Create or retrieve event filters

ONTAP 9.15.1 REST API reference

NetApp
September 11, 2024

Table of Contents

Create or retrieve event filters

Support EMS filters endpoint overview

Overview

Manages the list of available filters. A filter is a named collection of rules that enable the system to identify events that require additional handling. A filter is linked with a destination to which the system sends specific events.

When EMS processes an event, each filter is evaluated for a match. More than one filter can handle a single event.

The system defines default filters that cannot be removed or modified. These filters are specified by setting the "system_defined" field to "true".

Filter rule position

A filter's rules are evaluated sequentially, according to their position index. When a rule is added or modified, the position can be set to customize the filter's logic. If no position is specified, a new rule is appended to the end of the list.

Filter rule types

A filter rule can be one of two types: 'include' or 'exclude'. If an event matches the criteria of the rule, the type dictates whether it should be forwarded to the destination or ignored.

Filter rule matching criteria

A valid filter rule must contain at least one set of criteria.

Name pattern

A name pattern is matched against an event's name. Multiple characters can be matched using the wildcard character '*'.

Severity

The severity pattern is matched against an event's severity. Multiple severities can be specified in a comma separated list. A single wildcard `*` will match all severities. When multiple severities are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard `*` characters. Valid values are:

- emergency
- alert
- error
- notice
- informational
- debug

SNMP trap type

The SNMP trap type pattern is matched against an event’s trap type. Multiple trap types can be specified in a comma separated list. A single wildcard * matches all trap types. When multiple trap types are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard * characters. Valid values are:

- standard
- built_in
- severity_based

Parameter criteria

A parameter criterion is matched against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.

Examples

Retrieving a list of filters whose names contain a hyphen

```
# The API:
GET /api/support/ems/filters

# The call:
curl -X GET "https://<mgmt-ip>/api/support/ems/filters?name=*-*" -H
"accept: application/hal+json"

# The response:
200 OK

# JSON Body
{
"records": [
  {
    "name": "default-trap-events",
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/default-trap-events"
      }
    }
  },
  {
    "name": "important-events",
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/important-events"
      }
    }
  },
  {
    "name": "no-info-debug-events",
    "_links": {
      "self": {
        "href": "/api/support/ems/filters/no-info-debug-events"
      }
    }
  }
],
"num_records": 3,
"_links": {
  "self": {
    "href": "/api/support/ems/filters?name=*-*"
  }
}
}
```

Creating a new filter using various matching criteria

```
# The API:
POST /api/support/ems/filters

# The call:
curl -X POST "https://<mgmt-ip>/api/support/ems/filters" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_filters_post.txt"
test_ems_filters_post.txt(body):
{
"name": "test-filter",
"rules": [
  {
    "index": 1,
    "type": "include",
    "message_criteria": {
      "name_pattern": "LUN.*",
      "severities": "alert,error",
      "snmp_trap_types": "severity_based"
    },
    "parameter_criteria": [
      {
        "name_pattern": "type",
        "value_pattern": "volume"
      },
      {
        "name_pattern": "vol",
        "value_pattern": "cloud*"
      }
    ]
  }
]
}

# The response:
201 Created
```

Retrieve event filters

GET `/support/ems/filters`

Introduced In: 9.6

Retrieves a collection of event filters.

Related ONTAP commands

- `event filter show`

Parameters

Name	Type	In	Required	Description
name	string	query	False	Filter by name
system_defined	boolean	query	False	Filter by system_defined • Introduced in: 9.10
access_control_role.name	string	query	False	Filter by access_control_role.name • Introduced in: 9.13
rules.index	integer	query	False	Filter by rules.index
rules.parameter_criteria.value_pattern	string	query	False	Filter by rules.parameter_criteria.value_pattern • Introduced in: 9.13
rules.parameter_criteria.name_pattern	string	query	False	Filter by rules.parameter_criteria.name_pattern • Introduced in: 9.13
rules.type	string	query	False	Filter by rules.type
rules.message_criteria.severities	string	query	False	Filter by rules.message_criteria.severities
rules.message_criteria.name_pattern	string	query	False	Filter by rules.message_criteria.name_pattern

Name	Type	In	Required	Description
rules.message_criteria.snmp_trap_types	string	query	False	Filter by rules.message_criteria.snmp_trap_types
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
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. • Default value: 1 • Max value: 120 • Min value: 0
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[records]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access_control_role": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "admin"
      },
      "name": "wafl-critical-events",
      "rules": [
        {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "index": 1,
          "message_criteria": {
            "_links": {
              "related": {
                "href": "/api/resourcelink"
              }
            },
            "name_pattern": "wafl.*",
            "severities": "emergency,alert,error",
            "snmp_trap_types": "standard,built_in"
          },
```

```
          "parameter_criteria": [
            {
              "name_pattern": "vol",
              "value_pattern": "cloud*"
            }
          ],
          "type": "include"
        }
      ],
      "system_defined": 1
    }
  ]
}
```


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	

access_control_role

Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
_links	_links	
name	string	Role name

_links

Name	Type	Description
related	href	

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
_links	_links	
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.

Name	Type	Description
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

rules

Rule for an event filter

Name	Type	Description
_links	_links	
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

records

Name	Type	Description
_links	_links	
access_control_role	access_control_role	Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

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 event filter

POST `/support/ems/filters`

Introduced In: 9.6

Creates an event filter.

Required properties

- `name` - String that uniquely identifies the filter.

Recommended optional properties

- `rules` - List of criteria which is used to match a filter with an event.

Related ONTAP commands

- `event filter create`

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	
access_control_role	access_control_role	Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_control_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "name": "wafl-critical-events",
  "rules": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "index": 1,
      "message_criteria": {
        "_links": {
          "related": {
            "href": "/api/resourcelink"
          }
        },
        "name_pattern": "wafl.*",
        "severities": "emergency,alert,error",
        "snmp_trap_types": "standard,built_in"
      },
      "parameter_criteria": [
        {
          "name_pattern": "vol",
          "value_pattern": "cloud*"
        }
      ],
      "type": "include"
    }
  ],
  "system_defined": 1
}
```

Response

```
Status: 201, Created
```

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

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access_control_role": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "admin"
      },
      "name": "wafl-critical-events",
      "rules": [
        {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "index": 1,
          "message_criteria": {
            "_links": {
              "related": {
                "href": "/api/resourcelink"
              }
            },
            "name_pattern": "wafl.*",
            "severities": "emergency,alert,error",
            "snmp_trap_types": "standard,built_in"
          },
```

```
          "parameter_criteria": [
            {
              "name_pattern": "vol",
              "value_pattern": "cloud*"
            }
          ],
          "type": "include"
        }
      ],
      "system_defined": 1
    }
  ]
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
983088	The filter name provided is empty
983089	The filter name provided cannot contain spaces
983092	The index of the rule provided is outside the allowed range for the filter provided
983094	The filter name provided is invalid. The filter name must contain between 2 and 64 characters and start and end with an alphanumeric symbol or (underscore). The allowed special characters are (underscore) and -(hyphen)
983095	The rule index provided is invalid for the filter provided
983101	No event is matched by the rule provided
983113	Default filters cannot be modified or removed
983114	The maximum number of filters is reached
983115	The maximum number of filter rules is reached

Error Code	Description
983126	A rule requires at least one name_pattern, severities, snmp_trap_types, or parameter pattern to be defined
983127	A property cannot contain a combination of the wildcard character and other values
983128	An invalid value is provided for the property 'snmp_trap_types'
983146	An invalid value is provided for the property 'severities'
983147	The severities provided are not supported
983155	The provided severities property does not match that of the name_pattern
983156	The provided snmp_trap_types property does not match that of the name_pattern
983157	The provided severities and snmp_trap_types properties do not match those of the name_pattern
983158	The name_pattern provided does not exist
983195	Empty field in parameter_criteria. Both name and value patterns must be specified
983196	name_pattern and value_pattern fields in parameter_criteria are empty
983211	Parameter criteria based filtering is not supported in this version of ONTAP
983216	The provided parameter criteria does not match that of the message name

Also see the table of common errors in the Response body overview section of this documentation.

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	

access_control_role

Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.

Name	Type	Description
_links	_links	
name	string	Role name

_links

Name	Type	Description
related	href	

message_criteria

Matching message definitions for the filter. A property must be specified.

Name	Type	Description
_links	_links	
name_pattern	string	Message name filter on which to match. Supports wildcards. Defaults to * if not specified.
severities	string	A comma-separated list of severities or a wildcard.
snmp_trap_types	string	A comma separated list of snmp_trap_types or a wildcard.

parameter_criteria

Criterion used for parameter based filtering

Name	Type	Description
name_pattern	string	Parameter name pattern. Wildcard character '*' is supported.
value_pattern	string	Parameter value pattern. Wildcard character '*' is supported.

rules

Rule for an event filter

Name	Type	Description
_links	_links	
index	integer	Rule index. Rules are evaluated in ascending order. If a rule's index order is not specified during creation, the rule is appended to the end of the list.
message_criteria	message_criteria	Matching message definitions for the filter. A property must be specified.
parameter_criteria	array[parameter_criteria]	Parameter criteria used to match against events' parameters. Each parameter consists of a name and a value. When multiple parameter criteria are provided in a rule, all must match for the rule to be considered matched. A pattern can include one or more wildcard '*' characters.
type	string	Rule type

ems_filter

Name	Type	Description
_links	_links	

Name	Type	Description
access_control_role	access_control_role	Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

_links

Name	Type	Description
next	href	
self	href	

records

Name	Type	Description
_links	_links	
access_control_role	access_control_role	Indicates the access control role that created the event filter and is used to control access to the filter based on role-based access control (RBAC) rules. If created by the 'admin' user, the field is unset.
name	string	Filter name
rules	array[rules]	Array of event filter rules on which to match.
system_defined	boolean	Flag indicating system-defined filters.

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