event filter commands

ONTAP 9.15.1 commands

NetApp
December 18, 2024

Table of Contents

event filter commands

event filter copy

Copy an event filter

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter copy` command copies an existing filter to a new filter. The new filter will be created with rules from the source filter. For more information, see the event filter create command.

Parameters

`-filter-name <text>` - Filter Name

Use this mandatory parameter to specify the name of the event filter to copy.

`-new-filter-name <text>` - New Event Filter Name

Use this mandatory parameter to specify the name of the new event filter to create and copy the rules.

Examples

The following example copies an existing event filter named emer-wafl-events to a new filter named filter1:

```
cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
emer-wafl-events
            1    include  wafl.*           EMERGENCY     *         *=*
            2    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
```

```
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                      *          *=*
            2    exclude  *                *              *          *=*
10 entries were displayed.

cluster1::> event filter copy -filter-name emer-wafl-events -new-filter
-name filter1

cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                      *          *=*
            2    include  *                *              Standard, Built-
in
                                                                 *=*
            3    exclude  *                *              *          *=*
emer-wafl-events
            1    include  wafl.*           EMERGENCY      *          *=*
            2    exclude  *                *              *          *=*
filter1
            1    include  wafl.*           EMERGENCY      *          *=*
            2    exclude  *                *              *          *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                      *          *=*
            2    include  callhome.*       ERROR          *          *=*
            3    exclude  *                *              *          *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                      *          *=*
            2    exclude  *                *              *          *=*
12 entries were displayed.
```

Related Links

- event filter create

event filter create

Create a new event filter.

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter create` command creates a new event filter. An event filter is used to select the events of interest and is made up of one or more rules, each of which contains the following three fields:

*

- name - event (message) name.
- severity - event severity.
- snmp-trap-type - event SNMP trap type.

```
 These fields are evaluated for a match using a logical "AND" operation:
name AND severity AND SNMP trap type. Within a field, the specified
values are evaluated with an implicit logical "OR" operation. So, if `-
snmp-trap-type```_Standard, Built-in_`` is specified, then the event
must match ``_Standard_`` OR ``_Built-in_`` . The wildcard matches all
values for the field.
* Type - include or exclude. When an event matches an include rule, it
will be included into the filter, whereas it will be excluded from the
filter if it matches an exclude rule.
```

Rules are checked in the order they are listed for a filter, until a match is found. There is an implicit rule at the end that matches every event to be excluded. For more information, see the `event filter rule` command.

There are three system-defined event filters provided for your use:

- default-trap-events - This filter matches all ALERT and EMERGENCY events. It also matches all Standard, Built-in SNMP trap type events.
- important-events - This filter matches all ALERT and EMERGENCY events.
- no-info-debug-events - This filter matches all non-INFO and non-DEBUG messages (EMERGENCY, ALERT, ERROR and NOTICE).

The system-defined event filters cannot be modified or deleted.

Parameters

`-filter-name <text>` - Filter Name

Use this mandatory parameter to specify the name of the event filter to create. An event filter name is 2 to 64 characters long. Valid characters are the following ASCII characters: A-Z, a-z, 0-9, "*", and "-". The name must start and end with: A-Z, a-z, "*", or 0-9.

`[-access-control-role <text>]` - Access Control Role (privilege: advanced)

Use this parameter to specify the access control role of the event filter. Access control role indicates the user role which created the filter and is used to control access to the filter based on RBAC rules.

This is an optional field. If not specified, the currently logged in user role is used. If created by the 'admin' user, the field is left unset.

Examples

The following example creates an event filter named filter1:

```
cluster1::> event filter create -filter-name filter1

cluster1::> event filter show
Filter      Rule Rule                                      SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
filter1
            1    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
9 entries were displayed.
```

event filter delete

Delete existing event filters

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter delete` command deletes an existing event filter, along with all its rules.

The system-defined event filters cannot be deleted.

For more information, see the event filter create command.

Parameters

-filter-name <text> - Filter Name

Use this mandatory parameter to specify the name of the event filter to delete.

Examples

The following example deletes an event filter named filter1:

```
cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
filter1
            1    include  wafl.*           EMERGENCY     *         *=*
            2    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
10 entries were displayed.

cluster1::> event filter delete -filter-name filter1

cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
```

```
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                   *          *=*
            2    include  *                *             Standard, Built-
in
                                                              *=*
            3    exclude  *                *             *          *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                   *          *=*
            2    include  callhome.*       ERROR         *          *=*
            3    exclude  *                *             *          *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                   *          *=*
            2    exclude  *                *             *          *=*
8 entries were displayed.
```

Related Links

- event filter create

event filter prepare-for-revert

Deletes unsupported filter or updates unsupported parameter-criteria (parameter-criteria values other than **=**)

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

The `event filter prepare-for-revert` command can be used to remove event filters or update event filter rules that are not supported when the cluster reverts to the previous release. Event filters with rules having a `parameter-criteria` value other than `*=*` are not supported.

Parameters

{ `-delete-unsupported-filters {true|false}` - Clear Unsupported Filters (privilege: advanced)

Use this parameter to delete the event filters that are not supported in the previous release.

| `-update-unsupported-filter-param-criteria {true|false}` - Update Unsupported Filter Parameter Criteria (privilege: advanced) }

Use this parameter to update the event filter rules that are not supported in the previous release to `*=*` .

Examples

The following shows examples of "event filter prepare-for-revert":

```
cluster1::> event filter show
Filter      Rule Rule                                SNMP Trap
Name        Posn Type     Message Name  Severity     Type       Parameters
----------- ---- -------- ------------- ----------- ---------- ----------
default-trap-events
            1    include  *             EMERGENCY, ALERT
                                                    *          *=*
            2    include  *             *           Standard, Built-in
                                                               *=*
            3    exclude  *             *           *          *=*
important-events
            1    include  *             EMERGENCY, ALERT
                                                    *          *=*
            2    include  callhome.*    ERROR       *          *=*
            3    exclude  *             *           *          *=*
no-info-debug-events
            1    include  *             EMERGENCY, ALERT, ERROR, NOTICE
                                                    *          *=*
            2    exclude  *             *           *          *=*
wafl-filter
            1    include  wafl.*        EMERGENCY   *          vol=xyz
            2    exclude  *             *           *          *=*
10 entries were displayed.

cluster1::*> event filter prepare-for-revert -delete-unsupported-filters
true

cluster1::> event filter show
Filter      Rule Rule                                SNMP Trap
Name        Posn Type     Message Name  Severity     Type       Parameters
----------- ---- -------- ------------- ----------- ---------- ----------
default-trap-events
            1    include  *             EMERGENCY, ALERT
                                                    *          *=*
            2    include  *             *           Standard, Built-in
                                                               *=*
            3    exclude  *             *           *          *=*
important-events
            1    include  *             EMERGENCY, ALERT
                                                    *          *=*
            2    include  callhome.*    ERROR       *          *=*
            3    exclude  *             *           *          *=*
no-info-debug-events
            1    include  *             EMERGENCY, ALERT, ERROR, NOTICE
                                                    *          *=*
            2    exclude  *             *           *          *=*
```

```
8 entries were displayed.
```

event filter rename

Rename an event filter

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter rename` command is used to rename an existing event filter.

There are system-defined event filters provided for your use. The system-defined event filters cannot be modified or deleted.

For more information, see the event filter create comamnd.

Parameters

`-filter-name <text>` - Filter Name

Use this mandatory parameter to specify the name of the event filter to rename.

`-new-filter-name <text>` - New Event Filter Name

Use this mandatory parameter to specify the new name the event filter should be renamed to.

Examples

The following example renames an existing filter named filter1 as emer-wafl-events:

```
cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
filter1
            1    include  wafl.*           EMERGENCY     *         *=*
            2    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
```

```
                                                          *          *=*
            2    include  callhome.*       ERROR          *          *=*
            3    exclude  *                *              *          *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                          *          *=*
            2    exclude  *                *              *          *=*
10 entries were displayed.
cluster1::> event filter rename -filter-name filter1 -new-filter-name
emer-wafl-events

cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                          *          *=*
            2    include  *                *             Standard, Built-
in
                                                                     *=*
            3    exclude  *                *              *          *=*
emer-wafl-events
            1    include  wafl.*           EMERGENCY      *          *=*
            2    exclude  *                *              *          *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                          *          *=*
            2    include  callhome.*       ERROR          *          *=*
            3    exclude  *                *              *          *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                          *          *=*
            2    exclude  *                *              *          *=*
10 entries were displayed.
```

Related Links

- event filter create

event filter show-summary

Display event filter summary

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

The `event filter show-summary` command displays a summary of all the event filters. For more details, use the event filter show command.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-filter-name <text>] - Filter Name (privilege: advanced)

Selects the event filters that match this parameter value.

[-rule-count <integer>] - Number of Rules (privilege: advanced)

Selects the event filters that match this parameter value.

[-system-defined {true|false}] - System-Defined Filter (privilege: advanced)

Selects the event filters that match this parameter value. System-defined filters are defined by the system and cannot be modified or deleted.

[-access-control-role <text>] - Access Control Role (privilege: advanced)

Selects the event filters that match this parameter value. The access control role indicates the user role that created the filter and is used to control access to the filter based on RBAC rules. For filters created by 'admin', the access control role is empty (indicated by '-').

Examples

The following example displays the event filter summary:

```
cluster-1::*> event filter show-summary
Filter Name         Rule Count  System-Defined Access Control Role
------------------  ----------  -------------- ------------------
default-trap-events
                    4           true           -
important-events    3           true           -
no-info-debug-events
                    2           true           -
test_filter         1           false          test_role
4 entries were displayed.
```

Related Links

- event filter show

event filter show

Display the list of existing event filters.

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter show` command displays all the event filters which are configured. An event filter is used to select the events of interest and is made up of one or more rules, each of which contains the following three fields:

*

- name - event (message) name.
- severity - event severity.
- snmp-trap-type - event SNMP trap type.

```
 These fields are evaluated for a match using a logical "AND" operation:
name AND severity AND SNMP trap type. Within a field, the specified
values are evaluated with an implicit logical "OR" operation. So, if `-
snmp-trap-type```_Standard, Built-in_`` is specified, then the event
must match ``_Standard_`` OR ``_Built-in_`` . The wildcard matches all
values for the field.
* Type - include or exclude. When an event matches an include rule, it
will be included into the filter, whereas it will be excluded from the
filter if it matches an exclude rule.
```

Rules are checked in the order they are listed for a filter, until a match is found. There is an implicit rule at the end that matches every event to be excluded. For more information, see `event filter rule` command.

There are three system-defined event filters provided for your use:

- default-trap-events - This filter matches all ALERT and EMERGENCY events. It also matches all Standard, Built-in SNMP trap type events.
- important-events - This filter matches all ALERT and EMERGENCY events.
- no-info-debug-events - This filter matches all non-INFO and non-DEBUG messages (EMERGENCY, ALERT, ERROR and NOTICE).

The system-defined event filters cannot be modified or deleted.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-filter-name <text>] - Filter Name

Selects the event filters that match this parameter value.

[-position <integer>] - Rule Position

Selects the event filters that match this parameter value.

[-type {include|exclude}] - Rule Type

Selects the event filters that match this parameter value. The rule types are as follows:

- include - Events matching this rule are included in the specified filter.
- exclude - Events matching this rule are excluded in the specified filter.

[-message-name <text>] - Message Name

Selects the event filters that match this parameter value.

[-severity <text>,…] - Severity

Selects the events that match this parameter value. Severity levels:

- EMERGENCY - Disruption.
- ALERT - Single point of failure.
- ERROR - Degradation.
- NOTICE - Information.
- INFORMATIONAL - Information.
- DEBUG - Debug information.
- * - Includes all severities.

[-snmp-trap-type <text>,…] - SNMP Trap Type

Selects the event filters that match this parameter value. The SNMP trap types are as follows:

- Standard - Traps defined in RFCs.
- Built-in - Enterprise traps specific to events.
- Severity-based - Traps specific to events that do not belong to the above two types.
- * - Includes all SNMP trap types.

[-parameter-criteria [key>=<value],…] - Parameter Criteria

Selects the event filters that match this parameter-criteria value.

[-system-defined {true|false}] - System-Defined Filter

Selects the event filters that match this parameter value.

[-access-control-role <text>] - Access Control Role (privilege: advanced)

Selects the event filters that match this parameter value.

Examples

The following example displays the event filters:

```
cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    include  *                *             Standard, Built-
in
                                                                   *=*
            4    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
9 entries were displayed.
```

The following example displays the event filters queried on the SNMP trap type value "Standard":

```
cluster1::> event filter show -snmp-trap-type Standard
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            3    include  *                *             Standard, Built-
in
                                                                   *=*
```

The following example displays the event filters with one or more rules that have no condition on the SNMP trap type. Note that the wildcard character has to be specified in double-quotes. Without double-quotes, output would be the same as not querying on the field.

```
cluster1::> event filter show -snmp-trap-type "*"
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            4    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
8 entries were displayed.
```

event filter test

Test an event filter

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter test` command is used to test an event filter. When specified with a message name, the command displays whether the message name is included or excluded from the filter. When specified without a message name, the command displays the number of events from the catalog that match the filter. For more information, see the event filter create command.

Parameters

`-filter-name <text>` - Filter Name

Use this mandatory parameter to specify the name of the event filter to test.

`[-message-name <Message Name>]` - Message Name

Use this optional parameter to specify the message name of the event to test against the filter.

Examples

The following example tests an event filter named err-wafl-no-scan-but-clone:

```
cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
err-wafl-no-scan-but-clone
            1    include  wafl.scan.clone.*
                                          *             *         *=*
            2    exclude  wafl.scan.*      *             *         *=*
            3    include  wafl.*           EMERGENCY, ALERT, ERROR
                                                         *         *=*
            4    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
```

```
Filter      Rule Rule                                      SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
no-info-debug-events
            2    exclude  *                *             *         *=*
12 entries were displayed.

cluster1::> event filter test -filter-name err-wafl-no-scan-but-clone
271 events will be included in the given filter.

cluster1::> event filter test -filter-name err-wafl-no-scan-but-clone
-message-name wafl.scan.clone.split.cantLock
The message-name "wafl.scan.clone.split.cantLock" is included in the given
filter.

cluster1::> event filter test -filter-name err-wafl-no-scan-but-clone
-message-name wafl.scan.layout.cantWrite
The message-name "wafl.scan.layout.cantWrite" is excluded from the given
filter.
```

Related Links

- event filter create

event filter update-access-control-role

Update access-control-role of an event filter

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

The `event filter update-access-control-role` command is used to update the 'access-control-role' field of an existing event filter.

Parameters

`-filter-name <text>` - Filter Name (privilege: advanced)

Specify the event filter name with this mandatory parameter.

`-new-access-control-role <text>` - New Access Control Role (privilege: advanced)

Specify the new access control role with this mandatory parameter.

Examples

This example shows how to update the access control role of an event filter named filter1:

```
cluster1::*> event filter show-summary
Filter Name         Rule Count  System-Defined Access Control Role
------------------  ----------  -------------- ------------------
default-trap-events
                    4           true           -
filter1             2           false          -
important-events    3           true           -
no-info-debug-events
                    2           true           -
4 entries were displayed.

cluster1::*> event filter update-access-control-role -filter-name filter1
-new-access-control-role new_role

cluster1::*> event filter show-summary
Filter Name         Rule Count  System-Defined Access Control Role
------------------  ----------  -------------- ------------------
default-trap-events
                    4           true           -
filter1             2           false          new_role
important-events    3           true           -
no-info-debug-events
                    2           true           -
4 entries were displayed.
```

event filter rule add

Add a rule for an event filter

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter rule add` command adds a new rule to an existing event filter. See event filter create for more information on event filters and how to create a new event filter.

Parameters

`-filter-name <text>` - Filter Name

Use this mandatory parameter to specify the name of the event filter to add the rule. Rules cannot be added to system-defined event filters.

[-position <integer>] - Rule Position

Use this optional parameter to specify the position of the rule in the event filter. It should be in the range (1..n-1), where 'n' is the position of the last rule, which is an implicit rule. Rules are checked in the order they are listed for a filter, until a match is found.

-type {include|exclude} - Rule Type

Use this mandatory parameter to specify the type of the rule which determines whether to include or exclude the events that match this rule.

[-message-name <text>] - Message Name

Use this parameter to specify the message name of the event to include or exclude from the filter.

[-severity <text>,…] - Severity

Use this parameter to specify the list of severity values to match against the events. Enter multiple severities separated by a comma. To enter all severities, the wild card (*) can be used. The wild card cannot be specified with other severities. The default value is *.

[-snmp-trap-type <text>,…] - SNMP Trap Type

Use this parameter to specify the list of the SNMP trap type values to match against the events. Enter multiple SNMP trap types seperated by comma. To enter all SNMP trap types, the wild card (*) can be used. The wild card cannot be specified with other SNMP trap types. The default value is *.

[-parameter-criteria [key>=<value],…] - Parameter Criteria

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

Examples

The following example adds a rule to an existing event filter "emer-and-wafl": All events with severity EMERGENCY and message name starting with "wafl.**" are included in the filter. Not specifiying the SNMP trap type implies a default value of ""**.

```
cluster1::> event filter rule add -filter-name emer-and-wafl -type include
-message-name wafl.*  -severity EMERGENCY
cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
emer-and-wafl
            1    include  wafl.*           EMERGENCY     *         *=*
            2    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
10 entries were displayed.
```

The following example adds a rule to the event filter "emer-and-wafl" at position 1: All events with severity ALERT and message name starting with "wafl.scan.*" are included in the filter.

```
cluster1::> event filter rule add -filter-name emer-and-wafl -type include
-message-name wafl.scan.* -position 1 -severity ALERT

cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
emer-and-wafl
            1    include  wafl.scan.*      ALERT         *         *=*
            2    include  wafl.*           EMERGENCY     *         *=*
            3    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
11 entries were displayed.
```

The following example adds a rule to the event filter "emer-and-wafl" to include all "Standard" SNMP trap type events:

```
cluster1::> event filter rule add -filter-name emer-and-wafl -type include
-snmp-trap-type Standard

cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
emer-and-wafl
            1    include  wafl.scan.*      ALERT         *         *=*
            2    include  wafl.*           EMERGENCY     *         *=*
            3    include  *                *             Standard  *=*
            4    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
12 entries were displayed.
```

The following example adds a rule to the event filter "emer-and-wafl" to include all "wafl" events whose parameters have a parameter named "type" and its value matches "volume":

```
cluster1::> event filter rule add -filter-name emer-and-wafl -type include
-message-name wafl.* -position 1 -parameter-criteria type=volume

cluster1::> event filter show -filter-name emer-and-wafl
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
emer-and-wafl
            1    include  wafl.*           *             *
type=volume
            2    include  wafl.scan.*      ALERT         *         *=*
            3    include  wafl.*           EMERGENCY     *         *=*
            4    include  *                *             Standard  *=*
            5    exclude  *                *             *         *=*
5 entries were displayed.
```

Related Links

- event filter create

event filter rule delete

Delete a rule for an event filter

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter rule delete` command deletes a rule from an event filter. The position of all the rules following the deleted rule is updated to maintain a contiguous sequence. Use event filter show command to view the filters and the rules associated with them.

Parameters

`-filter-name <text>` - Filter Name

Use this mandatory parameter to specify the name of the event filter from which you want to delete the rule. Rules cannot be deleted from system-defined filters.

`-position <integer>` - Rule Position

Use this mandatory parameter to specify the position of the rule to delete from the filter. It should be in the range (1..n-1), where 'n' is the position of the last rule, which is an implicit rule.

Examples

The following example deletes a rule at position 2 from an existing event filter "emer-and-wafl":

```
cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
emer-and-wafl
            1    include  wafl.scan.*      ALERT         *         *=*
            2    include  wafl.*           EMERGENCY     *         *=*
            3    include  *                *             Standard  *=*
            4    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
12 entries were displayed.
cluster1::> event filter rule delete -filter-name emer-and-wafl -position
2

cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
emer-and-wafl
```

```
            1    include  wafl.scan.*      ALERT          *          *=*
            2    include  *                *              Standard   *=*
            3    exclude  *                *              *          *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *          *=*
            2    include  callhome.*       ERROR          *          *=*
            3    exclude  *                *              *          *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *          *=*
            2    exclude  *                *              *          *=*
11 entries were displayed.
```

Related Links

- event filter show

event filter rule reorder

Modify the index of a rule for an event filter

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `event filter rule reorder` command moves a rule to a new position in an existing event filter. Use event filter show command to display all the event filters and the rules associated with them.

Parameters

`-filter-name <text>` - Filter Name

Use this mandatory parameter to specify the name of the event filter from which you want to change the position of the rule. Rules from system-defined event filters cannot be modified.

`-position <integer>` - Rule Positon

Use this mandatory parameter to specify the position of the rule you want to change. It should be in the range (1..n-1), where 'n' is the position of the last rule, which is an implicit rule.

`-to-position <integer>` - New Rule Position

Use this mandatory parameter to specify the new position to move the rule. It should be in the range (1..n-1), where 'n' is the position of the last rule, which is an implicit rule.

Examples

The following example changes the position of a rule from 1 to 2 from an existing event filter "emer-and-wafl":

```
cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
emer-and-wafl
            1    include  wafl.scan.*      ALERT         *         *=*
            2    include  *                *             Standard  *=*
            3    exclude  *                *             *         *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  callhome.*       ERROR         *         *=*
            3    exclude  *                *             *         *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *         *=*
            2    exclude  *                *             *         *=*
11 entries were displayed.

cluster1::> event filter rule reorder -filter-name emer-and-wafl -position
1 -to-position 2

cluster1::> event filter show
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
default-trap-events
            1    include  *                EMERGENCY, ALERT
                                                         *         *=*
            2    include  *                *             Standard, Built-
in
                                                                   *=*
            3    exclude  *                *             *         *=*
emer-and-wafl
            1    include  *                *             Standard  *=*
```

```
            2    include  wafl.scan.*      ALERT          *          *=*
            3    exclude  *                *              *          *=*
important-events
            1    include  *                EMERGENCY, ALERT
                                                         *          *=*
            2    include  callhome.*       ERROR          *          *=*
            3    exclude  *                *              *          *=*
no-info-debug-events
            1    include  *                EMERGENCY, ALERT, ERROR, NOTICE
                                                         *          *=*
            2    exclude  *                *              *          *=*
11 entries were displayed.
```

Related Links

- event filter show

Copyright information

Trademark information