SNMP PINsafe How to Guide

Contents

Overview

SNMP can be used to monitor hardware and software. There are no Swivel SNMP MIBS, but there are MIBS available for the OS and Apache Tomcat.

Also consider email alerting within the SNMP Administration console or for appliances part of the MON process, see MON Service Monitor How to guide

Swivel Appliance SNMP

Swivel Appliance Hardware Monitoring

For hardware monitoring you should be able to use the standard DELL MIBs here

This makes it possible to monitor the RAID on a hardware appliance.

Operating System SNMP

Swivel appliances use UDP port 161 for SNMP monitoring, the service is enabled by default but can be disabled through the CMI.

SNMPD is pre-installed and the configuration file is located here: /etc/snmp/snmpd.conf

You can edit the file using WinSCP. Refer to the WinSCP How To Guide.

The current version supports SNMP v3.

After editing the snmpd.conf restart snmp either through the CMI or from the command line with the command *service snmpd restart*

Adding a community string

Edit the /etc/snmp/snmpd.conf

The following can be edited as required:

```
## description
sysname         Appliance
sysdescr        PINsafe Appliance
syslocation     WETHERBY, GB
syscontact      root <sysadmin@localhost>

# First, map the community name "public" into a "security name"
#       sec.name        source          community
com2sec local           localhost       private
com2sec mynetwork       192.168.0.0/24  public
```

Examples:

```
#        sec.name  source          community
com2sec  local     localhost       private
com2sec  mynet     10.10.10.0/24   public
com2sec  public    default         public
com2sec6 mynet     fec0::/64       public
```

Adding the following allows the SNMP public to be read

```
rocommunity  public
```

Defining SNMP traps

Information can be sent from the Swivel appliances on particular events using SNMP traps. The format is as follow: host [community] [portnum]

Example:

```
trapsink  192.168.1.1 public 162
```

Testing with snmpwalk

snmpwalk can be used to verify that the community string can be read

```
snmpwalk -v2c -c public localhost system
```

Example output:

```
[admin@primary ~]# snmpwalk -v2c -c public locahost system
SNMPv2-MIB::sysDescr.0 = STRING: Swivel Appliance
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (17346) 0:02:53.46
SNMPv2-MIB::sysContact.0 = STRING: root <root@swivel.com>
SNMPv2-MIB::sysName.0 = STRING: Swivel Standby
SNMPv2-MIB::sysLocation.0 = STRING: Swivel server location
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.3 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.4 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.5 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.6 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.7 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.8 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.9 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module to describe generic objects for network interface sub-layers
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.7 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.9 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (2) 0:00:00.02
```

SNMP Users

To create users for SNMP v3 stop the SNMP agent and then add the below line to the file /var/net-snmp/snmpd.conf (where {myUser} and {myPassword} are the appropriate values for username and password, without the braces!). Then re-start the snmpd agent.

createUser {myUser} MD5 {myPassword} DES

Disable the SNMP daemon (snmpd)

Via the CMI Menu

On the Main Menu of the CMI, you should see SNMP listed. Select this option to stop the service. You then need to prevent it from running on startup of the appliance. To do this, goto Advanced Menu, Default Running Services. If the service is currently set to ON, then select the service to set it to be OFF.

Via the Command Line

Login to the CMI using the PuTTY How To Guide. For newer appliances see above or use the following commands via the Advanced Menu, Command Line option:

- Check the current run levels for the snmpd service:

```
[admin@standby ~]# chkconfig --list snmpd
snmpd           0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

- See that levels 3,4,5 are set to 'on', so to disable this service set these levels to be 'off':

```
[admin@standby ~]# chkconfig --level 345 snmpd off
```

- Check that the changes were successful:

```
[admin@standby ~]# chkconfig --list snmpd
snmpd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

To stop the snmpd service run the following commands.

- First check the status of the service to see if it's running or not:

```
[admin@standby ~]# service snmpd status
```

```
snmpd (pid 13904) is running...
```

- We can see that the service is running, so to stop it we run the following command:

[admin@standby ~]# service snmpd stop Stopping snmpd: [OK]