Plan the FPolicy external engine configuration

ONTAP 9

NetApp
November 29, 2021

Table of Contents

Plan the FPolicy external engine configuration

Before you configure the FPolicy external engine (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 (FPolicy servers), including the following information:

- storage virtual machine (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
- 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
SVM Specifies the SVM name that you want to associate with this external engine. 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.	`-vserver vserver_name`

Type of information	Option
Engine name 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. The name can be up to 256 characters long. The name should be up to 200 characters long if configuring the external engine name in a MetroCluster or SVM disaster recovery configuration. The name can contain any combination of the following ASCII-range characters: • `a` through `z` • `A` through `Z` • `0` through `9` • “_”, “-”, and “.”	`-engine-name engine_name`
Primary FPolicy servers 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. 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. 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.	`-primary-servers IP_address,...`
Port number Specifies the port number of the FPolicy service.	`-port integer`

Type of information	Option
Secondary FPolicy servers 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. 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.	`-secondary-servers IP_address,...`
External engine type Specifies whether the external engine operates in synchronous or asynchronous mode. By default, FPolicy operates in synchronous mode. When set to `synchronous`, 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. When set to `asynchronous`, file request processing sends a notification to the FPolicy server, and then continues.	`-extern-engine-type external_engine_type` The value for this parameter can be one of the following: • `synchronous` • `asynchronous`

Type of information	Option
SSL option for communication with FPolicy server 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: • When set to `no-auth`, no authentication takes place. The communication link is established over TCP. • When set to `server-auth`, the SVM authenticates the FPolicy server using SSL server authentication. • When set to `mutual-auth`, mutual authentication takes place between the SVM and the FPolicy server; the SVM authenticates the FPolicy server, and the FPolicy server authenticates the SVM. If you choose to configure mutual SSL authentication, then you must also configure the `-certificate-common-name`, `-certificate-serial`, and `-certifcate-ca` parameters.	`-ssl-option` {`no-auth`|`server-auth`|`mutual-auth`}
Certificate FQDN or custom common name 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. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-common-name` parameter.	`-certificate-common-name` `text`
Certificate serial number Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-serial` parameter.	`-certificate-serial` `text`

Type of information	Option
Certificate authority Specifies the CA name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certifcate-ca` parameter.	`-certifcate-ca text`

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
Timeout for canceling a request Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) that the node waits for a response from the FPolicy server. 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. 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`.	`-reqs-cancel-timeout integer`[h|m|s]
Timeout for aborting a request Specifies the timeout in hours (`h`), minutes (`m`), or seconds (`s`) for aborting a request. The range for this value is `0` through `200`.	`-reqs-abort-timeout ` `integer`[h|m|s]

Type of information	Option
Interval for sending status requests Specifies the interval in hours (`h`), minutes (`m`), or seconds (`s`) after which a status request is sent to the FPolicy server. 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`.	`-status-req-interval integer`[h|m|s]
Maximum outstanding requests on the FPolicy server Specifies the maximum number of outstanding requests that can be queued on the FPolicy server. The range for this value is `1` through `10000`. The default is `50`.	`-max-server-reqs integer`
Timeout for disconnecting a nonresponsive FPolicy server Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) after which the connection to the FPolicy server is terminated. 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. The range for this value is `1` through `100`. The default is `60s`.	`-server-progress-timeout integer`[h|m|s]
Interval for sending keep-alive messages to the FPolicy server Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) at which keep-alive messages are sent to the FPolicy server. Keep-alive messages detect half-open connections. 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`.	`-keep-alive-interval- integer`[h|m|s]

Type of information	Option
Maximum reconnect attempts Specifies the maximum number of times the SVM attempts to reconnect to the FPolicy server after the connection has been broken. The range for this value is `0` through `20`. The default is `5`.	`-max-connection-retries integer`
Receive buffer size 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.	`-recv-buffer-size integer`
Send buffer size Specifies the send 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 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.	`-send-buffer-size integer`

Type of information	Option
Timeout for purging a session ID during reconnection 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. 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. The default value is set to 10 seconds.	`-session-timeout` [`integer`h][`integer` m][`integer`s]

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 reenable 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		