to exclude	No		
File extensions to include	No		
File extension to exclude	No		

Is file extension check on directory enabled?	No		
---	----	--	--

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.