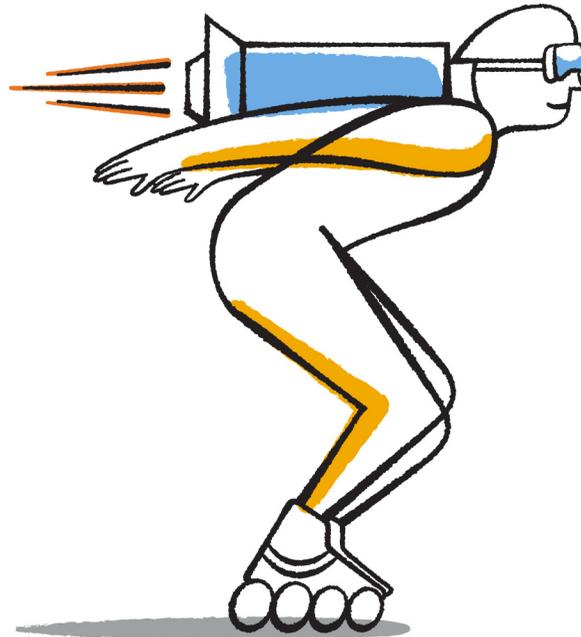




NetApp®

Clustered Data ONTAP® 8.3

SNMP Configuration Express Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-09652_A0
January 2015

Contents

Deciding whether to use this guide	4
SNMP configuration workflow	5
Verifying that SNMP is enabled	5
Adding an SNMP community	7
Adding an SNMPv3 security user	8
Adding an SNMP traphost	9
Testing SNMP traps	10
Testing SNMP polling	11
Where to find additional information	13
Copyright information	14
Trademark information	15
How to send comments about documentation and receive update notification	16
Index	17

Deciding whether to use this guide

This guide describes how to configure SNMP at the cluster management level, how to add communities, security users, and traphosts, and how to test the SNMP communication.

You should use this guide if you want to configure SNMP access to a cluster in the following way:

- You are working with clusters running Data ONTAP 8.3 or later.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to use OnCommand System Manager, not the Data ONTAP command-line interface or an automated scripting tool.

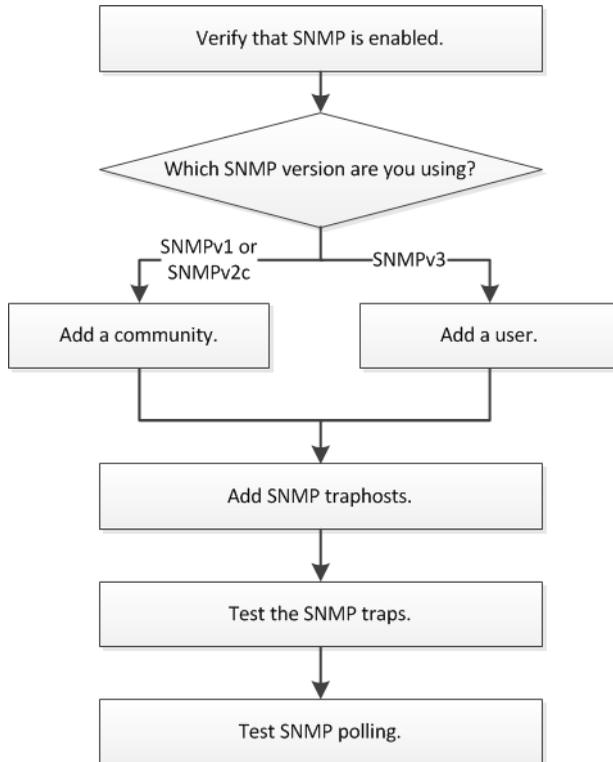
Note, however, that there are a few steps in this guide for which you must use the command-line interface.

If this guide is not suitable for your situation, you should see the following documentation instead:

- [*Clustered Data ONTAP 8.3 Network Management Guide*](#)
Describes how to configure subnets, intercluster LIFs, routes, firewall policies, and other networking components. It also describes how to create an SNMP community for a data Storage Virtual Machine (SVM) and how to manage SNMP traphosts.
- [*NetApp Technical Report 4220: SNMP Support in Data ONTAP 8.2.x and Data ONTAP 8.3.x*](#)
Describes SNMP support in Data ONTAP, including a detailed comparison of SNMP support for Data ONTAP operating in 7-Mode and clustered Data ONTAP and a list of all default events that are supported by SNMP traps.

SNMP configuration workflow

Configuring SNMP involves enabling SNMP, optionally configuring an SNMPv1 or SNMPv2c community, optionally adding an SNMPv3 user, adding SNMP traphosts, and testing SNMP polling and traps.



Verifying that SNMP is enabled

You can use System Manager to verify whether SNMP is enabled on the cluster.

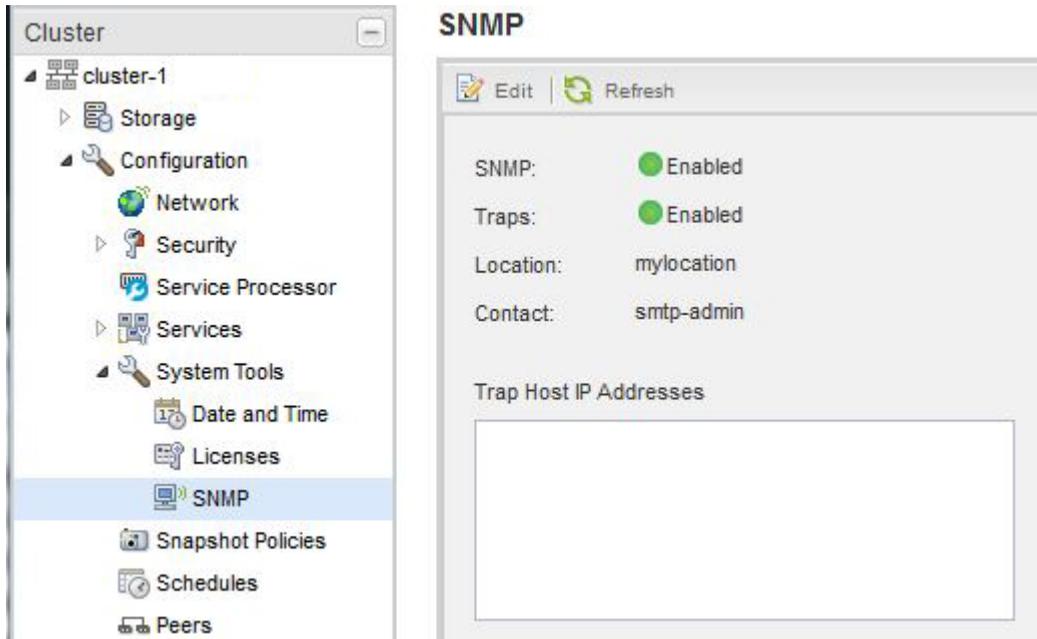
About this task

In new installations of Data ONTAP, SNMPv3 is enabled by default at the cluster level and SNMPv1 and SNMPv2c are disabled by default. SNMPv1 and SNMPv2c are enabled when you create an SNMP community.

SNMP is disabled by default on data LIFs. For information about enabling SNMP on data LIFs, see [Clustered Data ONTAP 8.3 Network Management Guide](#).

Steps

1. Expand the **Cluster** hierarchy in the left navigation pane.
2. In the navigation pane, click **Configuration > System Tools > SNMP**.



The SNMP window enables you to view the current SNMP status for the cluster.

If SNMP is not enabled, enable it from the CLI:

```
options -option-name snmp.enable -option-value on
```

Adding an SNMP community

You can use the System Manager SNMP window to add a community to the administrative Storage Virtual Machine (SVM) for a cluster that is running SNMPv1 or SNMPv2c. System Manager uses SNMP protocols SNMPv1 and SNMPv2c, and an SNMP community to discover storage systems.

About this task

This procedure is for adding an SNMP community to the administrative SVM for the cluster. The procedure for adding an SNMP community to a data SVM is described in the [Clustered Data ONTAP 8.3 Network Management Guide](#).

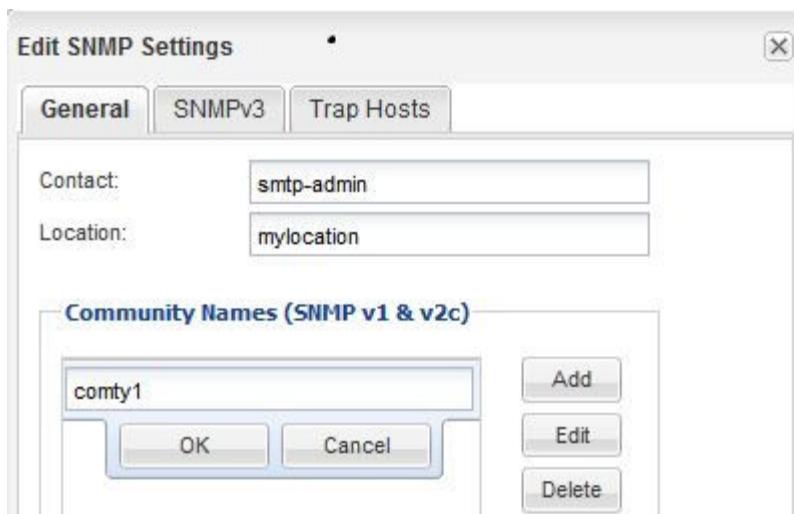
In new installations of Data ONTAP, SNMPv1 and SNMPv2c are disabled by default. SNMPv1 and SNMPv2c are enabled when you create an SNMP community.

Note: Releases earlier than Data ONTAP 8.3 included a default “public” community. Data ONTAP 8.3 and later releases do not create a default community.

Steps

1. In the **SNMP** window, click **Edit** to open the **Edit SNMP Settings** dialog box.
2. In the **General** tab, specify the storage system contact personnel and location.
3. Click **Add**, enter a community name, and then click **OK** in the **Community Names** pane.

You can add multiple community names. A community name can be a maximum of 32 characters and must not contain the following special characters: , / : " ' |



4. When you finish adding community names, click **OK** in the **Edit SNMP Settings** dialog box.

Adding an SNMPv3 security user

SNMPv3 offers advanced security by using passphrases and encryption. You can use the System Manager SNMP window to add an SNMPv3 user at the cluster level. The SNMPv3 user can run SNMP utilities from the traphost (SNMP manager) using the authentication and privacy settings that you specify.

About this task

When you add an SNMPv3 user at the cluster level, that user is accessible through all the LIFs that have the **mgmt** firewall policy applied.

Steps

1. In the **Configuration > System Tools > SNMP** window, click **Edit** to open the **Edit SNMP Settings** dialog box.
2. In the **SNMPv3** tab, click **Add** to open the **Add SNMPv3 User** dialog box.
3. Enter the following values:

- a. Enter an SNMPv3 user name.

A security user name must not exceed 31 characters and must not contain the following special characters:

, / : " ' |

- b. For Engine ID, select the default value

Local Engine ID

The Engine ID is used to generate authentication and encryption keys for SNMPv3 messages.

- c. Select an authentication protocol and enter a authentication password.

A password must contain a minimum of eight characters.

- d. Optional: Select a privacy protocol and enter a password for it.

4. Click **OK** in the **Add SNMPv3 User** dialog box.

You can add multiple security user names, clicking **OK** after each addition. For example, if you use SNMP to monitor different applications that require different privileges, you might need to add an SNMPv3 user for each monitoring or management function.

5. When you finish adding user names, click **OK** in the **Edit SNMP Settings** dialog box.

Adding an SNMP traphost

You can use the System Manager SNMP window to add a traphost (SNMP manager) to receive SNMP notifications (SNMP trap PDUs) when traps are generated in the cluster.

Before you begin

IPv6 must be enabled on the cluster if you configure SNMP traphosts that have IPv6 addresses.

About this task

SNMP and SNMP traps are enabled by default. The Technical Report [NetApp Technical Report 4220: SNMP Support in Data ONTAP 8.2.x and Data ONTAP 8.3.x](#) contains lists of all default events that are supported by SNMP traps.

Steps

1. In the **Configuration > System Tools > SNMP** window, click **Edit** to open the **Edit SNMP Settings** dialog box.
2. In the **Trap Hosts** tab, click **Add** and verify that the **Enable traps** check box is selected.
3. Enter the traphost IP address, and then click **OK** in the **Trap Hosts** pane.
The IP address of an SNMP traphost can be IPv4 or IPv6.



4. To add another traphost, repeat Steps 2 and 3.
5. When you finish adding traphosts, click **OK** in the **Edit SNMP Settings** dialog box.

Testing SNMP traps

Because communication with a traphost is not automatically validated when you add it, you should verify that the SNMP traphost can correctly receive traps.

About this task

You need to use CLI commands to send a test trap to a traphost, and then use your SNMP management software to verify that the trap was received.

Steps

1. Use the CLI command
system snmp init
to generate a trap from the cluster in which you added a traphost.

Example

The following commands send a coldStart trap to the traphost:

```
cluster1::> system snmp init -init 0
cluster1::> system snmp init -init 1
```

2. From the traphost location, verify that the trap was received.

Use whatever software you ordinarily use to manage the SNMP traphost.

Testing SNMP polling

After you configure SNMP, you should verify that you can poll the cluster.

About this task

To poll a cluster, you need to use a third-party command such as `snmpwalk`.

Step

1. Send an SNMP command to poll the cluster from a different cluster.

Example

For systems running SNMPv1, use the CLI command

`snmpwalk -v version -c community_string ip_address_or_host_name system`
to discover the contents of the MIB (Management Information Base).

In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
                        Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

Example

For systems running SNMPv2c, use the CLI command

`snmpwalk -v version -c community_string ip_address_or_host_name system`

12 | SNMP Configuration Express Guide

to discover the contents of the MIB (Management Information Base).

In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
      Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Example

For systems running SNMPv3, use the CLI command

```
snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A password  
ip_address_or_host_name system
```

to discover the contents of the MIB (Management Information Base).

In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3  
-a password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
      Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

Where to find additional information

There are other reference manuals to help you configure SNMP.

The following documentation provides more detailed information:

- [*Clustered Data ONTAP 8.3 Network Management Guide*](#)
Describes how to configure subnets, intercluster LIFs, routes, firewall policies, and other networking components. It also describes how to create an SNMP community or security user in a data Storage Virtual Machine (SVM) and how to manage SNMP traphosts.
- [*NetApp Technical Report 4220: SNMP Support in Data ONTAP 8.2.x and Data ONTAP 8.3.x*](#)
Describes SNMP support in Data ONTAP, including a detailed comparison of SNMP support for Data ONTAP operating in 7-Mode and clustered Data ONTAP, and a list of all default events that are supported by SNMP traps.

Copyright information

Copyright © 1994–2015 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, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

How to send comments about documentation and receive update notification

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

- A**
- additional information
 - where to find for configuring SNMP in your cluster [13](#)
- C**
- cluster management LIFs
 - adding SNMPv1 or SNMPv2c community to [7](#)
 - verifying that SNMP is enabled on [5](#)
 - clusters
 - requirements for using this guide to configure SNMP access to [4](#)
 - comments
 - how to send feedback about documentation [16](#)
 - communication
 - testing SNMP [11](#)
 - testing SNMP traps [10](#)
 - community
 - adding SNMPv1 or SNMPv2c to cluster management LIFs [7](#)
 - configuring
 - SNMP access, workflow for [5](#)
- D**
- documentation
 - how to receive automatic notification of changes to [16](#)
 - how to send feedback about [16](#)
- E**
- events
 - verifying that SNMP traphost can correctly receive [10](#)
 - express guides
 - requirements for using this guide to configure SNMP cluster access [4](#)
 - SNMP configuration workflow [5](#)
 - where to find additional information for configuring SNMP in your cluster [13](#)
- F**
- feedback
 - how to send comments about documentation [16](#)
- I**
- information
 - how to send feedback about improving documentation [16](#)
- L**
- LIFs
 - adding SNMPv1 or SNMPv2c community to cluster management [7](#)
 - verifying that SNMP is enabled on cluster management [5](#)
- M**
- management LIFs
 - adding SNMPv1 or SNMPv2c community to cluster [7](#)
 - verifying that SNMP is enabled on cluster [5](#)
- S**
- security users
 - adding SNMPv3 [8](#)
 - SNMP
 - adding SNMPv1 or SNMPv2c community [7](#)
 - adding SNMPv3 security user [8](#)
 - adding traphosts [9](#)
 - configuration workflow [5](#)
 - polling a cluster [11](#)
 - requirements for using this guide to configure cluster access [4](#)
 - testing communication [11](#)
 - verifying that it is enabled [5](#)
 - SNMP manager
 - .See traphosts
 - suggestions
 - how to send feedback about documentation [16](#)

T

traphosts

adding SNMP [9](#)

SNMP, verifying they can correctly receive traps [10](#)

traps

verifying that SNMP traphost can correctly receive [10](#)

twitter

how to receive automatic notification of documentation changes [16](#)

U

users

adding SNMPv3 security [8](#)

W

workflows

SNMP configuration [5](#)