



event log commands

ONTAP 9.7 commands

NetApp
December 14, 2022

Table of Contents

- event log commands 1
- event log show 1

event log commands

event log show

Display latest log events

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

Description

The `event log show` command displays the contents of the event log, which lists significant occurrences within the cluster. Use the [event catalog show](#) command to display information about events that can occur.

By default, the command displays EMERGENCY, ALERT and ERROR severity level events with the following information, with the most recent events listed first:

- The time at which the event occurred
- The node on which the event occurred
- The severity of the event
- The event's message

To display detailed information about events, use one or more of the optional parameters that affect how the command output is displayed and the amount of detail that is included. For example, to display all detailed event information, use the `-detail` parameter.

To display NOTICE, INFORMATIONAL or DEBUG severity level events, use the `-severity` parameter.

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.

| [-detail]

Displays additional event information such the sequence number of the event.

| [-detailtime]

Displays detailed event information in reverse chronological order.

| [-instance] }

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

[-node {<nodename>|local}] - Node

Displays a list of events for the node you specify. Use this parameter with the `-seqnum` parameter to display detailed information.

[-seqnum <Sequence Number>] - Sequence#

Selects the events that match this parameter value. Use with the `-node` parameter to display detailed

information.

[-time <MM/DD/YYYY HH:MM:SS>] - Time

Selects the events that match this parameter value. Use the format: MM/DD/YYYY HH:MM:SS [+ HH:MM]. You can specify a time range by using the ".." operator between two time statements.

```
show -time "08/13/2010 05:55:00".. "08/13/2010 06:10:00"
```

Comparative time values are relative to "now". For example, to display only events that occurred within the last minute:

```
show -time >1m
```

+
NOTE: The month and date fields of this parameter are not zero-padded. These fields can be single digits: for example, "7/1/2019 05:55:00".

+

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

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

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

To display all events, including ones with severity levels of NOTICE, INFORMATIONAL and DEBUG, specify severity as follows:

```
show -severity <=DEBUG
```

[-ems-severity

{NODE_FAULT|SVC_FAULT|NODE_ERROR|SVC_ERROR|WARNING|NOTICE|INFO|DEBUG|VAR}] - EMS Severity

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

- NODE_FAULT - Data corruption has been detected or the node is unable to provide client service
- SVC_FAULT - A temporary loss of service, typically a transient software fault, has been detected
- NODE_ERROR - A hardware error that is not immediately fatal has been detected
- SVC_ERROR - A software error that is not immediately fatal has been detected
- WARNING - A high-priority message that does not indicate a fault

- NOTICE - A normal-priority message that does not indicate a fault
- INFO - A low-priority message that does not indicate a fault
- DEBUG - A debugging message
- VAR - A message with variable severity, selected at runtime.

[-source <text>] - Source

Selects the events that match this parameter value (typically a software module).

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

Selects the events that match this parameter value (string). Message names are descriptive, so filtering output by message name displays messages of a specific type.

[-event <text>] - Event

Selects the events that match this parameter value. The "event" field contains the full text of the event, including any parameters. For example, a waf.vol.offline event will contain the name of the volume taken offline.

[-kernel-generation-num <integer>] - Kernel Generation Number

Selects the events that match this parameter value. Only events that emanate from the kernel have kernel generation numbers.

[-kernel-sequence-num <integer>] - Kernel Sequence Number

Selects the events that match this parameter value. Only events that emanate from the kernel have kernel sequence numbers.

[-action <text>] - Corrective Action

Selects the events that match this parameter value. The "action" field describes what steps, if any, you must take to remedy the situation.

[-description <text>] - Description

Selects the events that match this parameter value. The "description" field describes why the event was encountered and what it means.

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

Selects the events that match this parameter value. Only events that were included by existing filters that match this value are displayed.

Examples

The following example displays the event log:

```

cluster1::> event log show
Time                Node                Severity          Event
-----
-----
11/9/2015 13:54:19  node1                NOTICE           vifmgr.portup: A link
up event was received on node node1, port e0a.
11/9/2015 13:54:19  node1                NOTICE           vifmgr.portup: A link
up event was received on node node1, port e0d.
11/9/2015 13:54:19  node1                NOTICE           vifmgr.portup: A link
up event was received on node node1, port e0c.
11/9/2015 13:54:19  node1                NOTICE           vifmgr.portup: A link
up event was received on node node1, port e0b.
...

```

This example demonstrates how to use a range with the `-time` parameter to display all events that occurred during an extended time period. It displays all events that occurred between 1:45pm and 1:50pm on November 9, 2010.

```

cluster1::> event log show -time "11/9/2015 13:45:00".."11/9/2015 13:50:0"

```

The `-time` parameter also accepts values that are relative to "now". The following example displays events that occurred more than one hour ago:

```

cluster1::event log> show -time <1h
Time                Node                Severity          Event
-----
-----
11/9/2015 13:02:03  node1                INFORMATIONAL     monitor.globalStatus.ok: The system's global status is normal.
11/9/2015 13:02:03  node2                INFORMATIONAL     monitor.globalStatus.ok: The system's global status is normal.
...

```

Severity levels sort in the order opposite to what you might expect. The following example displays all events that have a severity level of ERROR or more severe:

```

cluster1::> event log show -severity <ERROR

```

Related Links

- [event catalog show](#)

Copyright information

Copyright © 2022 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.