



Manage FPolicy engine configuration

ONTAP 9.11.1 REST API reference

NetApp
May 08, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9111/ontap/protocols_fpolicy_svm.uuid_engines_endpoint_overview.html on May 08, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Manage FPolicy engine configuration 1
 - Protocols fpolicy svm.uuid engines endpoint overview 1
 - Retrieve an FPolicy engine configuration for all engines of an SVM 6
 - Create an FPolicy engine configuration for an SVM 18
 - Delete an FPolicy external engine configuration 34
 - Retrieve a particular FPolicy engine configuration for an SVM 36
 - Update a specific FPolicy engine configuration for an SVM 45

Manage FPolicy engine configuration

Protocols fpolicy svm.uuid engines endpoint overview

Overview

The FPolicy engine allows you to configure the external servers to which the file access notifications are sent. As part of FPolicy engine configuration, you can configure a server(s) to which the notification is sent, an optional set of secondary server(s) to which the notification is sent in the case of a primary server(s) failure, the port number for FPolicy application, the type of the engine, which is either synchronous or asynchronous and the format of the notifications, which is either xml or protobuf.

For the synchronous engine, ONTAP will wait for a response from the FPolicy application before it allows the operation. With an asynchronous engine, ONTAP proceeds with the operation processing after sending the notification to the FPolicy application. An engine can belong to multiple FPolicy policies. If the format is not specified, the default format, xml, is configured.

Examples

Creating an FPolicy engine

```
# The API:
POST /protocols/fpolicy/{svm.uuid}/engines

#The call:
curl -X POST "https://<mgmt-ip>/api/protocols/fpolicy/4f643fb4-fd21-11e8-ae49-0050568e2c1e/engines/" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"name\": \"engine0\", \"port\": 9876, \"primary_servers\": [ \"10.132.145.22\", \"10.140.101.109\" ], \"secondary_servers\": [ \"10.132.145.20\", \"10.132.145.21\" ], \"type\": \"synchronous\", \"format\": \"xml\", \"request_abort_timeout\": \"PT3M\", \"request_cancel_timeout\": \"PT29S\", \"server_progress_timeout\": \"PT1M\", \"status_request_interval\": \"PT23S\" }"

# The response:
{
  "num_records": 1,
  "records": [
    {
      "name": "engine0",
      "primary_servers": [
        "10.132.145.22",
        "10.140.101.109"
      ],
      "secondary_servers": [
        "10.132.145.20",
        "10.132.145.21"
      ],
      "port": 9876,
      "type": "synchronous",
      "format": "xml"
    }
  ]
}
```

Creating an FPolicy engine with the minimum required fields

```
# The API:
POST /protocols/fpolicy/{svm.uuid}/engines

#The call:
curl -X POST "https://<mgmt-ip>/api/protocols/fpolicy/4f643fb4-fd21-11e8-ae49-0050568e2c1e/engines/" -H "accept: application/json" -H "Content-Type: application/json" -d '{"name": "engine0", "port": 9876, "primary_servers": [ "10.132.145.22", "10.140.101.109" ], "type": "synchronous"}'

# The response:
{
  "num_records": 1,
  "records": [
    {
      "name": "engine0",
      "primary_servers": [
        "10.132.145.22",
        "10.140.101.109"
      ],
      "port": 9876,
      "type": "synchronous",
      "format": "xml"
    }
  ]
}
```

Retrieving an FPolicy engine configuration for a particular SVM

```
# The API:
GET /protocols/fpolicy/{svm.uuid}/engines

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/fpolicy/4f643fb4-fd21-11e8-ae49-0050568e2c1e/engines/?fields=*&return_records=true&return_timeout=15" -H "accept: application/json"

# The response:
{
  "records": [
    {
```

```

    "svm": {
      "uuid": "4f643fb4-fd21-11e8-ae49-0050568e2c1e"
    },
    "name": "cifs",
    "primary_servers": [
      "10.20.20.10"
    ],
    "port": 9876,
    "type": "synchronous"
  },
  {
    "svm": {
      "uuid": "4f643fb4-fd21-11e8-ae49-0050568e2c1e"
    },
    "name": "nfs",
    "primary_servers": [
      "10.23.140.64",
      "10.140.101.109"
    ],
    "secondary_servers": [
      "10.132.145.20",
      "10.132.145.22"
    ],
    "port": 9876,
    "type": "synchronous",
    "format": "xml",
    "ssl_option": "no_auth",
    "resiliency": {
      "enabled": false,
      "retention_duration": "PT3M"
    },
    "buffer_size": {
      "recv_buffer": 262144,
      "send_buffer": 1048576
    },
    "max_server_requests": 500,
    "request_cancel_timeout": "PT29S",
    "request_abort_timeout": "PT3M",
    "server_progress_timeout": "PT1M",
    "status_request_interval": "PT23S"
  }
],
"num_records": 2
}

```

Retrieving a specific FPolicy engine configuration for an SVM

```
# The Api:
GET /protocols/fpolicy/{svm.uuid}/engines/{name}

#The call:
curl -X GET "https://<mgmt-ip>/api/protocols/fpolicy/4f643fb4-fd21-11e8-ae49-0050568e2c1e/engines/cifs?fields=*" -H "accept: application/json"

# The response:
{
  "svm": {
    "uuid": "4f643fb4-fd21-11e8-ae49-0050568e2c1e"
  },
  "name": "cifs",
  "primary_servers": [
    "10.20.20.10"
  ],
  "port": 9876,
  "type": "synchronous",
  "format": "xml"
}
```

Updating an FPolicy engine for an SVM

```
# The API:
PATCH /protocols/fpolicy/{svm.uuid}/engines/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/fpolicy/4f643fb4-fd21-11e8-ae49-0050568e2c1e/engines/cifs" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"port\": 6666, \"secondary_servers\": [ \"10.132.145.20\", \"10.132.145.21\" ], \"type\": \"synchronous\"}"
```

Updating all the attributes of a specific FPolicy engine for an SVM

```
# The API:
PATCH /protocols/fpolicy/{svm.uuid}/engines/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/fpolicy/4f643fb4-fd21-11e8-ae49-0050568e2c1e/engines/cifs" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"port\": 9876, \"primary_servers\": [ \"10.132.145.20\", \"10.140.101.109\" ], \"secondary_servers\": [ \"10.132.145.23\", \"10.132.145.21\" ], \"type\": \"synchronous\", \"format\": \"protobuf\"}"
```

Deleting a specific FPolicy engine for an SVM

```
# The API:
DELETE /protocols/fpolicy/{svm.uuid}/engines/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/fpolicy/4f643fb4-fd21-11e8-ae49-0050568e2c1e/events/cifs" -H "accept: application/json"
```

Retrieve an FPolicy engine configuration for all engines of an SVM

GET /protocols/fpolicy/{svm.uuid}/engines

Introduced In: 9.6

Retrieves FPolicy engine configurations of all the engines for a specified SVM. ONTAP allows creation of cluster-level FPolicy engines that act as a template for all the SVMs belonging to the cluster. These cluster-level FPolicy engines are also retrieved for the specified SVM.

Related ONTAP commands

- `fpolicy policy external-engine show`

Learn more

- [DOC /protocols/fpolicy/{svm.uuid}/engines](#)

Parameters

Name	Type	In	Required	Description
buffer_size.send_buffer	integer	query	False	Filter by buffer_size.send_buffer <ul style="list-style-type: none">• Introduced in: 9.11
buffer_size.recv_buffer	integer	query	False	Filter by buffer_size.recv_buffer <ul style="list-style-type: none">• Introduced in: 9.11
max_server_requests	integer	query	False	Filter by max_server_requests <ul style="list-style-type: none">• Introduced in: 9.11• Max value: 10000• Min value: 1
primary_servers	string	query	False	Filter by primary_servers
request_cancel_timeout	string	query	False	Filter by request_cancel_timeout <ul style="list-style-type: none">• Introduced in: 9.11
name	string	query	False	Filter by name
resiliency.directory_path	string	query	False	Filter by resiliency.directory_path <ul style="list-style-type: none">• Introduced in: 9.11

Name	Type	In	Required	Description
resiliency.retention_duration	string	query	False	Filter by resiliency.retention_duration • Introduced in: 9.11
resiliency.enabled	boolean	query	False	Filter by resiliency.enabled • Introduced in: 9.11
format	string	query	False	Filter by format • Introduced in: 9.11
server_progress_timeout	string	query	False	Filter by server_progress_timeout • Introduced in: 9.11
ssl_option	string	query	False	Filter by ssl_option • Introduced in: 9.11
request_abort_timeout	string	query	False	Filter by request_abort_timeout • Introduced in: 9.11
certificate.serial_number	string	query	False	Filter by certificate.serial_number • Introduced in: 9.11
certificate.name	string	query	False	Filter by certificate.name • Introduced in: 9.11

Name	Type	In	Required	Description
certificate.ca	string	query	False	Filter by certificate.ca • Introduced in: 9.11
type	string	query	False	Filter by type
status_request_interval	string	query	False	Filter by status_request_interval • Introduced in: 9.11
port	integer	query	False	Filter by port
secondary_servers	string	query	False	Filter by secondary_servers
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Max value: 120 • Min value: 0 • Default value: 1
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[fpolicy_engine]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "certificate": {
      "ca": "TASample1",
      "name": "Sample1-FPolicy-Client",
      "serial_number": "8DDE112A114D1FBC"
    },
    "format": "xml",
    "max_server_requests": 500,
    "name": "fp_ex_eng",
    "port": 9876,
    "primary_servers": [
      "10.132.145.20",
      "10.140.101.109"
    ],
    "request_abort_timeout": "PT40S",
    "request_cancel_timeout": "PT20S",
    "resiliency": {
      "directory_path": "/dir1",
      "retention_duration": "PT3M"
    },
    "secondary_servers": [
      "10.132.145.20",
      "10.132.145.21"
    ],
    "server_progress_timeout": "PT1M",
    "ssl_option": "no_auth",
    "status_request_interval": "PT10S",
    "svm": {
      "uuid": "string"
    },
    "type": "synchronous"
  }
}
```

Error

Status: Default,

Name	Type	Description
error	error	

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

buffer_size

Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
recv_buffer	integer	Specifies the receive buffer size of the connected socket for the FPolicy server. Default value is 256KB.
send_buffer	integer	Specifies the send buffer size of the connected socket for the FPolicy server. Default value 1MB.

certificate

Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
ca	string	Specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.
name	string	Specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the SVM and the FPolicy server is configured.

Name	Type	Description
serial_number	string	Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

resiliency

If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.

Name	Type	Description
directory_path	string	Specifies the directory path under the SVM namespace, where notifications are stored in the files whenever a network outage happens.
enabled	boolean	Specifies whether the resiliency feature is enabled or not. Default is false.
retention_duration	string	Specifies the ISO-8601 duration, for which the notifications are written to files inside the storage controller during a network outage. The value for this field must be between 0 and 600 seconds. Default is 180 seconds.

svm

Name	Type	Description
uuid	string	SVM UUID

fpolicy_engine

Defines how ONTAP makes and manages connections to external FPolicy servers.

Name	Type	Description
buffer_size	buffer_size	Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
certificate	certificate	Provides details about certificate used to authenticate the FPolicy server.
format	string	<p>The format for the notification messages sent to the FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • xml - Notifications sent to the FPolicy server will be formatted using the XML schema. • protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.
max_server_requests	integer	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 value can be 500 , 1000 or 2000 depending on the hardware platform.
name	string	Specifies the name to assign to the external server configuration.
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.

Name	Type	Description
resiliency	resiliency	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.

Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> • no_auth When set to "no_auth", no authentication takes place. • server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. 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 SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM 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 SVM.
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>
svm	svm	

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.6

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create an FPolicy engine configuration for an SVM

POST /protocols/fpolicy/{svm.uuid}/engines

Introduced In: 9.6

Creates an FPolicy engine configuration for a specified SVM. FPolicy engine creation is allowed only on data

SVMs.

Required properties

- `svm.uuid` - Existing SVM in which to create the FPolicy engine.
- `name` - Name of external engine.
- `port` - Port number of the FPolicy server application.
- `primary_servers` - List of primary FPolicy servers to which the node will send notifications.

Recommended optional properties

- `secondary_servers` - It is recommended to configure secondary FPolicy server to which the node will send notifications when the primary server is down.

Default property values

- `type` - *synchronous*
- `format` - *xml*

Related ONTAP commands

- `fpolicy policy external-engine create`

Learn more

- [DOC /protocols/fpolicy/{svm.uuid}/engines](#)

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. <ul style="list-style-type: none">• Default value:
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
buffer_size	buffer_size	Specifies the send and receive buffer size of the connected socket for the FPolicy server.
certificate	certificate	Provides details about certificate used to authenticate the Fpolicy server.
format	string	<p>The format for the notification messages sent to the FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • xml - Notifications sent to the FPolicy server will be formatted using the XML schema. • protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.
max_server_requests	integer	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 value can be 500 , 1000 or 2000 depending on the hardware platform.
name	string	Specifies the name to assign to the external server configuration.
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.

Name	Type	Description
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.
resiliency	resiliency	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.

Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> • no_auth When set to "no_auth", no authentication takes place. • server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. 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 SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM 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 SVM.
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>
svm	svm	

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.6

Example request

```
{
  "certificate": {
    "ca": "TASample1",
    "name": "Sample1-FPolicy-Client",
    "serial_number": "8DDE112A114D1FBC"
  },
  "format": "xml",
  "max_server_requests": 500,
  "name": "fp_ex_eng",
  "port": 9876,
  "primary_servers": [
    "10.132.145.20",
    "10.140.101.109"
  ],
  "request_abort_timeout": "PT40S",
  "request_cancel_timeout": "PT20S",
  "resiliency": {
    "directory_path": "/dir1",
    "retention_duration": "PT3M"
  },
  "secondary_servers": [
    "10.132.145.20",
    "10.132.145.21"
  ],
  "server_progress_timeout": "PT1M",
  "ssl_option": "no_auth",
  "status_request_interval": "PT10S",
  "svm": {
    "uuid": "string"
  },
  "type": "synchronous"
}
```

Response

Status: 201, Created

Name	Type	Description
_links	_links	

Name	Type	Description
num_records	integer	Number of records
records	array[fpolicy_engine]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "certificate": {
      "ca": "TASample1",
      "name": "Sample1-FPolicy-Client",
      "serial_number": "8DDE112A114D1FBC"
    },
    "format": "xml",
    "max_server_requests": 500,
    "name": "fp_ex_eng",
    "port": 9876,
    "primary_servers": [
      "10.132.145.20",
      "10.140.101.109"
    ],
    "request_abort_timeout": "PT40S",
    "request_cancel_timeout": "PT20S",
    "resiliency": {
      "directory_path": "/dir1",
      "retention_duration": "PT3M"
    },
    "secondary_servers": [
      "10.132.145.20",
      "10.132.145.21"
    ],
    "server_progress_timeout": "PT1M",
    "ssl_option": "no_auth",
    "status_request_interval": "PT10S",
    "svm": {
      "uuid": "string"
    },
    "type": "synchronous"
  }
}
```

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
9764885	The primary secondary server has a redundant IP address
9764953	The name of the FPolicy engine is "native" which is reserved by the system

Name	Type	Description
error	error	

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

buffer_size

Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
recv_buffer	integer	Specifies the receive buffer size of the connected socket for the FPolicy server. Default value is 256KB.
send_buffer	integer	Specifies the send buffer size of the connected socket for the FPolicy server. Default value 1MB.

certificate

Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
ca	string	Specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.
name	string	Specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the SVM and the FPolicy server is configured.
serial_number	string	Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

resiliency

If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.

Name	Type	Description
directory_path	string	Specifies the directory path under the SVM namespace, where notifications are stored in the files whenever a network outage happens.
enabled	boolean	Specifies whether the resiliency feature is enabled or not. Default is false.
retention_duration	string	Specifies the ISO-8601 duration, for which the notifications are written to files inside the storage controller during a network outage. The value for this field must be between 0 and 600 seconds. Default is 180 seconds.

svm

Name	Type	Description
uuid	string	SVM UUID

fpolicy_engine

Defines how ONTAP makes and manages connections to external FPolicy servers.

Name	Type	Description
buffer_size	buffer_size	Specifies the send and receive buffer size of the connected socket for the FPolicy server.
certificate	certificate	Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
format	string	<p>The format for the notification messages sent to the FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • xml - Notifications sent to the FPolicy server will be formatted using the XML schema. • protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.
max_server_requests	integer	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 value can be 500 , 1000 or 2000 depending on the hardware platform.
name	string	Specifies the name to assign to the external server configuration.
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.

Name	Type	Description
resiliency	resiliency	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.

Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> • no_auth When set to "no_auth", no authentication takes place. • server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. 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 SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM 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 SVM.
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>
svm	svm	

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.6

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Delete an FPolicy external engine configuration

DELETE /protocols/fpolicy/{svm.uuid}/engines/{name}

Introduced In: 9.6

Deletes the FPolicy external engine configuration. Deletion of an FPolicy engine that is attached to one or more FPolicy policies is not allowed.

Related ONTAP commands

- `fpolicy policy external-engine modify`

Learn more

- [DOC /protocols/fpolicy/{svm.uuid}/engines](#)

Parameters

Name	Type	In	Required	Description
name	string	path	True	
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
9764940	At least one FPolicy policy is using the FPolicy engine
9764887	The FPolicy engine is a cluster level FPolicy engine

Name	Type	Description
error	error	

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve a particular FPolicy engine configuration for an SVM

GET /protocols/fpolicy/{svm.uuid}/engines/{name}

Introduced In: 9.6

Retrieves a particular FPolicy engine configuration of a specified SVM. A cluster-level FPolicy engine configuration cannot be retrieved for a data SVM.

Related ONTAP commands

- `fpolicy policy external-engine show`

Learn more

- [DOC /protocols/fpolicy/{svm.uuid}/engines](#)

Parameters

Name	Type	In	Required	Description
name	string	path	True	

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
buffer_size	buffer_size	Specifies the send and receive buffer size of the connected socket for the FPolicy server.
certificate	certificate	Provides details about certificate used to authenticate the Fpolicy server.
format	string	<p>The format for the notification messages sent to the FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • xml - Notifications sent to the FPolicy server will be formatted using the XML schema. • protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.
max_server_requests	integer	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 value can be 500 , 1000 or 2000 depending on the hardware platform.
name	string	Specifies the name to assign to the external server configuration.

Name	Type	Description
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.
resiliency	resiliency	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.

Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> • no_auth When set to "no_auth", no authentication takes place. • server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. 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 SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM 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 SVM.
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>
svm	svm	

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.6

Example response

```
{
  "certificate": {
    "ca": "TASample1",
    "name": "Sample1-FPolicy-Client",
    "serial_number": "8DDE112A114D1FBC"
  },
  "format": "xml",
  "max_server_requests": 500,
  "name": "fp_ex_eng",
  "port": 9876,
  "primary_servers": [
    "10.132.145.20",
    "10.140.101.109"
  ],
  "request_abort_timeout": "PT40S",
  "request_cancel_timeout": "PT20S",
  "resiliency": {
    "directory_path": "/dir1",
    "retention_duration": "PT3M"
  },
  "secondary_servers": [
    "10.132.145.20",
    "10.132.145.21"
  ],
  "server_progress_timeout": "PT1M",
  "ssl_option": "no_auth",
  "status_request_interval": "PT10S",
  "svm": {
    "uuid": "string"
  },
  "type": "synchronous"
}
```

Error

Status: Default, Error

Name	Type	Description
error	error	

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

buffer_size

Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
recv_buffer	integer	Specifies the receive buffer size of the connected socket for the FPolicy server. Default value is 256KB.
send_buffer	integer	Specifies the send buffer size of the connected socket for the FPolicy server. Default value 1MB.

certificate

Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
ca	string	Specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.
name	string	Specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the SVM and the FPolicy server is configured.
serial_number	string	Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

resiliency

If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.

Name	Type	Description
directory_path	string	Specifies the directory path under the SVM namespace, where notifications are stored in the files whenever a network outage happens.
enabled	boolean	Specifies whether the resiliency feature is enabled or not. Default is false.
retention_duration	string	Specifies the ISO-8601 duration, for which the notifications are written to files inside the storage controller during a network outage. The value for this field must be between 0 and 600 seconds. Default is 180 seconds.

svm

Name	Type	Description
uuid	string	SVM UUID

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update a specific FPolicy engine configuration for an SVM

PATCH /protocols/fpolicy/{svm.uuid}/engines/{name}

Introduced In: 9.6

Updates a specific FPolicy engine configuration of an SVM. Modification of an FPolicy engine that is attached to one or more enabled FPolicy policies is not allowed.

Related ONTAP commands

- `fpolicy policy external-engine modify`

Learn more

- [DOC /protocols/fpolicy/{svm.uuid}/engines](#)

Parameters

Name	Type	In	Required	Description
name	string	path	True	
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
buffer_size	buffer_size	Specifies the send and receive buffer size of the connected socket for the FPolicy server.
certificate	certificate	Provides details about certificate used to authenticate the Fpolicy server.
format	string	The format for the notification messages sent to the FPolicy servers. The possible values are: <ul style="list-style-type: none">• xml - Notifications sent to the FPolicy server will be formatted using the XML schema.• protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.

Name	Type	Description
max_server_requests	integer	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 value can be 500 , 1000 or 2000 depending on the hardware platform.
name	string	Specifies the name to assign to the external server configuration.
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.
resiliency	resiliency	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.

Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> • no_auth When set to "no_auth", no authentication takes place. • server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. 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 SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM 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 SVM.
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>
svm	svm	

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.6

Example request

```
{
  "certificate": {
    "ca": "TASample1",
    "name": "Sample1-FPolicy-Client",
    "serial_number": "8DDE112A114D1FBC"
  },
  "format": "xml",
  "max_server_requests": 500,
  "name": "fp_ex_eng",
  "port": 9876,
  "primary_servers": [
    "10.132.145.20",
    "10.140.101.109"
  ],
  "request_abort_timeout": "PT40S",
  "request_cancel_timeout": "PT20S",
  "resiliency": {
    "directory_path": "/dir1",
    "retention_duration": "PT3M"
  },
  "secondary_servers": [
    "10.132.145.20",
    "10.132.145.21"
  ],
  "server_progress_timeout": "PT1M",
  "ssl_option": "no_auth",
  "status_request_interval": "PT10S",
  "svm": {
    "uuid": "string"
  },
  "type": "synchronous"
}
```

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
9764922	The primary and secondary server has a redundant IP address
9764942	At least one FPolicy policy is using the FPolicy engine
9764886	FPolicy engine is a cluster-level FPolicy engine

Name	Type	Description
error	error	

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

buffer_size

Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
recv_buffer	integer	Specifies the receive buffer size of the connected socket for the FPolicy server. Default value is 256KB.
send_buffer	integer	Specifies the send buffer size of the connected socket for the FPolicy server. Default value 1MB.

certificate

Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
ca	string	Specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.
name	string	Specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the SVM and the FPolicy server is configured.
serial_number	string	Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

resiliency

If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.

Name	Type	Description
directory_path	string	Specifies the directory path under the SVM namespace, where notifications are stored in the files whenever a network outage happens.
enabled	boolean	Specifies whether the resiliency feature is enabled or not. Default is false.
retention_duration	string	Specifies the ISO-8601 duration, for which the notifications are written to files inside the storage controller during a network outage. The value for this field must be between 0 and 600 seconds. Default is 180 seconds.

svm

Name	Type	Description
uuid	string	SVM UUID

fpolicy_engine

Defines how ONTAP makes and manages connections to external FPolicy servers.

Name	Type	Description
buffer_size	buffer_size	Specifies the send and receive buffer size of the connected socket for the FPolicy server.
certificate	certificate	Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
format	string	<p>The format for the notification messages sent to the FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • xml - Notifications sent to the FPolicy server will be formatted using the XML schema. • protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.
max_server_requests	integer	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 value can be 500 , 1000 or 2000 depending on the hardware platform.
name	string	Specifies the name to assign to the external server configuration.
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.

Name	Type	Description
resiliency	resiliency	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.

Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> • no_auth When set to "no_auth", no authentication takes place. • server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. 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 SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM 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 SVM.
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>
svm	svm	

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.6

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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.