



## Installing SNMP Agents

The following section describes the installation procedure for several vendor specific SNMP agents. In some cases, the vendor agent acts like a sub-agent by interfacing with another main SNMP agent, or else listens on a TCP port other than 161.

NetVigil has built in support for the following vendor specific MIBs already. You just need to run a new tests discovery on the specific server after installing the SNMP agent and NetVigil will display the vendor specific tests automatically.

### C.1 NET-SNMP

This is a free SNMP agent available from <http://www.net-snmp.org> with excellent support for most Unix platforms, and bundled with most OS platforms.

#### C.1.1 Pre-compiled SNMP agents

Pre-compiled snmp agents for Linux and Solaris are available for download at <http://support.fidelia.com/downloads/NetVigil/snmp-agent/>. After downloading the appropriate archive, install the agent using the following steps:

1. `cd /usr/local`
2. `gunzip -c snmpd-<os>-<version>.tar.gz | tar xvf -`
3. Edit `net-snmp/share/snmp/snmpd.conf` and change the community string from `public` to something more secure.
4. Start the agent using (as root):  

```
sbin/snmpd -c share/snmp/snmpd.conf
```

## C.1.2 Editing the snmpd.conf file

The only line needed in the net-snmp/share/snmp/snmpd.conf file (also located in /etc/snmp/ on some vendor systems), is the community string:

```
## Define a read-only list of SNMP v1/v2 community strings
## Format is rocommunity <community> [hostIP|subnet/bits]
rocommunity public
rocommunity anotherString
```

After changing these, you should restart your snmpd.

## C.1.3 Configuring SNMP v3 in net-snmp

If you are using the net-snmp software on your server, you can enable SNMP v3 on the snmpd agent using the following steps. Note that there are 2 separate snmpd.conf files which need to be edited:

1. Edit snmpd.conf file (located in /etc/snmp/ or /usr/local/net-snmp/share/snmp/) and add the following line:

```
rouser myuser priv
```

This adds SNMP v3 user 'myuser' and specifies that both authentication and encryption of packets is required for this user.

2. Specify the authentication and encryption passwords for the user 'myuser' in the /usr/local/var/snmpd.conf file (this is a "runtime" file used by snmpd has comments in it about not editing manually except to add users). You must stop any running snmpd processes before editing this file:

```
createUser myuser MD5 "myAuthPasswd" DES myEncryptPasswd
```

This tells the snmpd process to create a user "myuser" with the MD5 authentication pass phrase and encryption password as specified.

Then restart snmpd. This line will automatically be replaced by a 'usmUser' entry without the cleartext passwords.

3. Now test the snmpd using the following command:

```
snmpwalk -v 3 -n "" -u myUser -l authPriv -a MD5 \
-A "myAuthPasswd" -X "myEncryptPasswd" \
192.168.1.100 sysUptime
```

In NetVigil, you specify these parameters by setting the community string to be:

```
user : authPassword : encryptPassword
```

(i.e. separated by colon characters).

## C.2 Solaris

Note that the Solaris agent only includes support for MIB-II tree, which will enable you to monitor the network interfaces on the server. Since the agent does not support HOST-MIB tree, NetVigil will not be able to find any disks or CPU. Also note that this agent only support SNMP version 1, so when creating a new device, make sure to select version 1 on the device creation page on the web interface.

Optionally, you can install the net-snmp software from <http://www.net-snmp.org> or from the Fidelia support web site. If you do this, then you must stop and disable the existing Sun provided agents using:

```
cd /etc/init.d
./init.snmpdx stop
./init.dmi stop
```

If you would like to use the Sun SNMP agent, then you should download and install the latest Solstice Enterprise Agent from <http://www.sun.com/software/entagents/>. The package includes instruction on how to uninstall the existing agent first.

The following config entries for `/etc/snmp/conf/snmpd.conf` should be sufficient to get basic information from the agent:

```
#-----
sysdescr                My Server
system-group-read-community public
read-community         public
trap                   localhost
trap-community         SNMP-trap
managers               localhost
#-----
```

## C.3 Windows 2003/XP/2000

**NOTE:** *If possible, it is preferable to use the native Windows WMI protocol instead of using SNMP on Windows devices because it allows monitoring of applications and parameters that the Windows SNMP agent does not provide.*

**NOTE:** *According to Microsoft Knowledge Base article, SNMP counters for storage devices (including physical and virtual memory) on Windows 2000 are not dynamically updated. Please refer to <http://support.microsoft.com/support/kb/articles/Q295/5/87.ASP> for additional information.*

### □ To install an SNMP Agent on a Windows2003/XP Server/2000:

1. Click on **Start | Settings | Control Panel**.
2. Double-click on **Add/Remove Programs**.
3. Click on **Add/Remove Windows Components**.
4. Click on **Management and Monitoring Tools** and click on **Details**.
5. Check **Simple Network Management Protocol** and click **OK**.
6. Click on **Next** and let the install process complete.
7. Double-click on **Administrative Tools** (inside **Control Panel**).
8. Double-click on **Computer Management**.
9. Expand the **Services and Applications** tree on the left frame.
10. Click on **Services** on the left frame.
11. Locate **SNMP Service** on right frame and double-click on it.
12. On the **General** tab, select **Automatic** for **Startup Type**.
13. On the **Security** tab, click on **Add...** for **Accepted community names**.
14. Leave **Community Rights** to **Read-Only** and pick a secure Community Name. Click on **OK**.

**NOTE** *Remember this name, as this information will be required to configure your Win2000 machine as a NetVigil device.*

15. Click on **OK** again and close the **Computer Management** and **Control Panel** windows.

For additional reference, please refer to:

<http://support.microsoft.com/support/kb/articles/Q237/2/95.ASP>

### Disk utilization for Windows 2000 host does not change

Recently Microsoft has release service pack 3 for Windows 2000, and a fix for this problem has been included in this update. If you are monitoring disk utilization on Windows 2000 workstations/servers using NetVigil, we recommend that you apply service pack 3 at your earliest convenience. This will ensure that you receive the correct utilization information, which also affects trend analysis for capacity planning.

#### ❑ To configure Windows NT 4.0 machine for SNMP monitoring:

Follow the same steps as above for Windows 2000. Minor differences may exist in the operating systems, so please refer to:

<http://support.microsoft.com/support/kb/articles/Q237/2/95.ASP> for the most recent information.

The SNMP agent provided with Windows NT 4.0 does not implement all elements of MIB-II and HOST-RESOURCES mibs, which provides information on system resources, such as CPU and disk utilization, etc.

## C.4 Oracle SNMP agent

### Installing the agent on Windows

The SNMP “Intelligent Agent” is shipped with the database and can be installed using the Oracle Universal Installer from the Enterprise Manager tree list or the database server tree list (check to see first if the agent is already installed by looking in the Windows “services” list. It will be listed in the Windows Services panel as “Oracle <ORACLE\_HOME> Agent”.

### Configure the Agent on Windows

Oracle has a master SNMP agent that runs on port 161, and the Windows SNMP agent must be configured to run as the sub-agent (on port 1161). Note however, that on a Windows platform, you can monitor all the Windows metrics using WMI instead of SNMP so you do not need to install the Windows SNMP agent.

1. Edit your `\windows\system32\drivers\etc\services` file and set the following entries:

```
snmp 1161/udp
snmp-trap 1162/udp
```

2. Edit `ORACLE_HOME\network\admin\MASTER.CFG` and add the following lines:

```
TRANSPORT ordinary SNMP
OVER UDP SOCKET
AT PORT 1161

COMMUNITY public
ALLOW ALL OPERATIONS
USE NO ENCRYPTION
```

3. Start the Peer SNMP Master Agent from the Windows Services Panel (the binary is `ORACLE_HOME\bin\agent.exe`).
4. Then start the Oracle sub-agent (the Intelligent Agent) which automatically registers itself with the master agent. To start the sub-agent, click on the Windows Control Panel->Services and start the Oracle Agent service (set to automatically start by right clicking on the service name).

To verify that the agent is running, look for the “dbsnmp” process in the Windows Task manager.

5. Check the listener status. If it shows “off” for SNMP, then you have to restart the listener using the following command:

```
lsnrctl status
lsnrctl stop
lsnrctl start listener
```

6. If you wish to run the Windows SNMP agent also (not needed for NetVigil installations), then you also will need to run the Oracle SNMP Encapsulator service from the Windows Services panel.

## Configuring Oracle Agent on Unix

On Unix platforms, install the Oracle SNMP Intelligent Agent from the Universal Installer. You will be required to run the `root.sh` script as superuser as part of this install, which installs

`ORACLE_HOME/bin/dbsnmp`. Then:

1. Stop any existing SNMP processes
2. Edit the `/etc/services` file and set the SNMP port to be 1161 for the native Unix agent. Change the line to:

```
snmp 1161/udp
snmp-trap 1162/udp
```

3. Edit `ORACLE_HOME/network/peer/config.master` and add the following lines:

```
TRANSPORT ordinary SNMP  
OVER UDP SOCKET  
AT PORT 1161
```

```
COMMUNITY public  
ALLOW ALL OPERATIONS  
USE NO ENCRYPTION
```

#### 4. Start the Peer SNMP Master Agent:

```
cd $ORACLE_HOME/network/snmp/peer  
start_peer -a
```

#### 5. Start the Oracle sub-agent (dbsnmp) using:

```
agentctl start agent
```

#### 6. Check the listener status. If it shows “off” for SNMP, then you have to restart the listener using the following command:

```
lsnrctl status  
lsnrctl stop  
lsnrctl start listener
```

## C.5 Lotus Notes SNMP agent

The Lotus Notes (Domino) SNMP agent allows monitoring of Domino statistics via the industry standard SNMP protocol (it currently supports SNMP v1). It consists of:

- **LNSNMP** -- Handles requests for Domino-related information from the management station by passing the request to the QuerySet Handler and responding back to the management station. Also receives trap notifications from the Event Interceptor and then sends them to the network management system via the platform-specific, master SNMP Agent.
- **QuerySet Handler** -- An add-in task that queries server statistics information and sets the value of configurable Domino-based parameters. The QuerySet Handler returns Domino statistics information to LNSNMP, which then forwards the information to the management station using the platform-specific, master SNMP Agent.
- **Event Interceptor** -- An add-in task that responds to the SNMP Trap notification for Domino Event Handlers by instructing the Trap Generator to issue a trap.

The Domino SNMP Agent constantly monitors the status of the server indirectly through an add-in task using IPC to determine whether the server is up or down. The Domino SNMP Agent is not a Lotus Notes API application; all of its status information is gathered out of band.

### Installing the Agent

1. Shut down the Domino server if it's running.
2. Run `nvinst`. The path is:  
`E:\apps\SysMgmt\Agents\W32Intel\nvinst`  
(Where e: is the CD-ROM drive.)  
Enter 1 to install only the Domino SNMP Agent;
3. If you are prompted to add the Reporter or Collector task, type `y`, then press Enter.
4. Restart your machine.

### Configuring the Agent:

To configure the SNMP agent for Lotus Notes (Domino server),

1. Make sure that the Windows SNMP service is installed by going to Control Panel -> Add Windows Components.
2. Stop the Lotus LNSNMP and Windows SNMP services from the command prompt in case they are running.

```
cd \Lotus\Domino
net stop lnsnmp
net stop snmp
```

3. Configure the Lotus Domino SNMP Agent as a service:

```
lnsnmp -Sc
```

4. Start the SNMP and LNSNMP services

```
net start snmp
net start lnsnmp
```

5. Start the QuerySet add-in task. Enter this command on the Domino Server console:

```
load qryset
```

6. To support SNMP traps for Domino events, start the Event Interceptor add-in task. Enter this command on the Domino Server console:

```
load intrcpt
```

Arrange for the add-in tasks to be restarted automatically when Domino is next restarted. Add `qryrset` and `intrcpt` to the `ServerTasks` variable in Domino's `NOTES.INI` file.

## C.6 BEA Weblogic SNMP

1. After installing BEA Weblogic, connect to the console of the Administrative server:

```
http://hostname:/7001/console
```

and then configure the SNMP agent.

Since the SNMP agent cannot be configured to run as a subagent (only as a master agent), if you are running Oracle on the same host you will have to run the BEA snmp agent on another port (such as 2161). Note that the Oracle agent expects the subagents on port 1161 (and the masquerade agent in Oracle can probably be told to communicate with the BEA snmp agent running on another port).

See <http://edocs.bea.com/wls/docs81/ConsoleHelp/snmp.html>

2. In the left pane, click on Services -> SNMP3. Click on enable checkbox, set the port number if needed.
3. Restart the server (Servers -> start/stop). You might need to restart by going to the windows Start -> Weblogic -> User projects again.

The BEA mib is at:

```
http://e-docs.bea.com/wls/docs81/snmp/index.html
```

## C.7 SCO Unix

1. login as "root"
2. edit `/etc/snmpd.peers` and add the following line at the end of the file:

```
"hostmib" 1.3.6.1.2.1.25 "aintNothing"
```

3. Associate the MIB system names with their numeric object identifier/ASN notation:

```
cd / etc/sysadm.d
```

```
post_mosy -i hostmib.defs -o hostmib.dfn
```

4. Enter the following command

```
mkdev hostmib
```

Select option 1 to install. You may want to verify progress by making sure that the following process exists:

```
/etc/smuxtcl /etc/sysadm.d/hostmib.tcl
```

in the process table using “ps -fe | grep smux”. When the process completes, you see:

```
Loading Host Resources MIB.....done
```

5. Restart the /etc/snmpd daemon by rebooting the system or killing and restarting the daemon manually with “ps” and “kill”
6. The “getmany” or “getmany” commands should now be able to obtain the system MIB information, as in this example:

```
getmany -f /etc/sysadm.d/hostmib.dfn localhost public hrSystem
```

The output should be similar to the following sample excerpt:

```
Name : hrSystemUptime.0  
Value : 118356496  
Name: hrSystemDate.0  
Value : 07 d0 03 0d 09 06 17 00 2d 00 00
```

Once the host resources agent is configured and running, when you re-discover the device, CPU/disk/memory etc tests should be found.