



Manage event filters

ONTAP 9.13.1 REST API reference

NetApp
August 29, 2024

Table of Contents

- Manage event filters 1
 - Support EMS filters name endpoint overview 1
 - Delete an event filter 3
 - Retrieve an event filter 6
 - Update an event filter 12

Manage event filters

Support EMS filters name endpoint overview

Overview

Manages a specific filter instance. See the documentation for </support/ems/filters> for details on the various properties.

Examples

Retrieving a specific filter instance

```
# The API:
GET /api/support/ems/filters/{name}

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

# The response:
200 OK

# JSON Body
{
  "name": "aggregate-events",
  "rules": [
    {
      "index": 1,
      "type": "include",
      "message_criteria": {
        "name_pattern": "*",
        "severities": "emergency,alert,error,notice",
        "snmp_trap_types": "*",
        "_links": {
          "related": {
            "href":
"/api/support/ems/messages?name=*&severity=emergency,alert,error,notice&snmp_trap_type=*"
          }
        }
      },
      "parameter_criteria": [
        {
          "name_pattern": "type",
          "value_pattern": "aggregate"
        }
      ]
    }
  ]
}
```

```

    }
  ],
  "_links": {
    "self": {
      "href": "/api/support/ems/filters/aggregate-events/rules/1"
    }
  }
},
{
  "index": 2,
  "type": "exclude",
  "message_criteria": {
    "name_pattern": "*",
    "severities": "*",
    "snmp_trap_types": "*",
    "_links": {
      "related": {
        "href":
"/api/support/ems/messages?name=*&severity=*&snmp_trap_type="
      }
    }
  },
  "parameter_criteria": [
    {
      "name_pattern": "*",
      "value_pattern": "*"
    }
  ],
  "_links": {
    "self": {
      "href": "/api/support/ems/filters/aggregate-events/rules/2"
    }
  }
}
],
"_links": {
  "self": {
    "href": "/api/support/ems/filters/aggregate-events"
  }
}
}
}

```

Updating an existing filter with a new rule

```
# The API:
PATCH /api/support/ems/filters/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/support/ems/filters/test-filter" -H
"accept: application/hal+json" -H "Content-Type: application/json" -d
"@test_ems_filters_patch.txt"
test_ems_filters_patch.txt (body):
{
  "rules": [
    {
      "type": "include",
      "message_criteria": {
        "name_pattern": "waf1.*",
        "severities": "error"
      }
    }
  ]
}

# The response:
200 OK
```

Deleting an existing filter

```
# The API:
DELETE /api/support/ems/filters/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/support/ems/filters/test-filter" -H
"accept: application/hal+json"

# The response:
200 OK
```

Delete an event filter

```
DELETE /support/ems/filters/{name}
```

Introduced In: 9.6

Deletes an event filter.

Related ONTAP commands

- `event filter delete`

Parameters

| Name | Type | In | Required | Description |
|------|--------|------|----------|-------------|
| name | string | path | True | Filter name |

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|------------|------------------------------------------------|
| 983113 | Default filters cannot be modified or removed |
| 983124 | Filter is being referenced by a destination |
| 983204 | Filter is being used for role-based operations |

| Name | Type | Description |
|-------|-----------------------|-------------|
| error | error | |

Example error

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

Definitions

See Definitions

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

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

Retrieve an event filter

GET /support/ems/filters/{name}

Introduced In: 9.6

Retrieves an event filter.

Related ONTAP commands

- `event filter show`

Parameters

| Name | Type | In | Required | Description |
|--------|---------------|-------|----------|-------------------------------|
| name | string | path | True | Filter name |
| fields | array[string] | query | False | Specify the fields to return. |

Response

Status: 200, Ok

| 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 response

A large, empty rectangular box with a thin, dashed border, occupying most of the page. It is intended for an example response.

```

{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_control_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "name": "snmp-traphost",
  "rules": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "index": 1,
      "message_criteria": {
        "_links": {
          "related": {
            "href": "/api/resourcelink"
          }
        },
        "name_pattern": "callhome.*",
        "severities": "error,informational",
        "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 | 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 |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

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

Update an event filter

PATCH /support/ems/filters/{name}

Introduced In: 9.6

Updates an event filter.

Recommended optional properties

- `new_name` - New string that uniquely identifies a filter.
- `rules` - New list of criteria used to match the filter with an event. The existing list is discarded.

Related ONTAP commands

- `event filter rename`
- `event filter rule add`
- `event filter rule delete`
- `event filter rule reorder`

Parameters

| Name | Type | In | Required | Description |
|----------|--------|-------|----------|----------------------------------------------|
| name | string | path | True | Filter name |
| new_name | string | query | False | New filter name for renames. Valid in PATCH. |

Request Body

| Name | Type | Description |
|----------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>_links</code> | <code>_links</code> | |
| <code>access_control_role</code> | <code>access_control_role</code> | 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. |
| <code>name</code> | string | Filter name |
| <code>rules</code> | array[<code>rules</code>] | Array of event filter rules on which to match. |
| <code>system_defined</code> | boolean | Flag indicating system-defined filters. |

Example request

A large, empty rectangular box with a thin, dashed border, occupying most of the page. It is intended for an example request.


```

{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access_control_role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "name": "snmp-traphost",
  "rules": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "index": 1,
      "message_criteria": {
        "_links": {
          "related": {
            "href": "/api/resourcelink"
          }
        },
        "name_pattern": "callhome.*",
        "severities": "error,informational",
        "snmp_trap_types": "standard|built_in"
      },
      "parameter_criteria": [
        {
          "name_pattern": "vol",
          "value_pattern": "cloud*"
        }
      ],
      "type": "include"
    }
  ],
  "system_defined": 1
}

```

Response

Status: 200, Ok

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 |
| 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 characters 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 |

| Error Code | Description |
|------------|-----------------------------------------------------------------------------------|
| 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 |

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```

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

```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| 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. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

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

Copyright information

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

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

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

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

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

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

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

Trademark information

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