Manage FPolicy configuration

ONTAP 9.14.1 REST API reference

NetApp
May 23, 2024

Table of Contents

Manage FPolicy configuration

Protocols fpolicy endpoint overview

Overview

FPolicy is an infrastructure component of ONTAP that enables partner applications to connect to ONTAP in order to monitor and set file access permissions. Every time a client accesses a file from a storage system, based on the configuration of FPolicy, the partner application is notified about file access. This enables partners to set restrictions on files that are created or accessed on the storage system. FPolicy also allows you to create file policies that specify file operation permissions according to file type. For example, you can restrict certain file types, such as .jpeg and .mp3 files, from being stored on the storage system. FPolicy can monitor file access from CIFS and NFS clients.

As part of FPolicy configuration, you can specify an FPolicy engine which defines the external FPolicy server, FPolicy events, which defines the protocol and file operations to monitor and the FPolicy policy that acts as a container for the FPolicy engine and FPolicy events. It provides a way for policy management functions, such as policy enabling and disabling.

Examples

Creating an FPolicy configuration

To create an FPolicy for an SVM use the following API. Note that the *return_records=true* query parameter is used to obtain the newly created entry in the response.

```
# The API:
POST /protocols/fpolicy/

#The call:
curl -X POST "https://<mgmt-ip>/api/protocols/fpolicy?return_records=true"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\"engines\": [ { \"name\": \"engine1\", \"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\" } ], \"events\": [ {
\"file_operations\": { \"read\": true, \"write\": true }, \"filters\": {
\"monitor_ads\": true }, \"name\": \"event_cifs\", \"protocol\": \"cifs\",
\"volume_monitoring\": true } ], \"policies\": [ { \"engine\": { \"name\":
\"engine1\" }, \"events\": [ { \"name\": \"event_cifs\" } ],
\"mandatory\": true, \"name\": \"pol0\", \"priority\": 1, \"scope\": {
\"include_volumes\": [ \"vol1\" ] } } ], \"persistent_stores\": [ {
\"name\": \"ps1\", \"volume\": \"psvol\" } ], \"svm\": { \"name\":
\"vs1\", \"uuid\": \"b34f5e3d-01d0-11e9-8f63-0050568ea311\" }}"

# The response:
{
"num_records": 1,
```

```
"records": [
  {
    "svm": {
      "uuid": "b34f5e3d-01d0-11e9-8f63-0050568ea311",
      "name": "vs1"
    },
    "engines": [
      {
        "name": "engine1",
        "primary_servers": [
          "10.132.145.22",
          "10.140.101.109"
        ],
        "secondary_servers": [
          "10.132.145.20",
          "10.132.145.21"
        ],
        "type": "synchronous",
        "port": 9876,
        "format": "xml"
      }
    ],
      "events": [
      {
        "name": "event_cifs",
        "protocol": "cifs",
        "volume_monitoring": true,
        "file_operations": {
          "read": true,
          "write": true
        },
        "filters": {
          "monitor_ads": true
        }
      }
    ],
    "policies": [
      {
        "name": "pol0",
        "priority": 1,
        "events": [
          {
            "name": "event_cifs"
          }
        ],
        "engine": {
```

```
          "name": "engine1"
        },
        "scope": {
          "include_volumes": [
            "vol1"
          ]
        },
        "mandatory": true
      }
    ],
    "persistent_stores": [
      {
        "name": "ps1",
        "volume": "psvol",
      }
    ]
  }
]
}
```

Retrieving the FPolicy configuration for all the SVMs in the cluster

```
# The API:
GET /protocols/fpolicy

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/fpolicy?fields=*&return_records=true&return_timeout=15"
-H "accept: application/json"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "b34f5e3d-01d0-11e9-8f63-0050568ea311",
      "name": "vs1"
    },
    "engines": [
      {
        "name": "engine1",
        "primary_servers": [
```

```
          "10.132.145.22",
          "10.140.101.109"
        ],
        "secondary_servers": [
          "10.132.145.20",
          "10.132.145.21"
        ],
        "type": "synchronous",
        "port": 9876,
        "format": "xml"
      }
    ],
    "events": [
      {
        "name": "event_cifs",
        "protocol": "cifs",
        "volume_monitoring": true,
        "file_operations": {
          "close": false,
          "create": false,
          "create_dir": false,
          "delete": false,
          "delete_dir": false,
          "getattr": false,
          "link": false,
          "lookup": false,
          "open": false,
          "read": true,
          "write": true,
          "rename": false,
          "rename_dir": false,
          "setattr": false,
          "symlink": false
        },
        "filters": {
          "monitor_ads": true,
          "close_with_modification": false,
          "close_without_modification": false,
          "close_with_read": false,
          "first_read": false,
          "first_write": false,
          "offline_bit": false,
          "open_with_delete_intent": false,
          "open_with_write_intent": false,
          "write_with_size_change": false,
          "setattr_with_owner_change": false,
```

```
          "setattr_with_group_change": false,
          "setattr_with_sacl_change": false,
          "setattr_with_dacl_change": false,
          "setattr_with_modify_time_change": false,
          "setattr_with_access_time_change": false,
          "setattr_with_creation_time_change": false,
          "setattr_with_mode_change": false,
          "setattr_with_size_change": false,
          "setattr_with_allocation_size_change": false,
          "exclude_directory": false
        }
      }
    ],
    "policies": [
      {
        "name": "pol0",
        "enabled": true,
        "priority": 1,
        "events": [
          {
            "name": "event_cifs"
          }
        ],
        "engine": {
          "name": "engine1"
        },
        "scope": {
          "include_volumes": [
            "vol1"
          ]
        },
        "mandatory": true,
        "passthrough_read": false,
        "allow_privileged_access": false,
        "persistent_store": "ps1"
      }
    ],
    "persistent_stores": [
      {
        "name": "ps1",
        "volume": "psvol",
      }
    ]
  }
],
"num_records": 1
```

```
}
```

Retrieving an FPolicy configuration for a particular SVM

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

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/fpolicy/b34f5e3d-01d0-11e9-
8f63-0050568ea311?fields=*&return_records=true&return_timeout=15" -H
"accept: application/json"

# The response:
{
"svm": {
  "uuid": "b34f5e3d-01d0-11e9-8f63-0050568ea311",
  "name": "vs1"
},
"engines": [
  {
    "name": "engine1",
    "primary_servers": [
      "10.132.145.22",
      "10.140.101.109"
    ],
    "secondary_servers": [
      "10.132.145.20",
      "10.132.145.21"
    ],
    "type": "synchronous",
    "port": 9876,
    "format": "xml"
  }
],
"events": [
  {
    "name": "event_cifs",
    "protocol": "cifs",
    "volume_monitoring": true,
    "file_operations": {
      "close": false,
      "create": false,
```

```
      "create_dir": false,
      "delete": false,
      "delete_dir": false,
      "getattr": false,
      "link": false,
      "lookup": false,
      "open": false,
      "read": true,
      "write": true,
      "rename": false,
      "rename_dir": false,
      "setattr": false,
      "symlink": false
    },
    "filters": {
      "monitor_ads": true,
      "close_with_modification": false,
      "close_without_modification": false,
      "close_with_read": false,
      "first_read": false,
      "first_write": false,
      "offline_bit": false,
      "open_with_delete_intent": false,
      "open_with_write_intent": false,
      "write_with_size_change": false,
      "setattr_with_owner_change": false,
      "setattr_with_group_change": false,
      "setattr_with_sacl_change": false,
      "setattr_with_dacl_change": false,
      "setattr_with_modify_time_change": false,
      "setattr_with_access_time_change": false,
      "setattr_with_creation_time_change": false,
      "setattr_with_mode_change": false,
      "setattr_with_size_change": false,
      "setattr_with_allocation_size_change": false,
      "exclude_directory": false
    }
  }
],
"policies": [
  {
    "name": "pol0",
    "enabled": true,
    "priority": 1,
    "events": [
      {
```

```
        "name": "event_cifs"
      }
    ],
    "engine": {
      "name": "engine1"
    },
    "scope": {
      "include_volumes": [
        "vol1"
      ]
    },
    "mandatory": true,
    "passthrough_read": false,
    "allow_privileged_access": false,
    "persistent_store": "ps1"
  }
],
"persistent_stores": [
  {
    "name": "ps1",
    "volume": "psvol",
  }
]
}
```

Deleting an FPolicy configuration for a particular SVM

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

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/fpolicy/b34f5e3d-01d0-
11e9-8f63-0050568ea311" -H "accept: application/json"
```

Retrieve an FPolicy configuration

GET `/protocols/fpolicy`

Introduced In: 9.6

Retrieves an FPolicy configuration.

Related ONTAP commands

- `fpolicy show`
- `fpolicy policy show`
- `fpolicy policy scope show`
- `fpolicy policy event show`
- `fpolicy policy external-engine show`
- `fpolicy persistent-store show`

Learn more

- DOC /protocols/fpolicy

Parameters

Name	Type	In	Required	Description
persistent_stores.name	string	query	False	Filter by persistent_stores.name • Introduced in: 9.14
persistent_stores.volume	string	query	False	Filter by persistent_stores.volume • Introduced in: 9.14
svm.uuid	string	query	False	Filter by svm.uuid
svm.name	string	query	False	Filter by svm.name
engines.certificate.serial_number	string	query	False	Filter by engines.certificate.serial_number • Introduced in: 9.11

Name	Type	In	Required	Description
engines.certificate.name	string	query	False	Filter by engines.certificate.name • Introduced in: 9.11
engines.certificate.ca	string	query	False	Filter by engines.certificate.ca • Introduced in: 9.11
engines.max_server_requests	integer	query	False	Filter by engines.max_server_requests • Introduced in: 9.11 • Max value: 10000 • Min value: 1
engines.server_progress_timeout	string	query	False	Filter by engines.server_progress_timeout • Introduced in: 9.11
engines.request_cancel_timeout	string	query	False	Filter by engines.request_cancel_timeout • Introduced in: 9.11
engines.request_abort_timeout	string	query	False	Filter by engines.request_abort_timeout • Introduced in: 9.11

Name	Type	In	Required	Description
engines.resiliency.directory_path	string	query	False	Filter by engines.resiliency.directory_path • Introduced in: 9.11
engines.resiliency.enabled	boolean	query	False	Filter by engines.resiliency.enabled • Introduced in: 9.11
engines.resiliency.retention_duration	string	query	False	Filter by engines.resiliency.retention_duration • Introduced in: 9.11
engines.primary_servers	string	query	False	Filter by engines.primary_servers
engines.port	integer	query	False	Filter by engines.port
engines.name	string	query	False	Filter by engines.name
engines.format	string	query	False	Filter by engines.format • Introduced in: 9.11
engines.keep_alive_interval	string	query	False	Filter by engines.keep_alive_interval • Introduced in: 9.13

Name	Type	In	Required	Description
engines.status_request_interval	string	query	False	Filter by engines.status_request_interval • Introduced in: 9.11
engines.secondary_servers	string	query	False	Filter by engines.secondary_servers
engines.ssl_option	string	query	False	Filter by engines.ssl_option • Introduced in: 9.11
engines.type	string	query	False	Filter by engines.type
engines.buffer_size.recv_buffer	integer	query	False	Filter by engines.buffer_size.recv_buffer • Introduced in: 9.11 • Max value: 7895160 • Min value: 0
engines.buffer_size.send_buffer	integer	query	False	Filter by engines.buffer_size.send_buffer • Introduced in: 9.11 • Max value: 7895160 • Min value: 0
policies.allow_privileged_access	boolean	query	False	Filter by policies.allow_privileged_access • Introduced in: 9.13

Name	Type	In	Required	Description
policies.name	string	query	False	Filter by policies.name
policies.persistent_store	string	query	False	Filter by policies.persistent_store • Introduced in: 9.14
policies.privileged_user	string	query	False	Filter by policies.privileged_user • Introduced in: 9.11
policies.priority	integer	query	False	Filter by policies.priority • Max value: 10 • Min value: 1
policies.scope.object_monitoring_with_no_extension	boolean	query	False	Filter by policies.scope.object_monitoring_with_no_extension • Introduced in: 9.11
policies.scope.exclude_export_policies	string	query	False	Filter by policies.scope.exclude_export_policies
policies.scope.include_export_policies	string	query	False	Filter by policies.scope.include_export_policies
policies.scope.check_extensions_on_directories	boolean	query	False	Filter by policies.scope.check_extensions_on_directories • Introduced in: 9.11

Name	Type	In	Required	Description
policies.scope.exclude_shares	string	query	False	Filter by policies.scope.exclude_shares
policies.scope.exclude_extension	string	query	False	Filter by policies.scope.exclude_extension
policies.scope.exclude_volumes	string	query	False	Filter by policies.scope.exclude_volumes
policies.scope.include_shares	string	query	False	Filter by policies.scope.include_shares
policies.scope.include_volumes	string	query	False	Filter by policies.scope.include_volumes
policies.scope.include_extension	string	query	False	Filter by policies.scope.include_extension
policies.passthrough_read	boolean	query	False	Filter by policies.passthrough_read • Introduced in: 9.11
policies.events.name	string	query	False	Filter by policies.events.name
policies.engine.name	string	query	False	Filter by policies.engine.name
policies.enabled	boolean	query	False	Filter by policies.enabled
policies.mandatory	boolean	query	False	Filter by policies.mandatory

Name	Type	In	Required	Description
events.filters.exclude_directory	boolean	query	False	Filter by events.filters.exclude_directory
events.filters.write_with_size_change	boolean	query	False	Filter by events.filters.write_with_size_change
events.filters.monitor_ads	boolean	query	False	Filter by events.filters.monitor_ads
events.filters.setattr_with_dacl_change	boolean	query	False	Filter by events.filters.setattr_with_dacl_change
events.filters.offline_bit	boolean	query	False	Filter by events.filters.offline_bit
events.filters.open_with_delete_intent	boolean	query	False	Filter by events.filters.open_with_delete_intent
events.filters.setattr_with_creation_time_change	boolean	query	False	Filter by events.filters.setattr_with_creation_time_change
events.filters.first_read	boolean	query	False	Filter by events.filters.first_read
events.filters.setattr_with_mode_change	boolean	query	False	Filter by events.filters.setattr_with_mode_change
events.filters.close_with_modification	boolean	query	False	Filter by events.filters.close_with_modification
events.filters.first_write	boolean	query	False	Filter by events.filters.first_write

Name	Type	In	Required	Description
events.filters.close_without_modification	boolean	query	False	Filter by events.filters.close_without_modification
events.filters.setattr_with_access_time_change	boolean	query	False	Filter by events.filters.setattr_with_access_time_change
events.filters.setattr_with_modify_time_change	boolean	query	False	Filter by events.filters.setattr_with_modify_time_change
events.filters.setattr_with_owner_change	boolean	query	False	Filter by events.filters.setattr_with_owner_change
events.filters.setattr_with_size_change	boolean	query	False	Filter by events.filters.setattr_with_size_change
events.filters.setattr_with_allocation_size_change	boolean	query	False	Filter by events.filters.setattr_with_allocation_size_change
events.filters.close_with_read	boolean	query	False	Filter by events.filters.close_with_read
events.filters.setattr_with_group_change	boolean	query	False	Filter by events.filters.setattr_with_group_change
events.filters.open_with_write_intent	boolean	query	False	Filter by events.filters.open_with_write_intent
events.filters.setattr_with_sacl_change	boolean	query	False	Filter by events.filters.setattr_with_sacl_change

Name	Type	In	Required	Description
events.file_operations.access	boolean	query	False	Filter by events.file_operations.access • Introduced in: 9.13
events.file_operations.rename_dir	boolean	query	False	Filter by events.file_operations.rename_dir
events.file_operations.read	boolean	query	False	Filter by events.file_operations.read
events.file_operations.delete_dir	boolean	query	False	Filter by events.file_operations.delete_dir
events.file_operations.create	boolean	query	False	Filter by events.file_operations.create
events.file_operations.create_dir	boolean	query	False	Filter by events.file_operations.create_dir
events.file_operations.open	boolean	query	False	Filter by events.file_operations.open
events.file_operations.getattr	boolean	query	False	Filter by events.file_operations.getattr
events.file_operations.setattr	boolean	query	False	Filter by events.file_operations.setattr
events.file_operations.write	boolean	query	False	Filter by events.file_operations.write
events.file_operations.close	boolean	query	False	Filter by events.file_operations.close

Name	Type	In	Required	Description
events.file_operations.delete	boolean	query	False	Filter by events.file_operations.delete
events.file_operations.symlink	boolean	query	False	Filter by events.file_operations.symlink
events.file_operations.rename	boolean	query	False	Filter by events.file_operations.rename
events.file_operations.link	boolean	query	False	Filter by events.file_operations.link
events.file_operations.lookup	boolean	query	False	Filter by events.file_operations.lookup
events.volume_monitoring	boolean	query	False	Filter by events.volume_monitoring
events.monitor_fileop_failure	boolean	query	False	Filter by events.monitor_fileop_failure • Introduced in: 9.13
events.name	string	query	False	Filter by events.name
events.protocol	string	query	False	Filter by events.protocol
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
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
return_timeout	integer	query	False	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. • 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]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "engines": {
      "certificate": {
        "ca": "TASample1",
        "name": "Sample1-FPolicy-Client",
        "serial_number": "8DDE112A114D1FBC"
      },
      "format": "xml",
      "keep_alive_interval": "PT2M",
      "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",
```

```
      "type": "synchronous"
    },
    "events": {
      "name": "event_cifs",
      "protocol": "cifs"
    },
    "persistent_stores": {
      "name": "ps1",
      "volume": "psvol"
    },
    "policies": {
      "engine": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        }
      },
      "events": [
        "event_cifs",
        "event_open"
      ],
      "name": "fp_policy_1",
      "persistent_store": "ps1",
      "priority": 1,
      "privileged_user": "mydomain\\testuser",
      "scope": {
        "exclude_export_policies": {
        },
        "exclude_extension": {
        },
        "exclude_shares": {
        },
        "exclude_volumes": [
          "vol1",
          "vol_svm1",
          "*"
        ],
        "include_export_policies": {
        },
        "include_extension": {
        },
        "include_shares": [
          "sh1",
          "share_cifs"
        ],
```

```
        "include_volumes": [
          "vol1",
          "vol_svm1"
        ]
      }
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_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	

_links

Name	Type	Description
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	Type	Description
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.

fpolicy_engines

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	The format for the notification messages sent to the FPolicy servers. The possible values are: • 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.
keep_alive_interval	string	Specifies the ISO-8601 interval time for a storage appliance to send Keep Alive message to an FPolicy server. The allowed range is between 10 to 600 seconds.
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 values are 500, 1000 or 2000 for Low-end(<64 GB memory), Mid-end(>=64 GB memory) and High-end(>=128 GB memory) Platforms respectively.
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]	

Name	Type	Description
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	Specifies the SSL option for external communication with the FPolicy server. Possible values include the following: • no_auth When set to "no_auth", no authentication takes place. • 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	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.

Name	Type	Description
type	string	The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are: • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.10 ◦ x-nullable: true

file_operations

Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.

Name	Type	Description
access	boolean	Access operations
close	boolean	File close operations
create	boolean	File create operations
create_dir	boolean	Directory create operations
delete	boolean	File delete operations
delete_dir	boolean	Directory delete operations
getattr	boolean	Get attribute operations
link	boolean	Link operations
lookup	boolean	Lookup operations
open	boolean	File open operations

Name	Type	Description
read	boolean	File read operations
rename	boolean	File rename operations
rename_dir	boolean	Directory rename operations
setattr	boolean	Set attribute operations
symlink	boolean	Symbolic link operations
write	boolean	File write operations

filters

Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.

Name	Type	Description
close_with_modification	boolean	Filter the client request for close with modification.
close_with_read	boolean	Filter the client request for close with read.
close_without_modification	boolean	Filter the client request for close without modification.
exclude_directory	boolean	Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.
first_read	boolean	Filter the client requests for the first-read.
first_write	boolean	Filter the client requests for the first-write.
monitor_ads	boolean	Filter the client request for alternate data stream.
offline_bit	boolean	Filter the client request for offline bit set. FPolicy server receives notification only when offline files are accessed.

Name	Type	Description
open_with_delete_intent	boolean	Filter the client request for open with delete intent.
open_with_write_intent	boolean	Filter the client request for open with write intent.
setattr_with_access_time_change	boolean	Filter the client setattr requests for changing the access time of a file or directory.
setattr_with_allocation_size_change	boolean	Filter the client setattr requests for changing the allocation size of a file.
setattr_with_creation_time_change	boolean	Filter the client setattr requests for changing the creation time of a file or directory.
setattr_with_dacl_change	boolean	Filter the client setattr requests for changing dacl on a file or directory.
setattr_with_group_change	boolean	Filter the client setattr requests for changing group of a file or directory.
setattr_with_mode_change	boolean	Filter the client setattr requests for changing the mode bits on a file or directory.
setattr_with_modify_time_change	boolean	Filter the client setattr requests for changing the modification time of a file or directory.
setattr_with_owner_change	boolean	Filter the client setattr requests for changing owner of a file or directory.
setattr_with_sacl_change	boolean	Filter the client setattr requests for changing sacl on a file or directory.
setattr_with_size_change	boolean	Filter the client setattr requests for changing the size of a file.
write_with_size_change	boolean	Filter the client request for write with size change.

fpolicy_events

The information that a 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.

Name	Type	Description
file_operations	file_operations	Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.
filters	filters	Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.
monitor_fileop_failure	boolean	Specifies whether failed file operations monitoring is required.
name	string	Specifies the name of the FPolicy event.
protocol	string	Protocol for which event is created. If you specify protocol, then you must also specify a valid value for the file operation parameters. The value of this parameter must be one of the following: • cifs - for the CIFS protocol. • nfsv3 - for the NFSv3 protocol. • nfsv4 - for the NFSv4 protocol.
volume_monitoring	boolean	Specifies whether volume operation monitoring is required.

fpolicy_persistent_stores

The information that an FPolicy process needs in order to configure a persistent store.

Name	Type	Description
name	string	The name specified for the FPolicy persistent store.
volume	string	The specified volume to store the events for the FPolicy persistent store.

fpolicy_engine_reference

FPolicy external engine

Name	Type	Description
_links	_links	
name	string	The name of the FPolicy external engine.

fpolicy_event_reference

FPolicy events

Name	Type	Description
_links	_links	
name	string	

scope

Name	Type	Description
check_extensions_on_directories	boolean	Specifies whether the file name extension checks also apply to directory objects. If this parameter is set to true, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match. Default is false.
exclude_export_policies	array[string]	
exclude_extension	array[string]	
exclude_shares	array[string]	

Name	Type	Description
exclude_volumes	array[string]	
include_export_policies	array[string]	
include_extension	array[string]	
include_shares	array[string]	
include_volumes	array[string]	
object_monitoring_with_no_extension	boolean	Specifies whether the extension checks also apply to objects with no extension. If this parameter is set to true, all objects with or without extensions are monitored. Default is false.

fpolicy_policies

Name	Type	Description
allow_privileged_access	boolean	Specifies whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. When this parameter is set to true, FPolicy servers can access files on the cluster using a separate data channel with privileged access.
enabled	boolean	Specifies if the policy is enabled on the SVM or not. If no value is mentioned for this field but priority is set, then this policy will be enabled.
engine	fpolicy_engine_reference	FPolicy external engine
events	array[fpolicy_event_reference]	
mandatory	boolean	Specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to true, file access events will be denied under these circumstances.

Name	Type	Description
name	string	Specifies the name of the policy.
passthrough_read	boolean	Specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are files that have been moved to secondary storage.
persistent_store	string	Specifies the persistent storage name. This can then be used to enable persistent mode for FPolicy events.
priority	integer	Specifies the priority that is assigned to this policy.
privileged_user	string	Specifies the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in "domain\username" format.
scope	scope	

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

fpolicy

FPolicy is an infrastructure component of ONTAP that enables partner applications connected to your storage systems to monitor and set file access permissions. Every time a client accesses a file from a storage system, based on the configuration of FPolicy, the partner application is notified about file access.

Name	Type	Description
_links	_links	
engines	array[fpolicy_engines]	
events	array[fpolicy_events]	
persistent_stores	array[fpolicy_persistent_stores]	
policies	array[fpolicy_policies]	
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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 configuration

POST `/protocols/fpolicy`

Introduced In: 9.6

Creates an FPolicy configuration.

Required properties

- `svm.uuid` or `svm.name` - Existing SVM in which to create the FPolicy configuration.

Recommended optional properties

- `engines` - External server to which the notifications will be sent.
- `events` - File operations to monitor.
- `policies` - Policy configuration which acts as a container for FPolicy event and FPolicy engine.
- `scope` - Scope of the policy. Can be limited to exports, volumes, shares or file extensions.

Default property values

If not specified in POST, the following default property values are assigned:

- `engines.type` - *synchronous*
- `policies.engine` - *native*
- `policies.mandatory` - *true*
- `events.volume_monitoring` - *false*
- `events.file_operations.*` - *false*
- `events.filters.*` - *false*
- `events.monitor_fileop_failure.*` - *false*

Related ONTAP commands

- `fpolicy policy event create`
- `fpolicy policy external-engine create`
- `fpolicy policy create`
- `fpolicy policy scope create`
- `fpolicy enable`
- `fpolicy persistent-store create`

Learn more

- DOC /protocols/fpolicy

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
_links	_links	
engines	array[fpolicy_engines]	
events	array[fpolicy_events]	
persistent_stores	array[fpolicy_persistent_stores]	
policies	array[fpolicy_policies]	
svm	svm	SVM, applies only to SVM-scoped objects.

Example request


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "engines": {
    "certificate": {
      "ca": "TASample1",
      "name": "Sample1-FPolicy-Client",
      "serial_number": "8DDE112A114D1FBC"
    },
    "format": "xml",
    "keep_alive_interval": "PT2M",
    "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",
    "type": "synchronous"
  },
  "events": {
    "name": "event_cifs",
    "protocol": "cifs"
  },
  "persistent_stores": {
    "name": "ps1",
    "volume": "psvol"
  },
```

```
  "policies": {
    "engine": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "events": [
      "event_cifs",
      "event_open"
    ],
    "name": "fp_policy_1",
    "persistent_store": "ps1",
    "priority": 1,
    "privileged_user": "mydomain\\testuser",
    "scope": {
      "exclude_export_policies": {
      },
      "exclude_extension": {
      },
      "exclude_shares": {
      },
      "exclude_volumes": [
        "vol1",
        "vol_svm1",
        "*"
      ],
      "include_export_policies": {
      },
      "include_extension": {
      },
      "include_shares": [
        "sh1",
        "share_cifs"
      ],
      "include_volumes": [
        "vol1",
        "vol_svm1"
      ]
    }
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
```

```
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
```


Response

```
Status: 201, Created
```

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

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "engines": {
      "certificate": {
        "ca": "TASample1",
        "name": "Sample1-FPolicy-Client",
        "serial_number": "8DDE112A114D1FBC"
      },
      "format": "xml",
      "keep_alive_interval": "PT2M",
      "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",
```

```
      "type": "synchronous"
    },
    "events": {
      "name": "event_cifs",
      "protocol": "cifs"
    },
    "persistent_stores": {
      "name": "ps1",
      "volume": "psvol"
    },
    "policies": {
      "engine": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        }
      },
      "events": [
        "event_cifs",
        "event_open"
      ],
      "name": "fp_policy_1",
      "persistent_store": "ps1",
      "priority": 1,
      "privileged_user": "mydomain\\testuser",
      "scope": {
        "exclude_export_policies": {
        },
        "exclude_extension": {
        },
        "exclude_shares": {
        },
        "exclude_volumes": [
          "vol1",
          "vol_svm1",
          "*"
        ],
        "include_export_policies": {
        },
        "include_extension": {
        },
        "include_shares": [
          "sh1",
          "share_cifs"
        ],
```

```
        "include_volumes": [
          "vol1",
          "vol_svm1"
        ]
      }
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
9765032	The FPolicy engine, FPolicy event or FPolicy policy specified already exists
9765031	If any of the FPolicy engine, FPolicy event, or FPolicy policy creation fails due to a systematic error or hardware failure, the cause of the failure is detailed in the error message
2621706	The SVM UUID specified belongs to different SVM
2621462	The SVM name specified does not exist

Name	Type	Description
error	returned_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
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.

fpolicy_engines

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	The format for the notification messages sent to the FPolicy servers. The possible values are: • 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.
keep_alive_interval	string	Specifies the ISO-8601 interval time for a storage appliance to send Keep Alive message to an FPolicy server. The allowed range is between 10 to 600 seconds.
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 values are 500, 1000 or 2000 for Low-end(<64 GB memory), Mid-end(>=64 GB memory) and High-end(>=128 GB memory) Platforms respectively.
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	Specifies the SSL option for external communication with the FPolicy server. Possible values include the following: • no_auth When set to "no_auth", no authentication takes place. • 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	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.

Name	Type	Description
type	string	The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are: • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.10 ◦ x-nullable: true

file_operations

Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.

Name	Type	Description
access	boolean	Access operations
close	boolean	File close operations
create	boolean	File create operations
create_dir	boolean	Directory create operations
delete	boolean	File delete operations
delete_dir	boolean	Directory delete operations
getattr	boolean	Get attribute operations
link	boolean	Link operations
lookup	boolean	Lookup operations
open	boolean	File open operations

Name	Type	Description
read	boolean	File read operations
rename	boolean	File rename operations
rename_dir	boolean	Directory rename operations
setattr	boolean	Set attribute operations
symlink	boolean	Symbolic link operations
write	boolean	File write operations

filters

Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.

Name	Type	Description
close_with_modification	boolean	Filter the client request for close with modification.
close_with_read	boolean	Filter the client request for close with read.
close_without_modification	boolean	Filter the client request for close without modification.
exclude_directory	boolean	Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.
first_read	boolean	Filter the client requests for the first-read.
first_write	boolean	Filter the client requests for the first-write.
monitor_ads	boolean	Filter the client request for alternate data stream.
offline_bit	boolean	Filter the client request for offline bit set. FPolicy server receives notification only when offline files are accessed.

Name	Type	Description
open_with_delete_intent	boolean	Filter the client request for open with delete intent.
open_with_write_intent	boolean	Filter the client request for open with write intent.
setattr_with_access_time_change	boolean	Filter the client setattr requests for changing the access time of a file or directory.
setattr_with_allocation_size_change	boolean	Filter the client setattr requests for changing the allocation size of a file.
setattr_with_creation_time_change	boolean	Filter the client setattr requests for changing the creation time of a file or directory.
setattr_with_dacl_change	boolean	Filter the client setattr requests for changing dacl on a file or directory.
setattr_with_group_change	boolean	Filter the client setattr requests for changing group of a file or directory.
setattr_with_mode_change	boolean	Filter the client setattr requests for changing the mode bits on a file or directory.
setattr_with_modify_time_change	boolean	Filter the client setattr requests for changing the modification time of a file or directory.
setattr_with_owner_change	boolean	Filter the client setattr requests for changing owner of a file or directory.
setattr_with_sacl_change	boolean	Filter the client setattr requests for changing sacl on a file or directory.
setattr_with_size_change	boolean	Filter the client setattr requests for changing the size of a file.
write_with_size_change	boolean	Filter the client request for write with size change.

fpolicy_events

The information that a 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.

Name	Type	Description
file_operations	file_operations	Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.
filters	filters	Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.
monitor_fileop_failure	boolean	Specifies whether failed file operations monitoring is required.
name	string	Specifies the name of the FPolicy event.
protocol	string	Protocol for which event is created. If you specify protocol, then you must also specify a valid value for the file operation parameters. The value of this parameter must be one of the following: • cifs - for the CIFS protocol. • nfsv3 - for the NFSv3 protocol. • nfsv4 - for the NFSv4 protocol.
volume_monitoring	boolean	Specifies whether volume operation monitoring is required.

fpolicy_persistent_stores

The information that an FPolicy process needs in order to configure a persistent store.

Name	Type	Description
name	string	The name specified for the FPolicy persistent store.
volume	string	The specified volume to store the events for the FPolicy persistent store.

fpolicy_engine_reference

FPolicy external engine

Name	Type	Description
_links	_links	
name	string	The name of the FPolicy external engine.

fpolicy_event_reference

FPolicy events

Name	Type	Description
_links	_links	
name	string	

scope

Name	Type	Description
check_extensions_on_directories	boolean	Specifies whether the file name extension checks also apply to directory objects. If this parameter is set to true, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match. Default is false.
exclude_export_policies	array[string]	
exclude_extension	array[string]	
exclude_shares	array[string]	

Name	Type	Description
exclude_volumes	array[string]	
include_export_policies	array[string]	
include_extension	array[string]	
include_shares	array[string]	
include_volumes	array[string]	
object_monitoring_with_no_extension	boolean	Specifies whether the extension checks also apply to objects with no extension. If this parameter is set to true, all objects with or without extensions are monitored. Default is false.

fpolicy_policies

Name	Type	Description
allow_privileged_access	boolean	Specifies whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. When this parameter is set to true, FPolicy servers can access files on the cluster using a separate data channel with privileged access.
enabled	boolean	Specifies if the policy is enabled on the SVM or not. If no value is mentioned for this field but priority is set, then this policy will be enabled.
engine	fpolicy_engine_reference	FPolicy external engine
events	array[fpolicy_event_reference]	
mandatory	boolean	Specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to true, file access events will be denied under these circumstances.

Name	Type	Description
name	string	Specifies the name of the policy.
passthrough_read	boolean	Specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are files that have been moved to secondary storage.
persistent_store	string	Specifies the persistent storage name. This can then be used to enable persistent mode for FPolicy events.
priority	integer	Specifies the priority that is assigned to this policy.
privileged_user	string	Specifies the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in "domain\username" format.
scope	scope	

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

fpolicy

FPolicy is an infrastructure component of ONTAP that enables partner applications connected to your storage systems to monitor and set file access permissions. Every time a client accesses a file from a storage system, based on the configuration of FPolicy, the partner application is notified about file access.

Name	Type	Description
_links	_links	
engines	array[fpolicy_engines]	
events	array[fpolicy_events]	
persistent_stores	array[fpolicy_persistent_stores]	
policies	array[fpolicy_policies]	
svm	svm	SVM, applies only to SVM-scoped objects.

_links

Name	Type	Description
next	href	
self	href	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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.

Delete the FPolicy configuration for an SVM

DELETE `/protocols/fpolicy/{svm.uuid}`

Introduced In: 9.6

Deletes the FPolicy configuration for the specified SVM. Before deleting the FPolicy configuration, ensure that

all policies belonging to the SVM are disabled.

Related ONTAP commands

- `fpolicy delete`
- `fpolicy policy scope delete`
- `fpolicy policy delete`
- `fpolicy policy event delete`
- `fpolicy policy external-engine delete`
- `fpolicy persistent-store delete`

Learn more

- DOC /protocols/fpolicy

Parameters

Name	Type	In	Required	Description
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
9765031	If any of the FPolicy engine, FPolicy event or FPolicy policy deletion fails due to a systemic error or hardware failure, the cause of the failure is detailed in the error message.

Name	Type	Description
error	returned_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

returned_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 the FPolicy configuration for an SVM

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

Introduced In: 9.6

Retrieves an FPolicy configuration of an SVM.

Related ONTAP commands

- `fpolicy show`
- `fpolicy policy show`
- `fpolicy policy scope show`
- `fpolicy policy event show`
- `fpolicy policy external-engine show`
- `fpolicy persistent-store show`

Learn more

- DOC /protocols/fpolicy

Parameters

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
_links	_links	
engines	array[fpolicy_engines]	
events	array[fpolicy_events]	
persistent_stores	array[fpolicy_persistent_stores]	
policies	array[fpolicy_policies]	
svm	svm	SVM, applies only to SVM-scoped objects.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "engines": {
    "certificate": {
      "ca": "TASample1",
      "name": "Sample1-FPolicy-Client",
      "serial_number": "8DDE112A114D1FBC"
    },
    "format": "xml",
    "keep_alive_interval": "PT2M",
    "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",
    "type": "synchronous"
  },
  "events": {
    "name": "event_cifs",
    "protocol": "cifs"
  },
  "persistent_stores": {
    "name": "ps1",
    "volume": "psvol"
  },
```

```
  "policies": {
    "engine": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "events": [
      "event_cifs",
      "event_open"
    ],
    "name": "fp_policy_1",
    "persistent_store": "ps1",
    "priority": 1,
    "privileged_user": "mydomain\\testuser",
    "scope": {
      "exclude_export_policies": {
      },
      "exclude_extension": {
      },
      "exclude_shares": {
      },
      "exclude_volumes": [
        "vol1",
        "vol_svm1",
        "*"
      ],
      "include_export_policies": {
      },
      "include_extension": {
      },
      "include_shares": [
        "sh1",
        "share_cifs"
      ],
      "include_volumes": [
        "vol1",
        "vol_svm1"
      ]
    }
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
```

```
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_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
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.

fpolicy_engines

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	The format for the notification messages sent to the FPolicy servers. The possible values are: • 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.
keep_alive_interval	string	Specifies the ISO-8601 interval time for a storage appliance to send Keep Alive message to an FPolicy server. The allowed range is between 10 to 600 seconds.
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 values are 500, 1000 or 2000 for Low-end(<64 GB memory), Mid-end(>=64 GB memory) and High-end(>=128 GB memory) Platforms respectively.
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	Specifies the SSL option for external communication with the FPolicy server. Possible values include the following: • no_auth When set to "no_auth", no authentication takes place. • 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	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.

Name	Type	Description
type	string	The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are: • synchronous - After sending a notification, wait for a response from the FPolicy server. • asynchronous - After sending a notification, file request processing continues. ◦ Default value: 1 ◦ enum: ["synchronous", "asynchronous"] ◦ Introduced in: 9.10 ◦ x-nullable: true

file_operations

Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.

Name	Type	Description
access	boolean	Access operations
close	boolean	File close operations
create	boolean	File create operations
create_dir	boolean	Directory create operations
delete	boolean	File delete operations
delete_dir	boolean	Directory delete operations
getattr	boolean	Get attribute operations
link	boolean	Link operations
lookup	boolean	Lookup operations
open	boolean	File open operations

Name	Type	Description
read	boolean	File read operations
rename	boolean	File rename operations
rename_dir	boolean	Directory rename operations
setattr	boolean	Set attribute operations
symlink	boolean	Symbolic link operations
write	boolean	File write operations

filters

Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.

Name	Type	Description
close_with_modification	boolean	Filter the client request for close with modification.
close_with_read	boolean	Filter the client request for close with read.
close_without_modification	boolean	Filter the client request for close without modification.
exclude_directory	boolean	Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.
first_read	boolean	Filter the client requests for the first-read.
first_write	boolean	Filter the client requests for the first-write.
monitor_ads	boolean	Filter the client request for alternate data stream.
offline_bit	boolean	Filter the client request for offline bit set. FPolicy server receives notification only when offline files are accessed.

Name	Type	Description
open_with_delete_intent	boolean	Filter the client request for open with delete intent.
open_with_write_intent	boolean	Filter the client request for open with write intent.
setattr_with_access_time_change	boolean	Filter the client setattr requests for changing the access time of a file or directory.
setattr_with_allocation_size_change	boolean	Filter the client setattr requests for changing the allocation size of a file.
setattr_with_creation_time_change	boolean	Filter the client setattr requests for changing the creation time of a file or directory.
setattr_with_dacl_change	boolean	Filter the client setattr requests for changing dacl on a file or directory.
setattr_with_group_change	boolean	Filter the client setattr requests for changing group of a file or directory.
setattr_with_mode_change	boolean	Filter the client setattr requests for changing the mode bits on a file or directory.
setattr_with_modify_time_change	boolean	Filter the client setattr requests for changing the modification time of a file or directory.
setattr_with_owner_change	boolean	Filter the client setattr requests for changing owner of a file or directory.
setattr_with_sacl_change	boolean	Filter the client setattr requests for changing sacl on a file or directory.
setattr_with_size_change	boolean	Filter the client setattr requests for changing the size of a file.
write_with_size_change	boolean	Filter the client request for write with size change.

fpolicy_events

The information that a 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.

Name	Type	Description
file_operations	file_operations	Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.
filters	filters	Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.
monitor_fileop_failure	boolean	Specifies whether failed file operations monitoring is required.
name	string	Specifies the name of the FPolicy event.
protocol	string	Protocol for which event is created. If you specify protocol, then you must also specify a valid value for the file operation parameters. The value of this parameter must be one of the following: • cifs - for the CIFS protocol. • nfsv3 - for the NFSv3 protocol. • nfsv4 - for the NFSv4 protocol.
volume_monitoring	boolean	Specifies whether volume operation monitoring is required.

fpolicy_persistent_stores

The information that an FPolicy process needs in order to configure a persistent store.

Name	Type	Description
name	string	The name specified for the FPolicy persistent store.
volume	string	The specified volume to store the events for the FPolicy persistent store.

fpolicy_engine_reference

FPolicy external engine

Name	Type	Description
_links	_links	
name	string	The name of the FPolicy external engine.

fpolicy_event_reference

FPolicy events

Name	Type	Description
_links	_links	
name	string	

scope

Name	Type	Description
check_extensions_on_directories	boolean	Specifies whether the file name extension checks also apply to directory objects. If this parameter is set to true, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match. Default is false.
exclude_export_policies	array[string]	
exclude_extension	array[string]	
exclude_shares	array[string]	

Name	Type	Description
exclude_volumes	array[string]	
include_export_policies	array[string]	
include_extension	array[string]	
include_shares	array[string]	
include_volumes	array[string]	
object_monitoring_with_no_extension	boolean	Specifies whether the extension checks also apply to objects with no extension. If this parameter is set to true, all objects with or without extensions are monitored. Default is false.

fpolicy_policies

Name	Type	Description
allow_privileged_access	boolean	Specifies whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. When this parameter is set to true, FPolicy servers can access files on the cluster using a separate data channel with privileged access.
enabled	boolean	Specifies if the policy is enabled on the SVM or not. If no value is mentioned for this field but priority is set, then this policy will be enabled.
engine	fpolicy_engine_reference	FPolicy external engine
events	array[fpolicy_event_reference]	
mandatory	boolean	Specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to true, file access events will be denied under these circumstances.

Name	Type	Description
name	string	Specifies the name of the policy.
passthrough_read	boolean	Specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are files that have been moved to secondary storage.
persistent_store	string	Specifies the persistent storage name. This can then be used to enable persistent mode for FPolicy events.
priority	integer	Specifies the priority that is assigned to this policy.
privileged_user	string	Specifies the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in "domain\username" format.
scope	scope	

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_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

Trademark information