Manage SNMP on the cluster (cluster administrators only)

ONTAP 9

NetApp
June 15, 2021

Table of Contents

Manage SNMP on the cluster (cluster administrators only)

Overview

You can configure SNMP to monitor SVMs in your cluster to avoid issues before they occur, and to respond to issues if they do occur. Managing SNMP involves configuring SNMP users and configuring SNMP traphost destinations (management workstations) for all SNMP events. SNMP is disabled by default on data LIFs.

You can create and manage read-only SNMP users in the data SVM. Data LIFs must be configured to receive SNMP requests on the SVM.

SNMP network management workstations, or managers, can query the SVM SNMP agent for information. The SNMP agent gathers information and forwards it to the SNMP managers. The SNMP agent also generates trap notifications whenever specific events occur. The SNMP agent on the SVM has read-only privileges; it cannot be used for any set operations or for taking a corrective action in response to a trap. ONTAP provides an SNMP agent compatible with SNMP versions v1, v2c, and v3. SNMPv3 offers advanced security by using passphrases and encryption.

For more information about SNMP support in ONTAP systems, see TR-4220: SNMP Support in Data ONTAP.

What MIBs are

A MIB (Management Information Base) is a text file that describes SNMP objects and traps.

MIBs describe the structure of the management data of the storage system and they use a hierarchical namespace containing object identifiers (OIDs). Each OID identifies a variable that can be read by using SNMP.

Because MIBs are not configuration files and ONTAP does not read these files, SNMP functionality is not affected by MIBs. ONTAP provides the following MIB file:

- A NetApp custom MIB (`netapp.mib`)

ONTAP supports IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113), and ICMP (RFC 2466) MIBs, which show both IPv4 and IPv6 data, are supported.

ONTAP also provides a short cross-reference between object identifiers (OIDs) and object short names in the `traps.dat` file.

The latest versions of the ONTAP MIBs and `traps.dat `files are available on the NetApp Support Site. However, the versions of these files on the support site do not necessarily correspond to the SNMP capabilities of your ONTAP version. These files are provided to help you evaluate SNMP features in the latest ONTAP version.

SNMP traps

SNMP traps capture system monitoring information that is sent as an asynchronous notification from the SNMP agent to the SNMP manager.

There are three types of SNMP traps: standard, built-in, and user-defined. User-defined traps are not supported in ONTAP.

A trap can be used to check periodically for operational thresholds or failures that are defined in the MIB. If a threshold is reached or a failure is detected, the SNMP agent sends a message (trap) to the traphosts alerting them of the event.

ONTAP supports SNMPv1 traps and, staring in ONTAP 9.1, SNMPv3 traps. ONTAP does not support SNMPv2c traps and INFORMs.

Standard SNMP traps

These traps are defined in RFC 1215. There are five standard SNMP traps that are supported by ONTAP: coldStart, warmStart, linkDown, linkUp, and authenticationFailure.

The authenticationFailure trap is disabled by default. You must use the `system snmp authtrap` command to enable the trap. For more informatin, see the man pages: ONTAP 9 commands

Built-in SNMP traps

Built-in traps are predefined in ONTAP and are automatically sent to the network management stations on the traphost list if an event occurs. These traps, such as diskFailedShutdown, cpuTooBusy, and volumeNearlyFull, are defined in the custom MIB.

Each built-in trap is identified by a unique trap code.

Create an SNMP community and assigning it to a LIF

You can create an SNMP community that acts as an authentication mechanism between the management station and the storage virtual machine (SVM) when using SNMPv1 and SNMPv2c.

By creating SNMP communities in a data SVM, you can execute commands such as `snmpwalk` and `snmpget` on the data LIFs.

About this task

- In new installations of ONTAP, SNMPv1 and SNMPv2c are disabled by default.

  SNMPv1 and SNMPv2c are enabled after you create an SNMP community.

- ONTAP supports read-only communities.
- By default, the "data" firewall policy that is assigned to data LIFs has SNMP service set to `deny`.

  You must create a new firewall policy with SNMP service set to `allow` when creating an SNMP user for a

data SVM.

- You can create SNMP communities for SNMPv1 and SNMPv2c users for both the admin SVM and the data SVM.
- Because an SVM is not part of the SNMP standard, queries on data LIFs must include the NetApp root OID (1.3.6.1.4.1.789)—for example, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Steps

1. Create an SNMP community by using the `system snmp community add` command. The following command shows how to create an SNMP community in the admin SVM cluster-1:

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   The following command shows how to create an SNMP community in the data SVM vs1:

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. Verify that the communities have been created by using the system snmp community show command.

   The following command shows the two communities created for SNMPv1 and SNMPv2c:

   ```
   system snmp community show
   cluster-1
   rocomty1
   vs1
   rocomty2
   ```

3. Check whether SNMP is allowed as a service in the "data" firewall policy by using the `system services firewall policy show` command.

   The following command shows that the snmp service is not allowed in the default "data" firewall policy (the snmp service is allowed in the "mgmt" firewall policy only):

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- --------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Create a new firewall policy that allows access using the `snmp` service by using the `system services firewall policy create` command.

   The following commands create a new data firewall policy named "data1" that allows the `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- --------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Apply the firewall policy to a data LIF by using the `network interface modify `command with the -firewall -policy parameter.

The following command assigns the new "data1" firewall policy to LIF "datalif1":

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

Configure SNMPv3 users in a cluster

SNMPv3 is a secure protocol when compared to SNMPv1 and SNMPv2c. To use SNMPv3, you must configure an SNMPv3 user to run the SNMP utilities from the SNMP manager.

Step

Use the "security login create command" to create an SNMPv3 user.

You are prompted to provide the following information:

- Engine ID: Default and recommended value is local Engine ID
- Authentication protocol
- Authentication password
- Privacy protocol
- Privacy protocol password

Result

The SNMPv3 user can log in from the SNMP manager by using the user name and password and run the SNMP utility commands.

SNMPv3 security parameters

SNMPv3 includes an authentication feature that, when selected, requires users to enter their names, an authentication protocol, an authentication key, and their desired security level when invoking a command.

The following table lists the SNMPv3 security parameters :

Parameter	Command-line option	Description
engineID	-e EngineID	Engine ID of the SNMP agent. Default value is local EngineID (recommended).
securityName	-u Name	User name must not exceed 32 characters.
authProtocol	-a {none | MD5 | SHA | SHA-256}	Authentication type can be none, MD5, SHA, or SHA-256.

Parameter	Command-line option	Description
authKey	-A PASSPHRASE	Passphrase with a minimum of eight characters.
securityLevel	-l {authNoPriv | AuthPriv | noAuthNoPriv}	Security level can be Authentication, No Privacy; Authentication, Privacy; or no Authentication, no Privacy.
privProtocol	-x { none | des | aes128}	Privacy protocol can be none, des, or aes128
privPassword	-X password	Password with a minimum of eight characters.

Examples for different security levels

This example shows how an SNMPv3 user created with different security levels can use the SNMP client-side commands, such as `snmpwalk`, to query the cluster objects.

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

You must use `snmpwalk` 5.3.1 or later when the authentication protocol is SHA.

Security level: authPriv

The following output shows the creation of an SNMPv3 user with the authPriv security level.

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose  (none, md5, sha)
[none]:sha
```

FIPS mode

```
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose  (none, des) [none]: des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Security level: authNoPriv

The following output shows the creation of an SNMPv3 user with the authNoPriv security level.

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS Mode

```
Which privacy protocol do you want to choose (aes128) [aes128]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (none, des) [none]: none
```

snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Security level: noAuthNoPriv

The following output shows the creation of an SNMPv3 user with the noAuthNoPriv security level.

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS Mode

FIPS will not allow you to choose none

snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Configure traphosts to receive SNMP notifications

You can configure the traphost (SNMP manager) to receive notifications (SNMP trap PDUs) when SNMP traps are generated in the cluster. You can specify either the host name or the IP address (IPv4 or IPv6) of the SNMP traphost.

Before you begin

- SNMP and SNMP traps must be enabled on the cluster.

  SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster for resolving the traphost names.
- IPv6 must be enabled on the cluster to configure SNMP traphosts by using IPv6 addresses.
- For ONTAP 9.1 and later versions, you must have specified the authentication of a predefined User-based Security Model (USM) and privacy credentials when creating traphosts.

Step

Add an SNMP traphost:

```
system snmp traphost add
```

Traps can be sent only when at least one SNMP management station is specified as a traphost.

The following command adds a new SNMPv3 traphost named yyy.example.com with a known USM user:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

The following command adds a traphost using the IPv6 address of the host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Commands for managing SNMP

You can use the `system snmp` commands to manage SNMP, traps, and traphosts. You can use the `security` commands to manage SNMP users per SVM. You can use the `event` commands to manage events related to SNMP traps.

Commands for configuring SNMP

If you want to…	Use this command…
Enable SNMP on the cluster	options -option-name snmp.enable -option-value on The SNMP service must be allowed under the management (mgmt) firewall policy. You can verify whether SNMP is allowed by using the system services firewall policy show command.
Disable SNMP on the cluster	options -option-name snmp.enable -option-value off

Commands for managing SNMP v1, v2c, and v3 users

If you want to…	Use this command…
Configure SNMP users	security login create
Display SNMP users	security snmpusers and security login show -application snmp
Delete SNMP users	security login delete
Modify the access-control role name of a login method for SNMP users	security login modify

Commands for providing contact and location information

If you want to…	Use this command…
Display or modify the contact details of the cluster	system snmp contact
Display or modify the location details of the cluster	system snmp location

Commands for managing SNMP communities

If you want to…	Use this command…
Add a read-only (ro) community for an SVM or for all SVMs in the cluster	system snmp community add
Delete a community or all communities	system snmp community delete
Display the list of all communities	system snmp community show

Because SVMs are not part of the SNMP standard, queries on data LIFs must include the NetApp root OID (1.3.6.1.4.1.789), for example, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Command for displaying SNMP option values

If you want to…	Use this command…
Display the current values of all SNMP options, including cluster contact, contact location, whether the cluster is configured to send traps, the list of traphosts, and list of communities and access control type	system snmp show

Commands for managing SNMP traps and traphosts

If you want to…	Use this command…
Enable SNMP traps sent from the cluster	system snmp init -init 1
Disable SNMP traps sent from the cluster	system snmp init -init 0
Add a traphost that receives SNMP notifications for specific events in the cluster	system snmp traphost add

If you want to…	Use this command…
Delete a traphost	system snmp traphost delete
Display the list of traphosts	system snmp traphost show

Commands for managing events related to SNMP traps

If you want to…	Use this command…
Display the events for which SNMP traps (built-in) are generated	event route show Use the -snmp-support true parameter to view only SNMP-related events. Use the instance -messagename <message> parameter to view a detailed description why an event might have occurred, and any corrective action. Routing of individual SNMP trap events to specific traphost destinations is not supported. All SNMP trap events are sent to all traphost destinations.
Display a list of SNMP trap history records, which are event notifications that have been sent to SNMP traps	event snmphistory show
Delete an SNMP trap history record	event snmphistory delete

For more information about the `system snmp`, `security`, and `event` commands, see the man pages: ONTAP 9 commands