event catalog commands

Command reference

NetApp
July 17, 2026

Table of Contents

event catalog commands

event catalog show

Display event definitions

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

Description

The `event catalog show` command displays information about events in the catalog. By default, this command displays the following information:

- Message name of the event
- Severity of the event
- SNMP trap type of the event

To display detailed information about a specific event, run the command with the `-message-name` parameter, and specify the name of the event. The detailed view adds the following information:

- Full description of the event
- Action to be taken to address the event
- Event's deprecation status

You can specify additional parameters to limit output to the information that matches those parameters. For example, to display information only about events with an event name that begins with *`raid`* , enter the command with the `-message-name` *`raid*`* parameter. The parameter value can either be a specific text string or a wildcard pattern.

Alternatively, an event filter can also be specified to limit the output events.

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.

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

Selects the events that match this parameter value.

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

Selects the events that match this parameter value. The parameter value indicates an existing filter name that, when applied permits the inclusion of the listed events.

[-severity {EMERGENCY|ALERT|ERROR|NOTICE|INFORMATIONAL|DEBUG}] - Severity

Selects the events that match this parameter value.

[-description <text>] - Description

Selects the events that match this parameter value.

[-action <text>] - Corrective Action

Selects the events that match this parameter value.

[-snmp-trap-type {Standard|Built-in|Severity-based}] - SNMP Trap Type

Selects the events that match this parameter value. The parameter value describes the type of SNMP trap associated with the event. The value can be one of the following: *Standard* trap type events are those defined in the RFCs. *Built-in* trap types are those that are NetApp Enterprise traps specific to events. The remaining events are considered to have *Severity-based* SNMP trap types.

[-deprecated {true|false}] - Is Deprecated

Selects the events that match this parameter value. The parameter value indicates whether the event is deprecated or not.

Deprecated events may be removed in a future release of ONTAP.

Examples

The following example displays the event catalog:

```
cluster1::> event filter show -filter-name filter1
Filter      Rule Rule                                    SNMP Trap
Name        Posn Type     Message Name     Severity      Type
Parameters
----------- ---- -------- ---------------- ------------- ---------
-----------
filter1
            1    include  zapi.*           *             *         *=*
            2    exclude  *                *             *         *=*
2 entries were displayed.

cluster1::> event catalog show -filter-name filter1
Message                          Severity         SNMP Trap Type
-------------------------------- ---------------- -----------------
zapi.killed                      NOTICE           Severity-based
zapi.method.notfound             NOTICE           Severity-based
zapi.sf.up.ready                 INFORMATIONAL    Severity-based
zapi.snapshot.success            NOTICE           Severity-based
zapi.streamout.noMethod          NOTICE           Severity-based
5 entries were displayed.

cluster1::> event catalog show -message-name zsm.* -filter-name filter1
```

```
There are no entries matching your query.

cluster1::> event catalog show -message-name zapi.* -filter-name filter1
Message                              Severity         SNMP Trap Type
-------------------------------- ---------------- -----------------
zapi.method.notfound                 NOTICE           Severity-based
zapi.sf.up.ready                     INFORMATIONAL    Severity-based
zapi.snapshot.success                NOTICE           Severity-based
zapi.streamout.noMethod              NOTICE           Severity-based
4 entries were displayed.

cluster1::> event catalog show -message-name CR.*
Message                              Severity         SNMP Trap Type
-------------------------------- ---------------- -----------------
CR.Corrupt.Redir.Deleted             INFORMATIONAL    Severity-based
CR.Dangling.Redir.Deleted            INFORMATIONAL    Severity-based
CR.Data.File.Inaccessible            NOTICE           Severity-based
CR.Del.Corrupt.Redir.Failed          NOTICE           Severity-based
CR.Del.CrptStreamData.Fail           NOTICE           Severity-based
CR.Del.CrptStreamRedir.Fail          NOTICE           Severity-based
CR.Del.DangStreamData.Fail           NOTICE           Severity-based
CR.Del.DangStreamRedir.Fail          NOTICE           Severity-based
CR.Del.Dangling.Redir.Failed         NOTICE           Severity-based
CR.Fix.Corrupt.Redir.Failed          NOTICE           Severity-based
CR.Fix.Crpt.Data.Dir.Failed          INFORMATIONAL    Severity-based
CR.Fix.Crpt.Data.File.Failed         NOTICE           Severity-based
CR.Fix.CrptStreamRedir.Fail          NOTICE           Severity-based
CR.Fix.Dang.Data.File.Failed         NOTICE           Severity-based
CR.Fix.Nlinks.Failed                 NOTICE           Severity-based
CR.Fix.TempFiles.Failed              INFORMATIONAL    Severity-based
CR.Max.Session.Exceed                INFORMATIONAL    Severity-based
CR.RDB.Counters.Not.Updated          INFORMATIONAL    Severity-based
CR.RDB.State.Not.Updated             NOTICE           Severity-based
CR.Redir.File.Inaccessible           NOTICE           Severity-based
CR.Snapshot.Not.Deleted              NOTICE           Severity-based

Message                              Severity         SNMP Trap Type
-------------------------------- ---------------- -----------------
CR.Sync.ACL.Fail                     NOTICE           Severity-based
22 entries were displayed.

cluster1::> event catalog show -instance
...
...
     Message Name: Nblade.cifsEncSessAccessDenied
         Severity: ERROR
```

```
      Description: This message occurs when a client not capable of SMB
encryption tries to establish a CIFS session that requires SMB encryption.
Corrective Action: Either ensure that the client is capable of SMB
encryption or disable SMB encryption on the Vserver.
   SNMP Trap Type: Severity-based
    Is Deprecated: false
Message Name: Nblade.cifsEncShrAccessDenied
         Severity: ERROR
      Description: This message occurs when a client not capable of SMB
encryption tries to connect to a CIFS share that requires SMB encryption.
Corrective Action: Either ensure that the client is capable of SMB
encryption or disable SMB encryption on the CIFS share.
   SNMP Trap Type: Severity-based
    Is Deprecated: false
...
...
```

Copyright information

Trademark information