Configure SNMPv3 users in a cluster

ONTAP System Manager

NetApp
December 14, 2020

This PDF was generated from https://docs.netapp.com/us-en/ontap/networking-app/configure_snmpv3_users_in_a_cluster.html on December 16, 2020. Always check docs.netapp.com for the latest.

Table of Contents

Configure SNMPv3 users in a cluster 1

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 EngineID
- 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.
authKey	-A PASSPHRASE	Passphrase with a minimum of eight characters.

Parameter	Command-line option	Description
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

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
Please enter the authoritative entity's EngineID [local EngineID]:
Please choose an authentication protocol (none, md5, sha) [none]:sha
Please enter authentication protocol password (minimum 8 characters long):
Please enter authentication protocol password again:
Please choose a privacy protocol (none, des) [none]: des
Please enter privacy protocol password (minimum 8 characters long):
Please enter privacy protocol password again:
```

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

```
$ 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
Please enter the authoritative entity's EngineID [local EngineID]:
Please choose an authentication protocol (none, md5, sha) [none]: md5
Please enter authentication protocol password (minimum 8 characters long):
Please enter authentication protocol password again:
Please choose a privacy protocol (none, des) [none]: none
```

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

```
$ 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
Please enter the authoritative entity's EngineID [local EngineID]:
Please choose an authentication protocol (none, md5, sha) [none]: none
```

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

```
$ 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"
```

Copyright Information

Copyright © 2020 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.