

Troubleshooting



A.1 Troubleshooting the DGE - BVE Connection

Upon startup, each DGE component connects to the provisioning database (located on the provisioning server) and downloads all tests that are configured for that DGE. The DGE components maintain a connection to the provisioning database at all times. As devices and tests are added, updated, or removed, the provisioning server notifies the relevant DGE of the changes in real-time.

If the communications link between the provisioning database and the DGE is broken, the DGE repeatedly attempts to restore the connection, while continuing to monitor, using the configuration information that it has cached in memory. Once the connection to the provisioning database is restored, the DGE shuts down. A cron job restarts the DGE shortly thereafter. The reason for the shutdown and restart is that while the DGE was unable to communicate with the provisioning server, it may have missed notices about changes to device/test configurations. In the process of restarting, the DGE downloads a fresh copy of the list of tests and proceeds with normal operation.

A.2 Log Files Used in Troubleshooting

Several log files can be useful in troubleshooting. All log files are located under `NETVIGIL_HOME/logs` directory.

Log File	Use By
<code>stderr.log</code>	All startup scripts, monitors
<code>netvigil.error</code>	Any warning, error or critical level messages generated by any component is logged in this file.

Log File	Use By
monitor.info	Information on monitors are logged to this file as tests are performed, actions triggered, etc.
webapp.info	All user tasks, both in the web application and BVE socket server are logged to this file. Tasks include create, delete, update, suspend and resume tasks performed on devices, Departments, users, etc.
tomcat.log	Any errors generated inside jsp pages in the web application component is logged in this file.
poet.log	Provisioning database specific errors

A.3 Other Common Problems

Problem: Newly added tests remain in UNKNOWN state

For a detailed explanation of the factors that can cause tests to go into UNKNOWN state, see chapter “Real-time Status Monitoring” in the “NetVigil Web User Guide”. You can also click on the UNKNOWN icon itself for a test (not a device) and a little pop-up window will give the reason for the UNKNOWN state.

Make sure that the DGE that controls the device to which the tests belong hasn’t lost its connectivity to the provisioning server. If the connection is down and the DGE is running with its cached configuration, it does not know about newly added tests. The DGE should automatically restart itself when the connection is restored. If it doesn’t, see “Problem: DGE does not automatically restart when the connection to the provisioning database is restored” on page 361.

1. Check the load (CPU utilization, load average, blocked disk I/O) on the DGE host. In high-load situations, it may take longer to schedule and run newly-added tests.
2. Make sure that the DGE process is running. On UNIX systems, you can check this with the following command:

```
cd NETVIGIL_HOME
etc/monitor.init status
```

Where `NETVIGIL_HOME` is the directory in which NetVigil is installed (typically `/user/local/NetVigil`).

You can also see whether the DGE is running from the Web Interface. If the DGE is not running, when you drill down into older devices, `TEST TIME` and `DURATION` values for tests that are not in `UNKNOWN` state should be light blue, indicating that the test results are old.

Problem: DGE does not automatically restart when the connection to the provisioning database is restored

Make sure that the crontab entry for root on the DGE includes the contents of `NETVIGIL_HOME/etc/crontab.netvigil`.

Problem: Device test status showing up as unreachable and unable to retrieve historical test results. Following messages show up:

```
> java.sql.SQLException:General error: Can't open file:
>'lasttestresult.MYI'. (errno:145)
```

The error indicates that the DGE database experienced minor corruptions, possibly due to the power failure and needs to be repaired. To correct the issue, shutdown all NetVigil components using the service controller, open a command window and execute the following commands (substitute correct drive letter/path names)

```
C:
cd "\\Program Files\Fidelia Netvigil"
del logs\netvigil.error
mysql\bin\myisamchk -r database\mysql\aggregateddatadb\*.MYI
```

this should give an output similar to:

```
-recovering (with sort) MyISAM-table
'database\mysql\aggregateddatadb\AggregationInfo.MYI'
Data records: 1072

-Fixing index 1
-Fixing index 2
...
```

Problem: NetVigil Web Application does not start up or cannot connect to it

Make sure you do NOT have IIS running or some other web server on port 80. NetVigil comes complete with its own Web Server and does not need IIS to serve web pages. If IIS is not being used for anything else, it should either be uninstalled or configured so that it does not start automatically. To disable IIS, go to

Control panel ->Administrative Tools ->Services
and change the startup type for “World Wide Web Publishing Service”
to manual/disabled.

In order to check if IIS is disabled, do the following:

- Use “NetVigil Service Controller” to shut down all components
- Open a command window and execute the following commands:

```
netstat -an | findstr ":80"
```
- If the output from the command includes a line with “LISTENING”
then IIS is running

If you cannot disable IIS for any reason, the NetVigil Web Application
can be run on an alternate port. You will need to edit
tomcat\conf\server.xml as described in Section 3.4.11, “Web server
TCP/IP port” on page 37.

Problem: Cannot access Web Application

1. Make sure IIS is not running
2. Ensure that there is no firewall software, including the “Internet
Connection Firewall” (ICF) that is bundled with Windows 2003. You
can check if ICF is enabled:
 - Click on Control Panel -> Network Connections
 - Right Click on the Ethernet adapter (Local Area Connection)
 - Select “Properties”
 - Click on “Advanced” tab

If the “Protect my computer...” option is enabled, uncheck it and apply
the changes.

Problem: The error: ‘wpg report schedule’ occurs when several scheduled reports are created and it is not possible to schedule it on the report server

Take a look at “etc/netvigil.properties” file on your Web Application
host and locate the “org.quartz.dataSource.myDS.URL” parameter. See
if the IP address specified in the URL match the IP address of that host
(or set to 127.0.0.1). Also check the values of “report.server.hostname”
and “report.server.port” values under “tomcat/webapps/ROOT/WEB-
INF/web.xml”. If the values are not set correctly, update them and

restart the Web Application. Once configured, update each scheduled report to make any trivial change (e.g. the name) so that it is scheduled properly.

Problem: Compaq Insight Manager agent is reporting incorrect virtual memory

This is a known bug in older versions of Compaq Insight Manager. Please download the latest version 7.10 from:

<http://h18004.www1.hp.com/support/files/server/us/download/19909.html>

Problem: E-mail notification set to wrong time zone

Setting Time Zone for E-mail Notifications:

If you are using Windows version of NetVigil, use notepad to edit “NETVIGIL_DIR\bin\monitor.lax” and at the bottom of the file, add the following line:

user.timezone=America/Los_Angeles (e.g.for Pacific time zone)

Once the entry has been added, save the file and restart the “Data Gathering Element” using the service controller.

Problem: Some WMI metrics “missing” for windows applications

If you cannot discover WMI metrics for some applications on Windows hosts, you might need to “resync” the WMI agent on the Windows server:

On Win2000 hosts, run the following from a CMD window:

```
winmgmt /clearadap # clear all counters
winmgmt /resyncperf <process id>
```

You have to find the process ID of the winmgmt process in the “Process” tab of the Windows Task Manager.

On XP/2003 hosts, you need to use:

```
wmiadap /f
```

These problems are described more fully in the Microsoft KB article 820847.

A.4 Querying SNMP Devices Manually

For Windows:

```
cd \Program Files\Fidelia Netvigil  
bin\snmpwalk -m "" -c public -v 2c ipAddress:port mib  
e.g.  
bin\snmpwalk -m "" -c public -v 2c 10.1.2.3 .1.3.6.1.2
```

For Unix:

```
cd $NETVIGIL_DIR  
bin/snmpwalk -m "" -c public -v 2c ipaddr:port mib
```