COMMVAULT
Distributed
Storage

Hedvig MIB User Guide

Table of Contents

Hedvig MIB compliance.......... 3
Setting up the MIB and configuring SNMP.......... 3
Editing the SNMP Configuration in the Hedvig WebUI.......... 3
Restarting the SNMP agent in the Hedvig CLI (initial setup only).......... 5
Configuring the manager/trap receiver.......... 6
Sending a test trap.......... 6
Hedvig WebUI.......... 6
Hedvig CLI.......... 6
Trap Viewer.......... 7
Hedvig MIB nomenclature and Hedvig PEN.......... 8
Hedvig SNMP traps.......... 8
hedvigTrapsEntry (1.3.6.1.4.1.46525.8).......... 9
Glossary.......... 11

Hedvig MIB compliance

The Hedvig MIB complies with:

- SNMPv2c, which does not require authentication
- SNMPv3, which requires:
  - MD5 authentication
  - PrivAES128 privacy protocol

Setting up the MIB and configuring SNMP

To set up the MIB and configure SNMP, follow these steps:

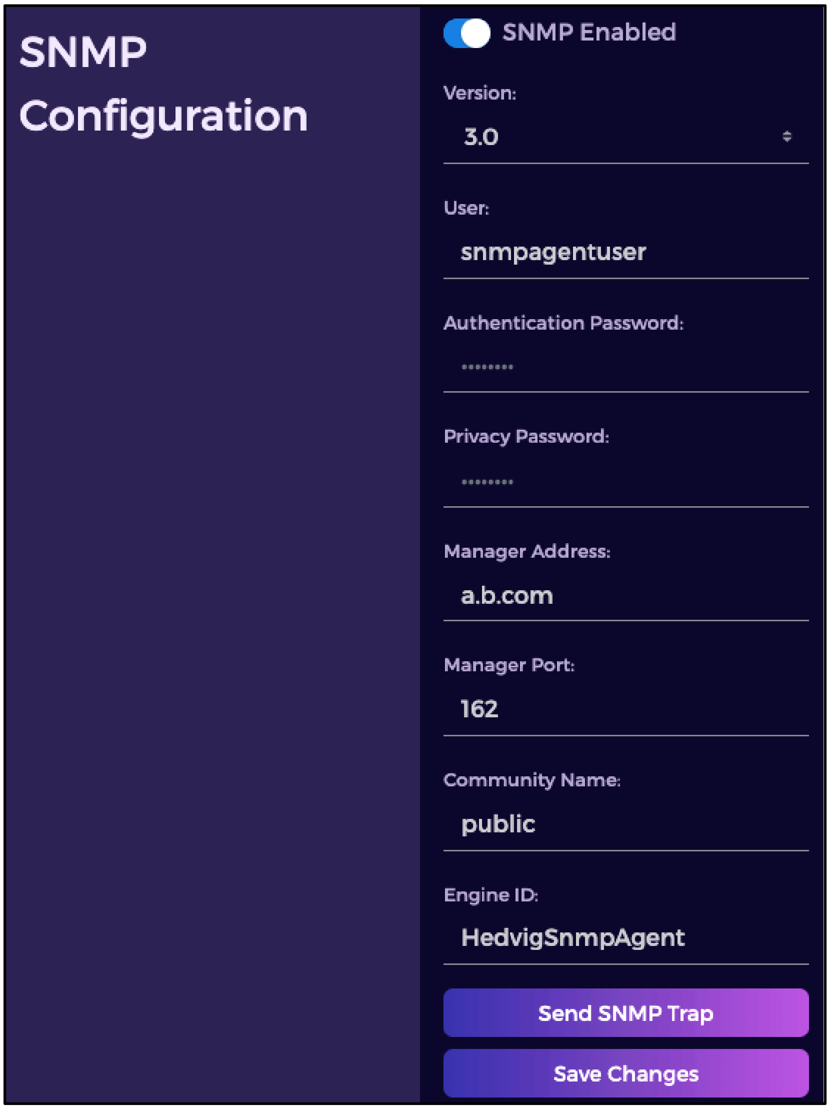
- *Editing the SNMP Configuration in the Hedvig WebUI*
- *Restarting the SNMP agent in the Hedvig CLI (initial setup only)*
- *Configuring the manager/trap receiver*
- *Sending a test trap*

Editing the SNMP Configuration in the Hedvig WebUI

You edit your SNMP configuration directly in the Hedvig WebUI.

Your SNMP configuration will be set *cluster-wide*, that is, when, you make configuration changes connected to one of your storage cluster nodes, your changes will apply to *all* of the nodes in the cluster.

In the Hedvig WebUI, select the **SNMP Configuration** entry in the **User** menu in the banner at the top right to see the configuration items that you can edit.



SNMP Configuration

SNMP Enabled

Version: 3.0

User: snmpagentuser

Authentication Password: ••••••••

Privacy Password: ••••••••

Manager Address: a.b.com

Manager Port: 162

Community Name: public

Engine ID: HedvigSnmpAgent

Figure 1: SNMP Configuration dialog

Here are descriptions and possible values for the fields in the **SNMP Configuration** dialog:

- **SNMP Enabled**: Enable (checked) or disable (unchecked) SNMP.
- **Version**: Select SNMPv2c or SNMPv3.
- **User**: Enter the SNMP user name, which must be no more than 30 characters.
- **Authentication Password**: Enter an authentication password, which must be from 8 to 30 characters.
- **Privacy Password**: Enter an AES (Advanced Encryption Standard) password, which must be from 8 to 30 characters. This can be the same password as the Authentication Password, or it may be different.

- **Manager Address**: Enter the address of the SNMP manager. You must change this from the default.
- **Manager Port**: Leave the default port of 162, or enter a different one, which must be a valid port number.
- **Community Name**: Leave the default name of public, or enter a customized community name.
- **Engine ID**: Leave the default identifier of HedvigSnmpAgent, or enter a customized engine identifier.

Select **Send SNMP Trap** to send a test SNMP trap.

Select **Save Changes** when you have completed your changes.

Restarting the SNMP agent in the Hedvig CLI (initial setup only)

After the initial setup of the SNMP configuration values in the Hedvig WebUI, you must restart the SNMP agent using the Hedvig CLI.

You will need to restart the SNMP agent only *this one time.*

After this restart of the SNMP agent, the next upgrade or restart of Hedvig services will then start the SNMP agent from the persisted configuration values.

1. Login to any cluster node as the `root` user.

   ```
   ssh root@<cluster node 1>
   ```

   ```
   password:  hedvig
   ```

2. Start the CLI.

   ```
   scripts
   ```

   ```
   ./secured-cli.sh
   ```

3. Run the `restartsnmpagent` command on each cluster node.

   ```
   restartsnmpagent -h <cluster node 1>
   restartsnmpagent -h <cluster node 2>
   restartsnmpagent -h <cluster node 3>
   …
   ```

   And so on, for each of your cluster nodes.

Configuring the manager/trap receiver

Configure the manager/trap receiver to listen for traps from the Hedvig application on port 9998.

Note: The SNMP Agent is started in the Hedvig Block Process (HBlock), and traps from the Hedvig Metadata Process (Pages) are routed to the manager via HBlock. The Hedvig Storage Proxy sends traps over to Pages, which are then forwarded to HBlock.

Sending a test trap

To test your SNMP setup, you can send a *test trap* using:

- *Hedvig WebUI*
- *Hedvig CLI*
- *Trap Viewer*

Hedvig WebUI

In the Hedvig WebUI, use the **Send SNMP Trap** button on the **SNMP Configuration** page (see *Editing the SNMP Configuration in the Hedvig WebUI).*

Hedvig CLI

In the Hedvig CLI, use the `sendtesttrap` command. Here is the procedure:

1. Login to any cluster node as the `root` user.

```
ssh root@<cluster node 1>
password:  hedvig
```

2. Start the CLI.

```
scripts
./secured-cli.sh
```

3. Send the test trap.

```
sendtesttrap -h <cluster node 1>
```

For example:

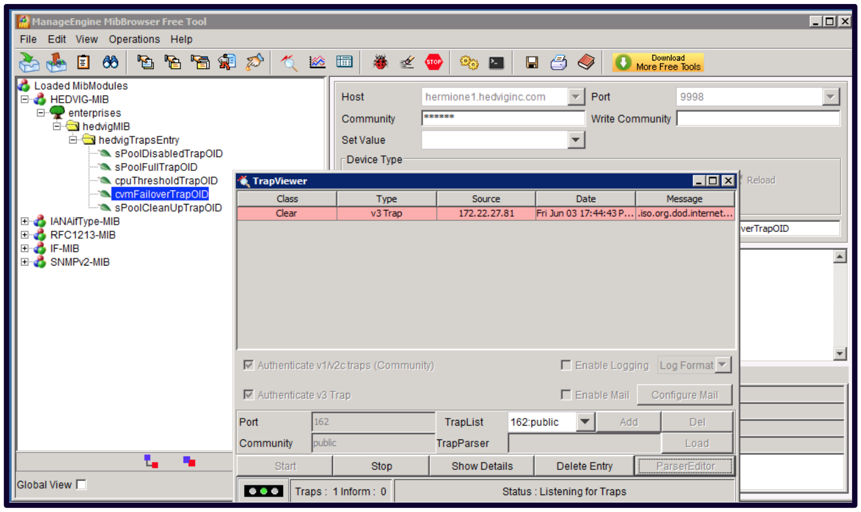
```
sendtesttrap -h ClusterNode1

Received 124 bytes from UDP: [172.22.27.81]:9998->[172.22.27.228]
0000: 30 7A 02 01  01 04 06 70  75 62 6C 69  63 A7 6D 02    0z.....public�m.
0016: 04 44 41 01  88 02 01 00  02 01 00 30  5F 30 0E 06    .DA........0_0..
0032: 08 2B 06 01  02 01 01 03  00 43 02 28  6E 30 19 06    .+.......C.(n0..
0048: 0A 2B 06 01  06 03 01 01  04 01 00 06  0B 2B 06 01    .+...........+..
0064: 04 01 82 EB  3D 08 0A 00  30 16 06 0A  2B 06 01 06    ...�=...0...+...
0080: 03 01 01 04  03 00 06 08  2B 06 01 04  01 82 EB 3D    ........+.....�=
0096: 30 1A 06 08  2B 06 01 02  01 01 01 00  04 0E 53 6E    0...+.........Sn
0112: 6D 70 20 54  65 73 74 20  54 72 61 70                mp Test Trap

2016-06-03 17:36:44 ClusterNode1.hedviginc.com [UDP: [172.22.27.81]:9998-
>[172.22.27.228]]:
RFC1213-MIB::sysUpTime.0 = Timeticks: (10350) 0:01:43.50 RFC1155-
SMI::internet.6.3.1.1.4.1.0 = OID: HEDVIG-MIB::hedvigTrapsEntry.10.0 RFC1155-
SMI::internet.6.3.1.1.4.3.0 = OID: HEDVIG-MIB::hedvigMIB RFC1213-
MIB::sysDescr.0 = STRING: "Snmp Test Trap"
```

Trap Viewer

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 0 hours, 9
minutes, 52 seconds.:
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmp
TrapEnterprise.0: Object ID: .1.3.6.1.4.1.46525:
.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0: Snmp Test Trap:
```



Host: hermione1.hedviginc.com
Port: 9998
Community: ******
Write Community:
Set Value:

Class	Type	Source	Date	Message
Clear	v3 Trap	172.22.27.81	Fri Jun 03 17:44:43 P...	.iso.org.dod.internet...

☑ Authenticate v1/v2c traps (Community) ☐ Enable Logging Log Format

☑ Authenticate v3 Trap ☐ Enable Mail

Port: 162
Community: public
TrapList: 162:public
TrapParser:

Traps : 1 Inform : 0
Status : Listening for Traps

Figure 2: Using a Trap Viewer

Hedvig MIB nomenclature and Hedvig PEN

Each object in the MIB is assigned an SNMP OID (object identifier) – the numerical equivalent of a path in the MIB hierarchy – written in ASN.1.

The ASN.1 prefix of 1.3.6.1.4.1., combined with the five-digit Hedvig PEN (private enterprise number) of 46525, produces a base number of 1.3.6.1.4.1.46525.

The MIB objects and sub-objects are then numbered in a hierarchical manner that reflects the hierarchy of the Hedvig MIB structure.

Hedvig SNMP traps

SNMP traps are sent from the SNMP agent to the SNMP manager. Conversely, communication is *not* sent from the SNMP manager to the SNMP agent.

The **hedvigTrapsEntry** is the Hedvig MIB module for sending traps.

To form the OID for **hedvigTrapsEntry**, a **.8** is added to the base number, resulting in a starting number of 1.3.6.1.4.1.46525**.8**.

Each individual trap then adds *another* number to produce a unique OID, for example, the first trap, **sPoolDisabledTrap**, is 1.3.6.1.4.1.46525**.8.1**.

hedvigTrapsEntry (1.3.6.1.4.1.46525.8)

trap (OID)	description and suggested action
sPoolDisabledTrap (1.3.6.1.4.1.46525.8.1)	Notifies you that the repair of a failed disk has been initiated. **Suggested action**: 1. In the Hedvig WebUI, verify that the storage pool identified by the trap has been disabled. 2. Check the Alerts (⚠) to determine if Storage Pool Migration (SPM) has begun. 3. Verify that SPM is complete by clicking on the message in the Alerts area.
sPoolFullTrap (1.3.6.1.4.1.46525.8.4)	Notifies you that a storage pool pertaining to a storage node is reaching its capacity. Traps are sent starting at 60% of capacity. **Suggested action**: 1. In the Hedvig WebUI, find the storage pool identified by the trap. 2. Verify that the storage pool is filled beyond the percentage specified in the trap. 3. Add more storage, as required.
cpuThresholdTrap (1.3.6.1.4.1.46525.8.6)	Notifies you that a cluster process could be consuming CPU > 60%.
cvmFailoverTrap (1.3.6.1.4.1.46525.8.8)	Notifies you that a Hedvig Storage Proxy (CVM) is failing over to the other proxy in the HA pair.
sPoolCleanUpTrap (1.3.6.1.4.1.46525.8.9)	Notifies you that a process has been initiated to handle any and all unresolved issues that may have occurred during an interrupted Storage Pool Migration (SPM).

trap (OID)	description and suggested action
testTrap (1.3.6.1.4.1.46525.8.10)	Notifies you that a test trap has been sent.
cLogAccumulationTrap (1.3.6.1.4.1.46525.8.11)	Notifies you when there is a commit log accumulation on Pages/HBlock. A `cron` job runs periodically (currently set at a 15-minute interval) on the server nodes, looking for the number of files in the commit log location of Pages and HBlock, and an alert is generated when any exceeds the threshold of 5.
decomissionNodeTrap (1.3.6.1.4.1.46525.8.12)	Notifies you when a node is getting decommissioned.
storageNodeDownTrap (1.3.6.1.4.1.46525.8.13)	Notifies you when the metadata or the data process in the node has gone down.
licenseExpirationTrap (1.3.6.1.4.1.46525.8.14)	Notifies you when your license has expired.
licenseDataCapacityTrap (1.3.6.1.4.1.46525.8.15)	Notifies you when the used space has exceeded the licensed data capacity.

Glossary

This glossary contains definitions of terms used in this document.

Table 3: Glossary of terms

term	definition
AES	The *Advanced Encryption Standard* is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
ASN.1	*Abstract Syntax Notation One* is a standard and notation that describes rules and structures for representing, encoding, transmitting, and decoding data in telecommunications and computer networking.
CVM	See *Hedvig Storage Proxy.*
failover	*Failover* is the ability of applications to migrate from one server to another if a server fails, so that these applications can continue to operate without interruption.
HA	*High availability* is the ability of a system to continue to function after the failure of one or more of its servers. A key part of high availability is *failover*.
Hedvig Block Process (HBlock)	The *Hedvig Block Process* is responsible for storing the physical blocks.
Hedvig Metadata Process (Pages)	The *Hedvig Metadata Process* is responsible for tracking all system *metadata*.
Hedvig Storage Pool	A *Hedvig Storage Pool* is a logical grouping of multiple physical disks that are presented as a single entity.

term	definition
Hedvig Storage Proxy	A *Hedvig Storage Proxy* is a lightweight software component that deploys at the application tier as a virtual machine or Docker container, or on bare metal, to provide storage access to any physical host or virtual machine in the application tier. A storage proxy provides intelligent access to the hyperscale storage nodes, directing I/O requests to the relevant backend storage nodes based on latency response times. *This may also be referred to as an HSP, controller, CVM, target, or tgt.*
MD5	The *MD5* message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32-digit hexadecimal number.
MIB	A *management information base* is a database used for managing the entities in a communication network. It is most often associated with SNMP.
NFS	A *network file system* is a distributed file system protocol that allows a user on a client computer to access files over a computer network much like local storage is accessed.
OID	An *object identifier* is an identifier used to name an object. Structurally, an OID consists of a node in a hierarchically assigned namespace, formally defined using ASN.1.
Pages	See *Hedvig Metadata Process (Pages).*
PEN	A *private enterprise number* is a unique, non-negative integer that is used to reference an organization in protocols that require numeric values instead of a human-readable name. PENs are created and maintained by the Internet Assigned Number Authority in a public registry.

term	definition
SNMP	*Simple Network Management Protocol* is an Internet-standard protocol for collecting and organizing information about *SNMP managed devices* on IP networks and for modifying that information to change device behavior.
SNMP agent	An *SNMP agent* is a network-management software module that resides on an *SNMP managed device*. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.
SNMP managed device	An *SNMP managed device* is a network node that implements an SNMP interface and allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information.
SNMP manager	An *SNMP manager* is an administrative computer that sends queries to, and receives traps from, an *SNMP agent*.
SNMP trap	An *SNMP trap* is an asynchronous notification from an *SNMP agent* to an *SNMP manager*. SNMP traps enable an agent to notify the manager of significant events by way of an unsolicited SNMP message.
SPM	*Storage Pool Migration* is the process of repairing a failed disk.

Commvault Systems, Inc., believes the information in this publication is accurate as of its publication date. The information is subject to change without notice. The information in this publication is provided as is. Commvault Systems, Inc., makes no representations or warranties of any kind with respect to the information in this publication and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any Commvault Systems, Inc., software described in this publication requires an applicable software license. All trademarks are the property of their respective owners. Revision date: 090221.

Software-defined AES-256, FIPS compliant encryption of data in flight and at rest.