event notification commands

ONTAP 9.8 commands

NetApp
September 27, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-98/event-notification-create.html on September 27, 2022. Always check docs.netapp.com for the latest.

Table of Contents

event notification commands

event notification create

Create an event notification

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

Description

The ` event notification create` command is used to create a new notification of a set of events defined by an event filter to one or more notification destinations.

Parameters

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

Use this mandatory parameter to specify the name of the event filter. Events that are included in the event filter are forwarded to the destinations specified in the destinations parameter.

The filter name passed to this command must be an existing filter. For more information, see the event filter create command.

`-destinations <text>,…` - List of Event Notification Destinations

Use this mandatory parameter to specify the list of destinations to which the notification should be forwarded. Enter multiple destinations separated by a comma.

The destination passed to this command must be an existing destination. For more information, see the event destination create command.

Examples

The following example creates an event notification for filter name "filter1" to destinations "email_dest, snmp-traphost and syslog_dest":

```
cluster1::> event notification destination show
                            Hide
Name            Type        Params   Destination
--------------  ----------  ------   --------------------
email_dest      email       false    test@example.com
snmp-traphost   snmp        true     10.27.12.1 (from "system snmp
traphost")
syslog_dest     syslog      false    10.23.12.1
3 entries were displayed.

cluster1::> event filter show -filter-name filter1
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
filter1
            1        exclude   callhome.bad.ram       *               *
            2        include   callhome.*             *
ALERT, ERROR
            3        exclude   *                      *               *
3 entries were displayed.

cluster1::> event notification create -filter-name filter1 -destinations
email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1      filter1           email_dest, syslog_dest, snmp-traphost
```

Related Links

- event filter create
- event destination create

event notification delete

Delete event notifications

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

Description

The `event notification delete` command deletes an existing event notification.

Parameters

-ID <integer> - Event Notification ID

Use this parameter to specify the ID of the notification to be deleted.

Examples

The following example shows the deletion of event notification with ID 1:

```
cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1      filter1           email_dest, syslog_dest, snmp-traphost

cluster1::> event notification delete -ID 1

cluster1::> event notification show
This table is currently empty.
```

event notification modify

Modify event notifications

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

Description

The `event notification modify` command is used to modify an existing notification.

Parameters

-ID <integer> - Event Notification ID

Use this mandatory parameter to specify the ID of the notification to be modified.

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

Use this parameter to specify the filter name to be modified.

[-destinations <text>,…] - List of Event Notification Destinations

Use this parameter to specify the destinations to be modified. Enter multiple destinations separated by a comma.

Provide the complete set of destinations to be modified. Individual destination cannot be added or removed.

Examples

The following example shows the modification of event notification with ID 1:

```
cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1      filter1           email_dest, syslog_dest, snmp-traphost

cluster1::> event notification modify -ID 1 -destinations email_dest,
syslog_dest

cluster1::>  event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1      filter1           email_dest, syslog_dest
```

event notification show

Display event notifications

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

Description

The `event notification show` command is used to display the list of existing event notifications.

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.

[-ID <integer>] - Event Notification ID

Use this parameter to display the detailed information about the notification ID you specify.

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

Use this parameter to display event notifications that use the filter-name you specify.

[-destinations <text>,…] - List of Event Notification Destinations

Use this parameter to display event notifications that use the destinations you specify.

Examples

The following example displays the event notification:

```
cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1      filter1           email_dest, syslog_dest, snmp-traphost
```

event notification destination create

Create an event notification destination

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

Description

The `event notification destination create` command creates a new event notification destination of either email or syslog type.

The following system-defined notification destination is configured for your use:

- snmp-traphost - This destination reflects the configuration in "system snmp traphost".

Parameters

`-name <text>` - Destination Name

Use this mandatory parameter to specify the name of the notification destination that is to be created. An event notification destination name must be 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.

{ `-email <mail address>` - Email Destination

Use this parameter to specify the email address to which event notifications will be sent. For events to properly generate email notifications, the event system must also be configured with an address and mail server from which the mail will be sent. See event config modify command for more information.

| `-syslog <text>` - Syslog Destination

Use this parameter to specify syslog server host name or IP address to which syslog entries will be sent.

| `-rest-api-url <text>` - REST API Server URL

Use this parameter to specify REST API server URL to which event notifications will be sent. Enter the full URL, which must start either with an http:// or https:// prefix. To specify a URL that contains a question mark, press ESC followed by the "?". + If an https:// URL is specified, then Data ONTAP verifies the identity of the destination host by validating its certificate. If the Online Certificate Status Protocol (OCSP) is enabled for EMS, then Data ONTAP uses that protocol to determine the certificate's revocation status. Use the `security config oscp show -application ems` command to determine if the OCSP-based certificate revocation status check is enabled for EMS.

`[-certificate-authority <text>]` - Client Certificate Issuing CA

Use this parameter to specify the name of the certificate authority (CA) that signed the client certificate that will be sent in case mutual authentication with the REST API server is required. + There can be multiple client certificates installed for the admin vserver in the cluster, and this parameter, along with the *`certificate-serial`* parameter, uniquely identifies which one. + Use the security certificate show

command to see the list of certificates installed in the cluster.

[-certificate-serial <text>] - Client Certificate Serial Number }

Use this parameter to specify the serial number of the client certificate that will be sent in case mutual authentication with the REST API server is required.

Examples

The following example shows the creation of a new event notification destination of type email called "StorageAdminEmail":

```
cluster1::> event notification destination create -name StorageAdminEmail
-email StorageAdmin@example.com

cluster1::> event notification destination show

Name            Type        Destination
--------------  ----------  --------------------
StorageAdminEmail
                email       StorageAdmin@example.com
snmp-traphost   snmp        10.30.40.10 (from "system snmp traphost")
2 entries were displayed.
```

The following example shows the creation of a new event notification destination of type rest-api called "RestApi":

```
cluster1::> event notification destination create -name RestApi -rest-api
-url https://rest.example.com/rest
-certificate-authority cluster1-root-ca -certificate-serial 052213E60B7088

cluster1::> event notification destination show -name RestApi -instance
Destination Name: RestApi
             Type of Destination: rest-api
              Destination Values: https://rest.example.com/rest
   Client Certificate Issuing CA: cluster1-root-ca
Client Certificate Serial Number: 052213E60B7088
```

Related Links

- event config modify
- security certificate show

event notification destination delete

Delete existing event destinations

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

Description

The `event notification destination delete` command deletes an event notification destination.

The following system-defined notification destination is configured for your use:

- snmp-traphost - This destination reflects the configuration in "system snmp traphost". To remove snmp-traphost addresses, use the `system snmp traphost` command.

Parameters

`-name <text>` - Destination Name

Use this mandatory parameter to specify the name of an event destination to be removed.

Examples

The following shows the examples of deleting event notification destinations:

```
cluster1::> event notification destination show
Name            Type        Destination
    -------------  ----------  --------------------
    StorageAdminEmail
                   email       StorageAdmin@example.com
    StorageAdminSyslog
                   syslog      example.com
    snmp-traphost   snmp        10.30.40.10 (from "system snmp traphost")
    3 entries were displayed.
cluster1::> event notification destination delete -name StorageAdminEmail

    cluster1::> event notification destination show

    Name            Type        Destination
    -------------  ----------  --------------------
    StorageAdminSyslog
                   syslog      example.com
    snmp-traphost   snmp        10.30.40.10 (from "system snmp traphost")
    2 entries were displayed.
cluster1::> event notification destination delete -name Storage*
cluster1::> event notification destination show
Name            Type        Destination
    -------------  ----------  --------------------
    snmp-traphost   snmp        10.30.40.10 (from "system snmp traphost")
    1 entries were displayed.
```

event notification destination modify

Modify an event notification destination

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

Description

The `event notification destination modify` command modifies event notification destination.

The following system-defined notification destination is configured for your use:

- snmp-traphost - This destination reflects the configuration in "system snmp traphost". To modify traphost addresses, use the `system snmp traphost` command.

Parameters

`-name <text>` - Destination Name

Use this mandatory parameter to specify the name of an event notification destination to be modified. The name of the destination must already exist.

{ `[-email <mail address>]` - Email Destination

Use this parameter to specify a new value of email address to replace the current address in the event notification destination. The parameter is specified only when the event notification destination type is already "email". It is not allowed to specify the parameter for a destination that already has another type of destination address.

| `[-syslog <text>]` - Syslog Destination

Use this parameter to specify a new syslog server host name or IP address to replace the current address of the event notification destination. The parameter is specified only when the event notification destination type is already "syslog". It is not allowed to specify the parameter for a destination that already has another type of destination address.

| `[-rest-api-url <text>]` - REST API Server URL

Use this parameter to specify a new REST API server URL to replace the current address of the event notification destination. Enter the full URL, which must start either with an http:// or https:// prefix. + To specify a URL that contains a question mark, press ESC followed by the "?". + If an https:// URL is specified, then Data ONTAP verifies the identity of the destination host by validating its certificate. If the Online Certificate Status Protocol (OCSP) is enabled for EMS, then Data ONTAP uses that protocol to determine the certificate's revocation status. Use the `security config oscp show -application ems` command to determine if the OCSP-based certificate revocation status check is enabled for EMS. The parameter is specified only when the event notification destination type is already "rest-api". It is not allowed to specify the parameter for a destination that already has another type of destination address.

`[-certificate-authority <text>]` - Client Certificate Issuing CA

Use this parameter to specify a new value of the certificate authority (CA) to replace the current value in the event notification destination. There can be multiple client certificates installed for the admin vserver in the cluster, and this parameter, along with the *`certificate-serial`* parameter, uniquely identifies which one. + Use the security certificate show command to see the list of certificates installed in the cluster.

[-certificate-serial <text>] - Client Certificate Serial Number }

Use this parameter to specify a new serial number of the client certificate to replace the current value in the event notification destination.

Examples

The following example shows the modification of event notification destinations:

```
cluster1::> event notification destination show

Name            Type        Destination
--------------  ----------  --------------------
StorageAdminEmail
                email       Storage@example.com
StorageAdminSyslog
                syslog      example.com
snmp-traphost   snmp        10.30.40.10 (from "system snmp traphost")
3 entries were displayed.

cluster1::> event notification destination modify -name StorageAdminEmail
-email StorageAdmin@example.com

cluster1::> event notification destination show

Name            Type        Destination
--------------  ----------  --------------------
StorageAdminEmail
                email       StorageAdmin@example.com
StorageAdminSyslog
                syslog      example.com
snmp-traphost   snmp        10.30.40.10 (from "system snmp traphost")
3 entries were displayed.
```

The following example shows how to clear the client certificate configuration when mutual authentication with the REST API server is no longer required:

```
cluster1::> event notification destination show -name RestApi -instance
Destination Name: RestApi
             Type of Destination: rest-api
              Destination Values: https://rest.example.com/rest
   Client Certificate Issuing CA: cluster1-root-ca
Client Certificate Serial Number: 052213E60B7088

cluster-1::> event notification destination modify -name RestApi
-certificate-authority - -certificate-serial -

cluster-1::> event notification destination show -name RestApi -instance
Destination Name: RestApi
             Type of Destination: rest-api
              Destination Values: https://rest.example.com/rest
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
```

Related Links

- security certificate show

event notification destination show

Display event notification destinations

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

Description

The `event notification destination show` command displays event notification destinations. Note: In the case of a rest-api destination type, OCSP information is not included. It's available in security config ocsp show -app ems 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.

[-name <text>] - Destination Name

Use this optional parameter to display information of an event notification destination that has the specified name.

[-type {snmp|email|syslog|rest-api}] - Type of Destination

Use this optional parameter to display information of event notification destinations that have the specified destination type.

[-destination <text>,…] - Destination

Use this optional parameter to display information of event notification destinations that have the specified destination address. Enter multiple addresses separated by a comma.

[-server-ca-present {true|false}] - Server CA Certificates Present?

Use this optional parameter to display information of event notification destinations that have the specified server-ca-present value. This field indicates whether there are certificates of the server-ca type exist in the system. If not, event messages will not be sent to a rest-api type destination having an HTTPS URL.

[-certificate-authority <text>] - Client Certificate Issuing CA

Use this optional parameter to display information of event notification destinations that have the specified certificate authority name.

[-certificate-serial <text>] - Client Certificate Serial Number

Use this optional parameter to display information of event notification destinations that have the specified certificate serial number.

[-certificate-valid {true|false}] - Client Certificate Valid?

Use this optional parameter to display information of event notification destinations that have the specified certificate-valid value. This field indicates whether the client certificate specified by the certificate-authority and certificate-serial fields is valid. If not, and if the REST API server requires client authentication, event messages will not be sent to the server.

Examples

The following shows examples of "event notification destination show":

```
cluster1::> event notification destination show

Name            Type        Destination
--------------  ----------  --------------------
StorageAdminEmail
                email       StorageAdmin@example.com
StorageAdminSyslog
                syslog      example.com
snmp-traphost   snmp        10.30.40.10 (from "system snmp traphost")
RestApi         rest-api    https://rest.example.com/rest
4 entries were displayed.

cluster1::> event notification destination show -type snmp -instance
Destination Name: snmp-traphost
    Type of Destination: snmp
     Destination values: 10.30.40.10 (from "system snmp traphost")
```

Related Links

- security config ocsp show

event notification history show

Display latest events sent to destination

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

Description

The `event notification history show` command displays a list of event messages that have been sent to a notification destination. Information displayed by the command for each event is identical to that of the event log show command. This command displays events sent to a notification destination while the event log show command displays all events that have been logged.

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.

-destination <text> - Destination

Specifies the destination to which event messages have been sent to be displayed.

[-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.

[-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.

[-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. This parameter is useful when entered with wildcards. The "event" field contains the full text of the event, including any parameters. For example, the wafl.vol.offline event displays the name of the volume that is taken offline.

Examples

The following example displays all the events which match "important-events" filter and forwarded to the "snmp-traphost" destination:

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

cluster1::> event notification destination show
Name            Type        Destination
--------------  ----------  --------------------
snmp-traphost   snmp        192.168.10.40 (from "system snmp traphost")

cluster1::> event notification show
ID      Filter Name       Destinations
------- ---------------  -----------------
1       important-events  snmp-traphost

cluster1::>event notification history show -destination snmp-traphost
Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
5/14/2015 03:02:09  node1            EMERGENCY     callhome.clam.node.ooq:
Call home for NODE(S) OUT OF CLUSTER QUORUM.
5/13/2015 12:05:45  node1            ALERT         od.rdb.mbox.read.error:
message="RDB-HA readPSlot: Failed to read blob_type 19, (pslot 16),
instance 1: 1 (1)."
2 entries were displayed.
```

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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.