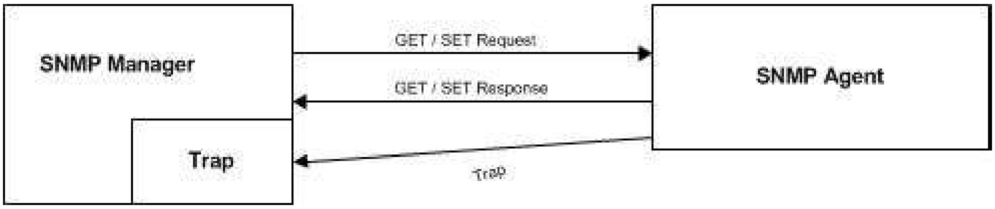
Using SNMP with Content Gateway, v7.7.x (not V-Series)

Topic 60056 | Using SNMP with Content Gateway | Updated 7-September-2012

Applies To:	Websense Web Security Gateway 7.7.x Websense Web Security Gateway Anywhere 7.7.x Websense Content Gateway 7.7.x

This article describes how to use Net-SNMP with software installations of Content Gateway to monitor the Content Gateway server and Content Gateway processes. Net-SNMP is an application used to implement Simple Network Management Protocol (SNMP).



For information about using SIEM and SNMP alerts with Web Security solutions, see Websense Security Information Event Management (SIEM) Solutions.

To use SNMP with Content Gateway, see:

1. *Installing Net-SNMP*
2. *Configuring SNMP to monitor and report on Content Gateway processes*
3. *Configuring CPU and disk usage events*

For information about using SNMP with V-Series appliances, see V-Series Appliance Manager online Help.

Additional Resources:

- An introduction to SNMP can be found on Wikipedia.
- Net-SNMP software resource: www.net-snmp.org
- Net-SNMP documentation: http://net-snmp.sourceforge.net/docs/man/

SNMP on the Content Gateway host system

Websense Content Gateway version 7.7.x is certified on the following Red Hat Enterprise Linux versions and corresponding CentOS versions:

- Red Hat Enterprise Linux, 6 series, updates 0, 1, and 2, 64-bit, Basic Server
- Red Hat Enterprise Linux, 5 series, updates 3, 4 and 5, base or Advanced Platform, 32-bit only

Note

For more information on Content Gateway v7.7 requirements, see System requirements for Websense Content Gateway in the Deployment and Installation Center.

The minimal installation does not include Net-SNMP.

To see if Net-SNMP is installed on your system, on the command line run:

```
rpm -qa | grep snmp
```

If SNMP is installed, you will see something like:

```
net-snmp-libs-5.3.2.2-5.EL5
net-snmp-5.3.2.2-5.EL5
net-snmp-utils-5.3.2.2-5.EL5
```

Note

SELinux should be disabled or in permissive mode when using Net-SNMP. To confirm its state, edit **/etc/sysconfig/selinux** and locate the “**SELINUX=**” variable.

Installing Net-SNMP

If Net-SNMP is not installed, install it now:

- *Installing Net-SNMP on Red Hat Enterprise Linux 6*
- *Installing Net-SNMP on Red Hat Enterprise Linux 5*

Installing Net-SNMP on Red Hat Enterprise Linux 6

The Net-SNMP software suite is available as a set of RPM packages in the Red Hat Enterprise Linux software distribution. For a list of available packages, see Available Net-SNMP packages.

To install Net-SNMP:

1. Make sure you have root permissions:

   ```
   su root
   ```

2. Install the Net-SNMP packages:

   ```
   yum install net-snmp net-snmp-libs net-snmp-utils
   ```

Installing Net-SNMP on Red Hat Enterprise Linux 5

The necessary RPMs are included with the Red Hat Enterprise Linux distribution media (disks or iso). For release 5, update 3, expect version 5.3.2.2-5.EL5.i386. The RPMs can also be downloaded from the Internet.

To install Net-SNMP:

1. Place the following RPMs in a temporary directory:

   ```
   net-snmp-libs-5.3.2.2-5.EL5.i386.rpm
   net-snmp-5.3.2.2-5.EL5.i386.rpm
   net-snmp-utils-5.3.2.2-5.EL5.i386.rpm
   ```

2. Install the RPMs with the following commands:

   ```
   rpm -ivh net-snmp-libs-5.3.2.2-5.EL5.i386.rpm
   rpm -ivh net-snmp-5.3.2.2-5.EL5.i386.rpm
   rpm -ivh net-snmp-utils-5.3.2.2-5.EL5.i386.rpm
   ```

After Net-SNMP is installed, it is important that you use **up2date** to get the latest Net-SNMP updates:

```
up2date -f net-snmp-libs net-snmp net-snmp-utils
```

Starting and stopping the SNMP service

After configuration is complete (see below) or any time it is necessary to start or stop the SNMP Agent service, use the following commands:

```
[root]# service snmpd start
[root]# service snmpd stop
```

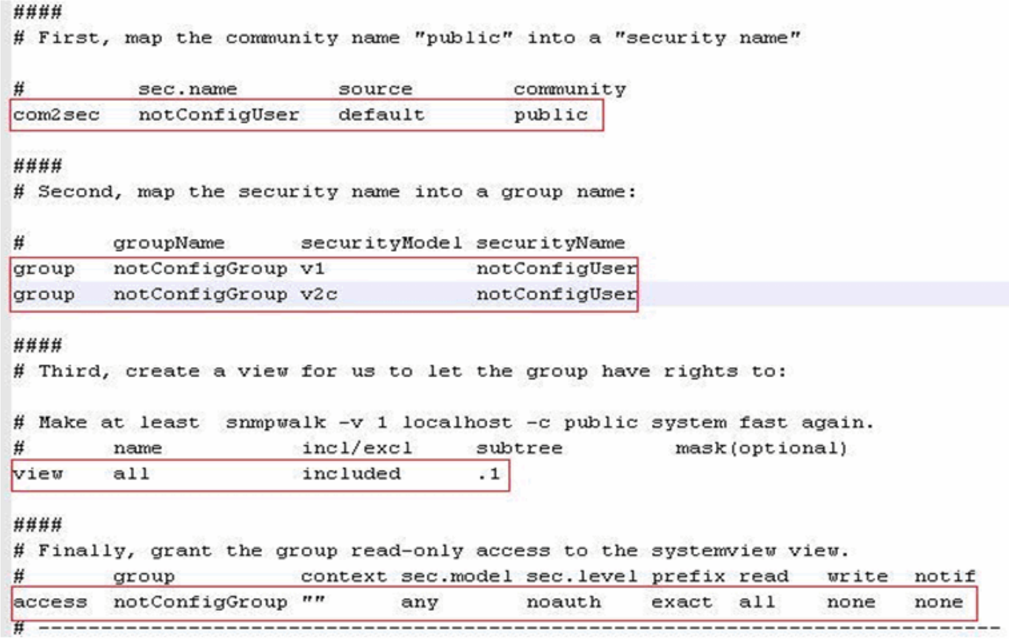
Basic SNMP configuration:

For detailed configuration information, see the comments in **/etc/snmp/snmpd.conf** and read the man page for **snmpd.conf(5)**.

After initial installation, for security purposes the SNMP service (snmpd) responds only to queries on the system MIB.

The following example shows how to configure **snmpd.conf** to change community names and open write access to the MIB tree.

Edit **/etc/snmp/snmpd.conf**, locate the lines boxed in red in the screen capture below, and modify each line to match the example.



```
####
# First, map the community name "public" into a "security name"

#          sec.name        source          community
com2sec    notConfigUser   default         public

####
# Second, map the security name into a group name:

#        groupName       securityModel securityName
group    notConfigGroup v1            notConfigUser
group    notConfigGroup v2c           notConfigUser

####
# Third, create a view for us to let the group have rights to:

# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#        name           incl/excl     subtree         mask(optional)
view     all            included      .1

####
# Finally, grant the group read-only access to the systemview view.
#        group          context sec.model sec.level prefix read   write  notif
access   notConfigGroup ""      any       noauth    exact  all    none   none
# -----------------------------------------------------------------------------
```

Important

To apply the changes to the configuration file, you must force the snmpd service to re-read the configuration by using the command:

```
service snmpd reload
```

Configuring SNMP to monitor and report on Content Gateway processes

To monitor Content Gateway processes, you must add the process names and MAX/MIN process values to the “Process checks” section of **snmpd.conf**. You also need to add the v2 trap specification.

Edit **/etc/snmp/snmpd.conf** and add the following lines in the “Process checks” area:

```
proc content_cop 1 1
proc content_gateway 1 1
proc content_manager 1 1
proc microdasys 2 1
proc microdasysws 1 1

# send v2 traps
```

```
trap2sink IP_address_of_SNMP_Manager:162
informsink IP_address_of_SNMP_Manager:162
rwuser all
agentSecName all
defaultMonitors yes
```

If Websense Web filtering is also running on the Content Gateway machine and you want to monitor it, add:

```
proc EIMServer 1 1
```

Important

To apply the changes to the configuration file, you must force the snmpd service to re-read the configuration by using the command:

```
service snmpd reload
```

Configuring CPU and disk usage events

To configure CPU usage events:

```
notificationEvent cpuUsgTrp cpuMaxUsageExceed
notificationEvent cpuUsgTrpClr cpuMaxUsageExceedClear
monitor -u wbsnQueryUser -r 60 -e cpuUsgTrp:cpuUsgTrpClr -o
ssErrorName -o ssCpuUser -o ssCpuSystem -o ssCpuIdle "High
CPU Usage" ssCpuIdle < 10
```

To configure disk usage events:

```
includeAllDisks 10%
notificationEvent freeDskTrp diskFreeMinSizeExceed
notificationEvent freeDskTrpClr diskFreeMinSizeExceedClear
monitor -u wbsnQueryUser -r 60 -e freeDskTrp:freeDskTrpClr -
o dskPath -o dskErrorMsg "dskTable" dskErrorFlag != 0
```

Verify SNMP configuration and trap reporting

Verify that the SNMP Agent (snmpd) is sending process trap messages, and that the SNMP Manager is receiving them.

snmptrapd is the process used by the SNMP Manager to listen for SNMP trap messages arriving on port 162 (default). A typical **snmptrapd** startup command might look like:

```
snmptrapd -f -Ls 162
```

where “-f” means do not fork() from the calling shell, and “-Ls” specifies where logging output is sent (“-Ls” sends output to **syslog**). 162 is the standard listening port for SNMP messages. For more detailed information, read the man page for **snmptrapd**.

> **Note**
>
> The default trap reporting interval for Agents is 10 minutes. If the default period is used, it can take as long as 10 minutes from the time a trap occurs to when the trap message is sent to the SNMP Manager. This parameter is configurable through the snmp “set” operation of “mteTriggerFrequency”. It can also be set in the **snmpd.conf** file for each **expression** with the “-r FREQUENCY” switch. See the **man** page for **snmpd.conf**.

To verify that SNMP Agent is sending trap messages:

1. On the SNMP Agent/Content Gateway machine, start a network packet analyzer and terminate the content_cop process.
2. In the packet capture data, look for an SNMPv2-Trap message for content_cop going to the SNMP Manager. The trap message might be similar to:

   ```
   Value: STRING: Too few content_cop running (# = 0)
   ```

To verify that SNMP Manager is receiving trap messages:

1. On the SNMP Agent/Content Gateway machine, terminate the content_cop process. Note that it may take several minutes from the time the trap occurs until the trap is sent to the SNMP Manager.
2. On the SNMP Manager machine, check the SNMP trap log for an entry for content_cop. The name and location of the log file is specified in the **snmptrapd** startup command (example provided above). Here is one way to find the message if it is being logged in /var/log/messages:

   ```
       cat /var/log/messages | grep content_cop
   ```

An entry might look like:

```
Nov 25 15:09:42 localhost snmptrapd[11980]: 10.10.10.10]: Trap,
DISPAN-EV = STRING , DISMAN-EVENT-MIB::mteHotOID = OID ,
DISMAN-EVENT-IB::prErrMessage.4 = STRING: Too few content_cop
    running (# = 0)
```

Grep for “snmptrapd” to see all log entries related to snmptrapd.

Use **nc** (netcat) to test basic UDP connectivity between the Agent and the Manager. For example, this command could be run on either side of the connection to test the designated UDP ports.

```
[root]# nc -u -v -z -w2 10.228.85.10 161-162
```

where “-u” indicates UPD, “-v” indicates verbose output, “-z” means to scan for listening daemons, and “-w2” indicates to wait 2 seconds before timing out.

Sample results:

```
10.228.85.10: inverse host lookup failed: Unknown host
(UNKNOWN) [10.228.85.10] 161 (snmp) open
```

For more information, see the man page for **nc**.

Important

Be sure to restart any processes or services that were terminated while verifying SNMP configuration and trap reporting.

Monitoring Red Hat Enterprise Linux system status with SNMP

snmpwalk is a query command that uses SNMP GETNEXT requests to retrieve tree values. The following are several examples of commands that return information about various aspects of system status. For more information, see the comments in **snmpd.conf**, the Linux man page for **snmpd.conf**, and www.net-snmp.org.

For all system status information:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-MIB::hrSWRun
```

or

```
[root]# snmpwalk -v 2c -c public HOST-RESOURCES-MIB::hrSWRun
```

For system information including date and time, initialized devices, kernel parameters, and more:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-MIB::hrSystem
```

For memory size, disk space, usage status, and more:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-
MIB::hrStorage
```

Note

Disk information is available at 1.3.6.1.2.1.25.2.3.1. Polling solutions should walk this table and identify the index corresponding to the root file system “/”.

For device ID and descriptions:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-
MIB::hrDevices
```

For process ID, process name, parameter, and status:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-MIB::hrSWRun
```

For CPU times and memory consumed by the process:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-
MIB::hrSWRunPerf
```

For installed software package names:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-
MIB::hrSWInstalled
```