system snmp commands

ONTAP 9.11.1 commands

NetApp
May 23, 2023

Table of Contents

system snmp commands

system snmp authtrap

Enables or disables SNMP authentication traps

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

Description

Use this command to either enable or disable the standard SNMP authentication failure traps.

Parameters

`[-authtrap <integer>]` - Enables SNMP Authentication Trap

Enter the value of 1 to enable SNMP authentication failure traps. By default, SNMP authentication trap is disabled and the value is 0.

Examples

The following example demonstrates how to set the SNMP authtrap. +

```
cluster1::> system snmp authtrap -authtrap 1
uster1::> system snmp show
contact:
        private
location:
        NB
authtrap:
        1
init:
        0
traphosts:
        -
community:
               -   -
```

system snmp contact

Displays or modifies contact details

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

Description

Sets the contact name as the System.sysContact.0 MIB-II variable.

Parameters

`[-contact <text>]` - Contact

Specifies the contact name. Without any value specified, this command displays current setting of contact name.

Examples

The following example sets the contact name for SNMP. +

```
cluster1::> system snmp contact -contact private
uster1::> system snmp show
contact:
        private
location:
        NB
authtrap:
        1
init:
        0
traphosts:
        -
community:
               -   -
```

system snmp enable-snmpv3

Enables SNMPv3 cluster-wide

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

Description

The `system snmp enable-snmpv3` command enables SNMPv3 server on the entire cluster. When this command is run, SNMP users and SNMP traphosts that are non-compliant to FIPS will be deleted automatically, since cluster FIPS mode is enabled. Any SNMPv1 user, SNMPv2c user or SNMPv3 user (with none or MD5 as authentication protocol or none or DES as encryption protocol or both) is non-compliant to FIPS. Any SNMPv1 traphost or SNMPv3 traphost (configured with an SNMPv3 user non-compliant to FIPS) is non-compliant to FIPS.

Examples

The following command enables SNMPv3 server on the entire cluster, within a cluster named cluster1:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y

cluster1::*> system snmp enable-snmpv3

Warning: If you enable SNMPv3 using this command, any SNMP users and
         SNMP traphosts that are non-compliant to FIPS will be
         deleted automatically, since cluster FIPS mode is enabled.
         Any SNMPv1 user, SNMPv2c user or SNMPv3 user (with none or
         MD5 as authentication protocol or none or DES as encryption
         protocol or both) is non-compliant to FIPS. Any SNMPv1
         traphost or SNMPv3 traphost (configured with an SNMPv3 user
         non-compliant to FIPS) is non-compliant to FIPS.
Do you want to continue? {y|n}: y

1 entry was modified.

cluster1::*>
```

system snmp init

Enables or disables SNMP traps

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

Description

Initializes or disables sending of traps by the SNMP daemon from the cluster.

Parameters

`[-init <integer>]` - Initialize Traps

Use the value of 1 to initialize SNMP daemon to send traps or use a value of 0 to stop sending traps from the cluster. If no value is specified, this command displays the current setting of init. Traps are enabled by default.

Examples

The following command initializes SNMP daemon to send traps. +

```
cluster1::> system snmp init -init 1
uster1::> system snmp show
contact:
        private
location:
        NB
authtrap:
        1
init:
        1
traphosts:
        -
community:
  -   -
```

system snmp location

Displays or modifies location information

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

Description

Sets the location name as the System.sysLocation.0 MIB-II variable.

Parameters

`[-location <text>]` - Location

Specifies the location details. If no value is specified, this command displays the current setting of location.

Examples

This command sets the location name. +

```
cluster1::> system snmp location -location NB
cluster1::> system snmp show
  contact:
          private
  location:
          NB
  authtrap:
          1
  init:
          1
  traphosts:
          -
  community:
    -   -
```

system snmp prepare-to-downgrade

Change SNMP configuration to the default settings for releases earlier than Data ONTAP 9.3.0

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

Description

The `system snmp prepare-to-downgrade` command prepares the SNMP subsystem for a downgrade or a revert. More specifically, it prepares the SNMPv3 client feature for a downgrade or a revert. It deletes all storage switches that were explicitly added for monitoring and are using SNMPv3 as the underlying protocol. It also deletes any cluster switches that are using SNMPv3 for monitoring. Finally, it deletes any remote switch SNMPv3 users configured in ONTAP.

Examples

The following command prepares the SNMP subsystem for a downgrade or a revert, within a cluster named cluster1:

```
cluster1::*> system snmp prepare-to-downgrade
```

system snmp show

Displays SNMP settings

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

Description

Lists the current values of all the SNMP parameters.

Examples

The example below shows a typical command display.

```
cluster1::> system snmp show
  contact:
          private
  location:
          NB
  authtrap:
          1
  init:
          1
  traphosts:
          xxx.example.com(xxx.example.com)(192.168.xxx.xxx)
  community:
    -   -
```

system snmp community add

Adds a new community with the specified access control type

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

Description

The `system snmp community add` command adds communities with the specified access control type. Only read-only communities are supported. There is no limit for the number of communities supported.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the Vserver to which the community will be added. If no Vserver is specified, the community is added to the admin Vserver.

`-community-name <text>` - Community

This parameter specifies the name of the community.

`-type <ctype>` - access type

This parameter specifies 'ro' for read-only community.

Examples

The following example adds the read-only community name 'private'.

```
cluster1::> system snmp community add -type ro
        -community-name private
cluster1::> system snmp community show
            ro  private
```

system snmp community delete

Deletes community with the specified access control type

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

Description

The `system snmp community delete` command deletes communities with the specified access control type. Only read-only communities are supported.

Parameters

`-vserver <Vserver Name>` - Vserver

This parameter specifies the Vserver from which you wish to delete the community. If no Vserver is specified, the community is deleted from the admin Vserver.

`-community-name <text>` - Community

Specify the name of the community.

`-type <ctype>` - access type

Specify 'ro' for a read-only community.

Examples

The following example deletes the read-only community 'private':

```
cluster1::> system snmp community delete -type ro
      -community-name private
uster1::> system snmp community show
This table is currently empty.
```

system snmp community show

Displays communities

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

Description

Displays the current list of SNMP communities.

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.

[-vserver <Vserver Name>] - Vserver

Selects the Vserver to which the SNMP community belongs

[-community-name <text>] - Community

Selects the SNMP v1/v2c community string

[-access <ctype>] - access

Selects the access type of the SNMP v1/v2c community. Read-only (ro) is the only access type supported

Examples

```
cluster1::> system snmp community show
cluster1
    ro private
```

system snmp traphost add

Add a new traphost

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

Description

Adds the SNMP manager who receives the SNMP trap PDUs. The SNMP manager can be a hostname or IP address. There is no limit on the number of traphosts supported.

Parameters

-peer-address <Remote InetAddress> - Remote IP Address

Specifies the IP address or hostname of the traphost. If the USM user is associated, then the SNMPv3 traps are generated for this traphost using the associated USM user's authentication and privacy credentials. If no USM user is associated, then the SNMP v1/v2c traps are generated for this traphost. For the SNMP v1/v2c traps, the default community string is 'public', when no community is defined. When the community strings are defined, then the first community string is chosen for the SNMP v1/v2c traps.

[-usm-username <text>] - USM User Name

Specifies a predefined SNMPv3 USM user. The SNMPv3 traps are generated using this USM user's authentication and privacy credentials for the traphost identified by the peer-address parameter.

Examples

In the following example, the command adds a hostname 'yyy.example.com' for the SNMPv3 traps: +

```
cluster1::> system snmp traphost add -peer-address yyy.example.com -usm
-username MyUsmUser
cluster1::> system snmp traphost show
                  yyy.example.com(yyy.example.com)(192.168.xxx.xxx)    USM
User: MyUsmUser
```

In the following example, the command adds a hostname 'xxx.example.com' for the SNMP v1/v2c traps: +

```
cluster1::> system snmp traphost add xxx.example.com
cluster1::> system snmp traphost show
                  yyy.example.com(yyy.example.com)(192.168.xxx.xxx)    USM
User: MyUsmUser
                  xxx.example.com(xxx.example.com)(xxx.xxx.xxx.xxx)
Community: public
```

system snmp traphost delete

Delete a traphost

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

Description

Deletes the SNMP manager, who receives the SNMP trap PDUs. The SNMP manager can be a hostname or IP address. There is no limit on the number of traphosts supported.

Parameters

-peer-address <Remote InetAddress> - Remote IP Address

Specifies the IP address or hostname of the traphost. If the USM user is associated, then specify the USM user to delete the traphost.

[-usm-username <text>] - USM User Name

Specifies the USM user associated with traphost.

Examples

In the following example, the command deletes the SNMPv3 traphost 'yyy.example.com' associated with the

USM user: +

```
cluster1::> system snmp traphost delete -peer-address yyy.example.com -usm
-username MyUsmUser
```

In the following example, the command deletes the SNMP v1/v2c traphost 'xxx.example.com' associated with a community string: +

```
cluster1::> system snmp traphost delete -peer-address xxx.example.com
```

system snmp traphost show

Displays traphosts

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

Description

Displays list of the SNMP v1/v2c and SNMP v3 managers, that receive trap PDUs.

Examples

In the following example, the command displays all the host names or IP addresses that have been added until now: +

```
cluster1::> system snmp traphost show
                yyy.example.com(yyy.example.com)(192.168.xxx.xxx)    USM
User: MyUsmUser
                xxx.example.com(xxx.example.com)(xxx.xxx.xxx.xxx)
Community: public
```

Copyright information

Trademark information