

Chapter 6



NetVigil Monitors

6.1 Overview

NetVigil has a large number of monitors to handle different management protocols. For routers and Unix hosts, the commonly supported protocol is SNMP (Simple Network Management Protocol), whereas Microsoft Windows supports a native WMI protocol which allows agentless monitoring. In addition to these, NetVigil also supports custom monitors for application such as HTTP, POP, IMAP, SMTP, Radius, DNS, etc. which allows a single console for all elements of your IT infrastructure.

Numerical metrics collected from the different tests can be automatically post-processed and converted into delta, rate, percentage rate or percent values. These post processing directives can be applied using the TestTypes.xml file for auto-discovered tests or using the web interface for advanced tests.

6.2 SNMP

SNMP is a commonly supported management protocol for most routers and switches. It is a simple protocol where a management system (such as NetVigil) queries devices (such as routers and switches) for metrics, and the devices respond with the values for the queried metrics. NetVigil supports all versions of SNMP (v1, v2c and v3) and has a very efficient polling engine which reduces network traffic further by multiplexing multiple queries to a host in a single packet.

6.2.1 SNMP v1 and v2

In order to monitor an SNMP device using version 1 or 2c, all that is required is the correct SNMP “community” string which will allow querying the remote host. This community string (by default set to “public”) is specified on the Device management page in NetVigil. Keep in mind that most modern devices have access control lists which restrict which hosts can query it using SNMP- if such a list exists, you must enable access for the NetVigil host. See Appendix C, “Installing SNMP Agents”, for details on installing SNMP agents on specific hosts.

6.2.2 SNMP v3

SNMP version 3 has extended security features built in which require additional configuration. Instead of a community string, SNMP v3 has a username and an optional password, and an optional data encryption option. In NetVigil, you would specify these SNMP v3 parameters by setting the community string field to:

```
username : password : encryption_phrase
```

e.g.

```
fidelia:myPassword:encryptMe
```

The password is always encrypted using MD5 and must be at least 8 characters long. The currently supported data encryption method is DES.

6.2.3 SNMP MIB

Information in SNMP is organized hierarchically in a Management Information Base (MIB). The variables in the MIB table are called MIB objects, and each variable represents a characteristic of the managed device. Each object in the MIB table has a unique identifier, called an Object ID (OID), and these are arranged in a hierarchical order (like in a tree).

The standard MIB variables typically start with the OID prefix of “1.3.6.1.2.1” which translates as follows:

```
iso(1). org(3). dod(6). internet(1). mgmt(2). mib-2(1)
```

As an example, the OID for getting the description of a device:

```
system.sysDescr.0 = .1.3.6.1.2.1.1.1.0
```

Old legacy management systems required “loading” a MIB file for every device that needs to be monitored. This method was cumbersome, and required the user to correlate the different parts of the MIB tree to get a useful metric like “line utilization”. NetVigil uses an external XML library of SNMP variables, which eliminates the need to load MIB files since all the relevant MIB variables and the post-processing rules for each variable are stored in industry standard XML format.

6.2.4 Security Concerns

You can setup the community string on the router or switch to allow read-only SNMP queries or also allow “setting” variables. It is recommended that you only allow “reading” SNMP variables for security purposes and disable setting of the SNMP parameters.

6.2.5 RMON2

RMON2 support in network routers and switches allows gathering metrics on the type of network traffic using SNMP. You need to configure the RMON2 enabled device (interface) to log the type of traffic (instructions are implementation/hardware/vendor specific). By default, most RMON2 implementations monitor common ports, like TCP/http, TCP/telnet, UDP/dns, etc. Some vendor devices will not respond to RMON2 queries for a protocol until at least one packet of that particular type has crossed that interface (i.e. the stats table for that protocol will be empty and the host returns an invalid response to an SNMP query). So even if the RMON2 interface knows about SSH, no SSH specific stats will show up on the stats table, and therefore in the NetVigil auto-discovery.

The RMON2 protocol allows defining additional protocols that can be monitored in addition to the default ones. For details on how to determine the protocol identifier, see RFC-2074 at <http://www.ietf.org/rfc/rfc2074.txt>

6.3 Windows monitoring using WMI

6.3.1 Overview

NetVigil can monitor Windows hosts using the native Windows Management Instrumentation (WMI), which is installed by default on all Windows 2000, XP and 2003 or later versions, and available as an add-on for Windows NT hosts.

NetVigil performs WMI monitoring using the NetVigil WMI Query Server (nvwmiqd). This server is automatically installed on Windows DGEs, however, to perform WMI monitoring from a Linux or Solaris DGE, you must install and configure a NetVigil WMI Query Server as a “proxy” on a Windows system that can access the Windows hosts to be monitored. Note that there is a corresponding WMI Event Listener program (nvwmiel) to monitor windows events using WMI (see Section 7.10.1, “The NetVigil WMI Event Listener (nvwmiel)” on page 100)

The WMI query server makes WMI queries to the monitored hosts on TCP/UDP port 135 (which is the DCOM port). Also see Section 3.6, “Operating NetVigil Behind Firewalls” on page 41.

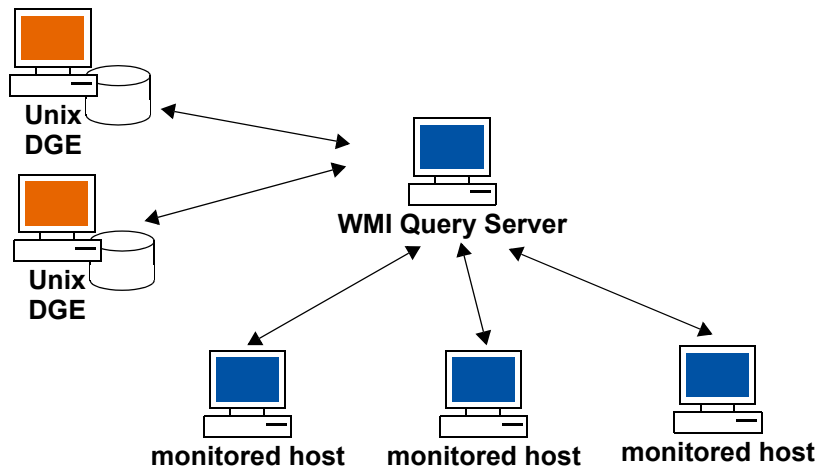


Figure 6.1 Relationship between DGEs, WMI Query Server, and monitored hosts

6.3.2 Installing the NetVigil WMI Query Server

NOTE: This service is automatically installed on Windows DGEs by default and is only needed if your NetVigil installation is on a Unix/Linux server.

The WMI Query Server (nvwmisd) should be installed on a Windows machine which has access to the windows hosts being monitored using NetBIOS. Test this by typing `NET VIEW \\remote_host` at a Windows Command Prompt.

Access requirements

The WMI Query Server queries all windows hosts using a common username and password for ease of management, instead of a separate user for each host. So you will need to ensure that each Windows host to be monitored through WMI has a user account that can be accessed by the WMI Query Server (with administrative rights to access various system tables). This username and password are stored in clear text in the `nvwmisd.ini` configuration file in the `NETVIGIL_HOME/etc/` directory.

- If the Windows hosts to be monitored is part of a domain, you will need the username and the corresponding password for a user who is part of the “Domain Administrator” group. The WMI Query Server will use this user’s credentials to connect to the Windows hosts being monitored for retrieving the WMI performance information.
- If the hosts are configured in one or more workgroups, and not part of a domain, then each host, including the host where the WMI Query Server is being installed, will need to have the same password for the “Administrator” user, or have another such common user which is part of the “Administrators” group

System Requirements

Install the NetVigil WMI Query Server on a system that meets or exceeds the following requirements:

- Pentium III processor, 512MB RAM, 10MB free disk space
- Windows 2000/2003/XP

Firewall requirements

When used in a 'proxy' mode, the DGE communicates with the WMI Query Server on TCP port 7667 by default. To specify a different port number, edit the configuration files on the Query Server and DGE as described in "Operating NetVigil Behind Firewalls" on page 41. If firewalls, access lists, etc. exist between the DGE and the WMI Query Server, the rules must be modified to allow incoming connections from the DGE to the WMI Query Server on the specified port. The rules should allow persistent connections (i.e., connections should not be forcibly timed out, even if there is no data flowing).

Installing the WMI Query Server

1. Download the WMI Query Server (wmiQDinstaller.exe) from the NetVigil CD-ROM or the Fidelia Support site (<http://support.fidelia.com>).
2. Double-click the install file, `wmiQDinstaller.exe`
3. Read the Introduction, and then click **Next** to continue.
4. Optionally, in the Choose Install Folder window, specify the folder in which you want to install the WMI Query Server. Click **Next** to continue.
5. In the Remote Query Credentials window, enter the username and password that the WMI Query Server will use to access monitored Windows hosts. The username can include a domain name (e.g., `ACMECORP\wmi_user`). In the **Password (Again)** field, enter the password a second time for validation. If you do not enter a **Remote Username** and **Remote Password**, the WMI Query Server will use the username and password of its local system account.
This username and password are stored in clear text in the configuration file, so this file should be protected from general user access. It is strongly recommended that a separate user account be setup on all hosts being monitored using WMI.
Click **Next** to continue.
6. In the Pre-Installation Summary window, review the configuration options. If they are correct, click **Install** to continue.
7. After the installation completes, click **Done** to close the installer.

The NetVigil WMI Query Server Configuration File

.....

After the NetVigil WMI Query Server is installed, either on a stand-alone server to be used with DGE on a Linux/Solaris server, or as part of the DGE on a Windows server, you can fine-tune it's configuration. The table below lists the configurable parameters in the configuration file `nvwmqid.ini`. This file can be found in the `WMI_Query_Server_Install_Dir\bin` (stand-alone install), or `NETVIGIL_HOME\etc`. If the file, or any of the parameters are missing, default values are used by the server.

NOTE: The configuration file may contain parameters that are not listed here. Do not modify unlisted parameters unless advised to do so by Fidelia technical support.

Table 6.1

Parameter	Description	Default Value
Port	TCP port on which NetVigil WMI Query Server listens for incoming connections from DGEs	7667
Username	User name that a DGE must use when logging in to NetVigil WMI Query Server	wmiuser
Password	Password that a DGE must use when logging in to NetVigil WMI Query Server	fixme
Server_Username	User name that the NetVigil WMI Query Server uses to connect to Windows hosts being monitored	n/a
Server_Password	Password that the NetVigil WMI Query Server uses to connect to the Windows hosts being monitored.	n/a

Example: Sample Configuration File (nvwmqid.ini)

.....

```
[ServerConfig]
Port = 7667
Username = dgeuser
Password = fixme
Timeout = 100000
Threads = 4
```

```
Server_Username = ACMECORP\localuser  
Server_Password = testpassword
```



6.3.3 DGE Configuration for Proxy WMI Server

If you have any Unix/Linux DGEs which need to use the WMI Query Server on a Windows machine as a proxy, edit the following parameters in `$NETVIGIL_HOME/etc/dge.xml`:

```
<wmiQueryServer>  
  <host name="my_host_1" address="1.1.1.1" port="7667"  
    username="wmiuser" password="wmipassword" />  
</wmiQueryServer>
```

and restart the DGE so that the changes can take effect.

The various parameters in the `dge.xml` file are:

host name	is a unique, descriptive name for the WMI Query Server host that this DGE uses for WMI monitoring (e.g., <code>Denver_WMI_QueryHost</code>).
address	is the IP address of the WMI Query Server host, in dotted quad notation. If the DGE is running on Windows, this will be set to <code>127.0.0.1</code>
port	is the TCP port on the WMI Query Server to which the DGE connects. This must match the <code>Port</code> parameter in the <code>nvwmisd.ini</code> file on the WMI Query Server.
username	is the username that the DGE uses to log in to the WMI Query Server. This must match the <code>Username</code> parameter in the <code>nvwmisd.ini</code> file on the WMI Query Server.
password	is the password that the DGE uses to log in to the WMI Query Server. This must match the <code>Password</code> parameter in the <code>nvwmisd.ini</code> file on the WMI Query Server.

You can have up to 4 DGEs using a single WMI Query Server as a proxy.

6.3.4 Provision WMI Hosts in NetVigil

Once you have the WMI Query Server installed, adding hosts to be monitored using WMI is done similar to other devices. You need to ensure that the devices are added to a location where all the DGEs are 'WMI Enabled' (have access to a NetVigil WMI Query Server). Provisioning these devices is described in the Web User Guide under "Manage Devices".

6.3.5 Troubleshooting WMI Issues

This section lists problems that may arise with WMI monitoring, possible causes, and solutions.

❑ Problem: “The DGE can’t discover WMI tests for Windows hosts.”

- Ensure that the NetVigil WMI Query Server is running
- Verify that the username and password being used by the WMI Query server (in `nvwmqid.ini`) is for a valid administrator account on the target hosts.
- Check the error log on the WMI Query server for errors.

❑ Problem: “The DGE discovered WMI tests, but it can’t monitor configured tests using WMI.”

- Ensure that the NetVigil WMI Query Server is running
- Check the error log on the WMI Query server for any errors.

❑ Problem: “Ever since I installed WMI, I’m getting test provisioning errors.”

- When you use NetVigil to discover tests, it may discover SNMP and WMI tests with the same name. However, if you try to create SNMP and WMI tests with the same, you will get provisioning errors. To keep names unique, use a naming convention to distinguish between SNMP and WMI tests. For example, start the names of all WMI tests with “`wmi_`”.

6.4 Setting up Apache Web Monitor

NetVigil can monitor various performance metrics from apache directly from the http server process. The apache server will need to be compiled with `mod_status` support. By default this module is included in the build process, but you can verify this using the following commands:

```
(on Unix)
cd /path/to/apache
bin/httpd -l | grep mod_status
```

```
(on Windows)
cd \path\to\apache
bin\httpd -l | findstr "mod_status"
```

If the output shows “mod_status.c” then this module is included in the web server. You will need to enable this module in “httpd.conf”. Refer to the documentation at

http://httpd.apache.org/docs/mod/mod_status.html for instructions on how to enable and configure it. You will need to make sure that:

1. The URL for the module matches the URI specified for the NetVigil Apache monitor specified in the configuration file (described below).
2. “ExtendedStatus On” directive is applied
3. NetVigil hosts (WebApp, DGE) are included in the “Allow” directive

For example, if the Web Application is running on host 192.168.100.5, and the DGE is on host with address 192.168.200.10, the module configuration in httpd.conf may look like:

```
<Location /server-status>
  SetHandler server-status
  ExtendedStatus On
  Order Deny,Allow
  Deny from all
  Allow from 192.168.100.5
  Allow from 192.168.200.10
</Location>
```

Once the configuration has been enabled/modified, the httpd process will need to be restarted (<http://httpd.apache.org/docs/stopping.html>) to apply the changes.

Editing NetVigil Configuration

On each DGE, edit “NETVIGIL_HOME/lib/ext/gp_apache/config.xml” and locate the following section:

```
<uri>
  <protocol>http</protocol>
  <port></port>
  <file>/server-status?auto</file>
</uri>
```

Edit the <file>...</file> property to match the URL specified in the configuration of the “mod_status” module. If the apache server is configured to provide the performance stats via URL “/internal/stats/apache”, then the configuration above would be changed to:

```
<uri>
  <protocol>http</protocol>
  <port></port>
  <file>/internal/stats/apache?auto</file>
</uri>
```

Note that the “?auto” parameter should be left as-is. The remaining configuration items should not be altered in any way without specific instructions from Fidelia Support.

6.5 SQL Performance Monitor for Databases

You can issue SQL queries to databases and measure the response time for the query or even verify that the return value matches any specified value. Note that this is separate from monitoring the internal metrics of databases which is done using WMI or SNMP on Oracle, SQL Server, etc.

A standard JDBC driver is included for the most commonly used databases. However, you can add monitoring of additional databases by adding the JDBC driver for this database.

Example: To monitor DB2 using SQL

.....
 First a copy of the JDBC (type 3) driver is required for DB2. This driver cannot be distributed with NetVigil as the driver has to match the product and “fixpack” version of the database itself. Otherwise the connections may fail, or the data across client/server communication may be corrupted. You should be able to find the JDBC driver in “java” directory in the DB2 installation path in the form of a file named “db2java.zip”

Copy this file from the DB2 host to NetVigil host in the “lib” directory under NetVigil installation path. If NetVigil has been installed in a distributed environment, copy “db2java.zip” to each host running a NetVigil component. On Windows version of NetVigil, edit (use “notepad”, making sure that the word wrap feature is disabled) “bin\monitor.lax” and locate the line that starts with:

```
lax.class.path=..
```

At the end of the line, add “;../lib/db2jdbc.zip” (w/o the quotes). Save the file. No such changes are required on Linux/Solaris versions of NetVigil.

Edit “etc/netvigil.xml” and locate the “<jdbc-drivers>” section. Above the existing “<jdbc-driver name...” entries, create a new entry for the DB2 database:

```
<jdbc-driver name = "IBM DB2"  
  url="jdbc:db2://$DEVICE:6789/$DATABASE"  
  driver="com.ibm.db2.jdbc.net.DB2Driver"/>
```

If the DB2 database is listening on a TCP port other than 6789, make sure to specify the correct port number. Make the same changes on all hosts where NetVigil is installed (for distributed configuration).

Restart the Web Application and DGE components. Now when you create a new SQL query test, you should see “IBM DB2” in the drop down list of database vendors. Provide the necessary database name, login username and password and an appropriate SQL query and NetVigil should execute the query against the specified database.

6.6 Internet Services (Mail, HTTP, etc)

NetVigil has built in monitors for all Internet Services such as:

- POP3 - simulate a user and log into the POP server
- IMAP - simulate a user and log into the IMAP mail server
- SMTP - connect and issue the SMTP handshake
- FTP - simulate a user and log into the FTP server
- HTTP/HTTPS - download a page and check if it can be downloaded completely. Also see the URL Transaction Monitor below.
- DNS - query and match the response from the DNS servers
- Radius - make a query to the radius server
- DHCP - request an address from the DHCP server

These require parameters custom to each service in order to do a complete “synthetic” transaction and test the service. The provisioning of these tests is described in the Web User Guide.

NetVigil measures the time to complete each transaction, and raises an alert if the response time exceeds the warning or critical thresholds. It also generates an alert if the transaction is incomplete or cannot be completed or times out.

6.7 URL Transaction Monitor

NetVigil has a built in monitor to simulate a user logging into a Web site, filling in a form or clicking on a series of links and expect to see the complete transaction similar to an end user. This is different from the HTTP/HTTPS monitors which just test downloading of a single page, since this monitor can walk through a complete series of pages like a user transaction.

