Performance Endpoints 5.1

Sun Solaris

April 2006

Legal Notice

Contents

About This Guide

This guide provides practical information about the free Performance Endpoint software NetIQ Corporation provides in association with its Systems Management products. It explains installation and configuration for all the endpoint platforms supported by NetIQ AppManager Networks Response Time and VoIP Quality modules, NetIQ Vivinet Assessor, and NetIQ Vivinet Diagnostics. You can also download individual endpoint guides in PDF format from the Internet at www.netiq.com/download/endpoints.

Intended Audience

This guide contains information about Performance Endpoint software for users of NetIQ AppManager, Vivinet Assessor, and Vivinet Diagnostics.

Using This Guide

Depending on your environment and your role as a user of the aforementioned NetIQ products, you may want to read portions of this guide selectively. It contains the following chapters:

- Chapter 1, "Introduction to Performance Endpoints," describes the software and hardware requirements and the supported functions of the Performance Endpoints, version 5.1.
- Chapter 2, "Endpoint Initialization File," discusses the functions of the endpoint initialization file, which is installed with each Performance Endpoint.

- Chapter 3, "Sun Solaris," explains the installation, configuration, and operation of the Performance Endpoint software for Sun Solaris version 2.4 (or later).

In addition to these chapters, an index is provided for your reference.

Conventions Used in this Guide

The following conventions are used in this guide:

- `Fixed-width font` is used for source code, program names or output, file names, and commands that you enter at the command line.
- An *`italicized`* fixed-width font is used to indicate variables.
- **Bold text** is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- *Italics* are used for book titles.

Complementary NetIQ Products

NetIQ Corporation is a leading provider of intelligent, e-business management software solutions for all components of your corporate infrastructure. These components include servers, networks, directories, Web servers, and various applications.

NetIQ provides integrated products that simplify and unify directory, security, operations, and network performance management in your extended enterprise. NetIQ provides the following categories of products:

- **Systems Management** NetIQ Systems Management products provide control and automation for monitoring the performance and availability of your critical servers, applications, and devices; tools for diagnosing and

analyzing system operation; and extensive network monitoring capabilities to provide a complete, end-to-end management solution for the enterprise. These products enable you to pinpoint existing and potential server and network problems and resolve those problems quickly and effectively.

- **Security Management** NetIQ Security Management products enable you to administer, assess, enforce, and protect all aspects of security within your Windows environment. These products provide incident management and intrusion detection, vulnerability assessment, firewall reporting and analysis, and Windows security administration.
- **Smart Solutions for Windows Administration** NetIQ Smart Solutions for Windows Administration include tools for managing, migrating, administering and analyzing your Windows, Exchange, and SQL Server environments. These products include tools for setting and enforcing policies that govern user accounts, groups, resources, services, events, files, and folders, and products that automate time-consuming administration tasks.

Contacting NetIQ

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our

partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

Telephone:	713-418-5678
Support:	support@netiq.com
Web site:	www.netiq.com/support

Chapter 1

Introduction to Performance Endpoints

This guide contains information about the Performance Endpoints, which are available for more than 15 different operating systems.

All the information you need to install, configure, and run the endpoints in your network is included here. In addition to topics discussing issues common to all the endpoints, this guide also contain information about each operating system, organized in separate chapters.

The following topics describe the software and hardware requirements and the supported functions of the Performance Endpoints, version 5.1.

- "Operating System and Protocol Stack Support" on page 2
- "Endpoint Capabilities" on page 2

The latest version of the endpoint software can always be downloaded free from the Internet. A single installable file is available for each supported operating system. Endpoints are available for downloading at www.netiq.com/download/endpoints.

You cannot run endpoint software from a CD-ROM; you must install it on a computer.

Operating System and Protocol Stack Support

The following table lists the software with which we have tested the Performance Endpoints for each operating system.

Endpoint	OS Version	TCP, UDP, RTP	IP Multicast Version
Cobalt RaQ3 (x86)	Kernel 2.0.32	Included	Kernel 2.0.32
HP-UX	HP-UX v10.10	Included	v10.10
IBM AIX	AIX v4.1.4	Included	v4.1.4
Linux (x86 and MIPS)	Kernel 2.0.32	Included	Kernel 2.0.32
Microsoft Windows Millennium Edition (Me)	Windows Me	Included	Included
Microsoft Windows 2000	Windows 2000	Included	Included
Microsoft Windows 2003 Server	Windows XP (32-bit)	Included	Included
Microsoft Windows XP	Windows XP (32-bit)	Included	Included
Sun Solaris for SPARC	Solaris v2.4	Included	v2.4
Sun Solaris for x86	Solaris v2.4	Included	v2.4

Endpoint Capabilities

The following table indicates which endpoints have been tested with and are supported by NetIQ products.

NetIQ Product	Vivinet Assessor	Vivinet Diagnostics	AppManager for Networks-RT	AppManager for VoIP Quality
Endpoint				
HP-UX	No	No	Yes	No
IBM AIX	No	No	Yes	No
Linux for Cobalt RaQ3 (x86)	Yes	Yes	Yes	Yes

NetIQ Product	Vivinet Assessor	Vivinet Diagnostics	AppManager for Networks-RT	AppManager for VoIP Quality
Endpoint				
Linux x86 (TAR)	Yes	Yes	Yes	Yes
Linux x86 (RPM)	Yes	Yes	Yes	Yes
Microsoft Windows Me/2000/XP/2003	Yes	Yes	Yes	Yes
Microsoft Windows Me/2000/XP/2003 (Web-Based)	Yes	No	No	No
Sun Solaris (SPARC)	Yes	Yes	Yes	Yes
Sun Solaris Endpoint (x86)	Yes	Yes	Yes	Yes

Chapter 2

Endpoint Initialization File

An endpoint initialization file is installed with each Performance Endpoint. With this file, you can do the following:

- Restrict the use of this endpoint to specific AppManager, Vivinet Diagnostics, or Vivinet Assessor Console.
- Control which access attempts are logged in an audit file.
- Change the filename of the audit file.
- Enable only particular protocols on this endpoint for setup connections.

On most operating systems, this file is named `endpoint.ini`. This file has the same format and structure on all the operating systems.

Here are the default contents of the endpoint initialization file. You can change these keywords and their parameters to tailor individual endpoints for your needs.

Keyword	Parameters
ALLOW	ALL
SECURITY_AUDITING	NONE
AUDIT_FILENAME	ENDPOINT.AUD
ENABLE_PROTOCOL	ALL

This file is an editable text file. There is a separate copy for each operating system. You might want to make changes to it once, before endpoint installation, which are then incorporated into all the installs for different sets of computers. You can modify this text file before installation by copying the endpoint installation directory for an

operating system to a hard drive (preferably a LAN drive), and then modifying the file before running the install from that drive.

We strongly recommend that you make any changes to your `endpoint.ini` files once, before you install any endpoints, as opposed to installing the endpoints and then going back to each of them and separately modifying each one.

ALLOW

This keyword determines which computers can run tests using this endpoint.

To allow any user to run tests on this endpoint, use the `ALL` parameter, which is the installation default:

```
ALLOW ALL
```

However, the default "**`ALLOW ALL`**" is ***not*** recommended. Although `ALLOW ALL` makes it easy to install an endpoint and see that it's running, it also lets any user who can reach the endpoint potentially use that endpoint as a traffic generator.

To allow only specific users to run tests with this endpoint, remove the `ALLOW ALL` line and identify one or more specific computers by their network addresses. You can specify more than one address per protocol. For example,

```
ALLOW TCP 192.86.77.120
ALLOW TCP 192.86.77.121
```

Specify a connection-oriented protocol (that is, TCP) as the first parameter and provide its corresponding network address as the second parameter. Endpoints listen only for incoming tests on connection-oriented protocols, such as TCP. Datagram tests are set up and results are returned using their "sister" connection-oriented protocol; thus, UDP tests are set up using TCP.

The network address in TCP/IP must be in dotted notation.

Endpoints do not respond to endpoint discovery requests unless the IP address of the computer is specifically allowed (or unless `ALLOW ALL` is specified). This prevents the user of a computer from finding endpoints to which it should not have access.

You cannot use the `ALLOW` parameter to restrict access from one endpoint to another endpoint. The `ALLOW` parameter can be used only to permit (or prevent) access from specific computers to the endpoint at which the parameter is defined.

If, for some reason, you need to restrict your endpoint to access only your own computer, specify your own IP network address rather than `127.0.0.1`. Specifying `127.0.0.1` (the equivalent of `localhost`) allows any other user who specifies `localhost` as Endpoint 1 to access your computer as Endpoint 2.

SECURITY_AUDITING

This keyword determines which access attempts the endpoint keeps track of in its audit file. Here are the possible parameters:

NONE	Writes nothing to the audit file
PASSED	Logs only access attempts that passed the ALLOW address check.
REJECTED	Logs only access attempts that failed the ALLOW address check.
ALL	Logs both passed and rejected access attempts.

If a test initialization fails for a reason other than address checking, no entry is made in the audit file.

AUDIT_FILENAME

This keyword specifies the filespec for the audit file. See "SECURITY_AUDITING" on page 7 to understand the types of events logged in its audit file. The default filename in `endpoint.ini` is `endpoint.aud`. If no drive or path is specified, the audit file uses the drive and path of the endpoint program.

This file contains at most two lines for each endpoint pair that is started on this endpoint. These two lines represent the start of an endpoint instance and the end of that instance.

Each line written to the audit file consists of a set of information about the endpoint instance and what it has been asked to do. The information is written in comma-separated form, so you can load the audit file into a spreadsheet or database. When the audit file is created, an initial header line explains the contents of the subsequent entries.

The following table shows the fields of each entry in the audit file:

Field	Description
Time	The date and time when the entry was created, in the local time zone.
Action	Whether an endpoint instance was "Started" or "Ended."
Endpoint	Whether the endpoint is in the role of Endpoint 1 or Endpoint 2.
Protocol of Console	The network protocol used to contact Endpoint 1.
Network Address of Console	The network address as seen by Endpoint 1. If you encounter problems setting up your `ALLOW` entries, use this value for the protocol address.
Security Result	Whether this `SECURITY_AUDITING` "passed" or was "rejected." If this is an entry for an "Ended" action, this field is reported as "n/a."
Endpoint Partner Protocol	The network protocol used to run the test with a partner endpoint.
Endpoint Partner Address	The network address of a partner endpoint.

ENABLE_PROTOCOL

This keyword lets you control which connection-oriented protocols an endpoint uses to listen for setup connections. This does not affect the network protocols, which can be used to run tests. Here are the possible parameters:

`ALL`

`TCP`

In general, you should use the `ALL` setting (the default). Specify protocols explicitly to reduce the overhead of listening on the other protocols or if you're encountering errors when listening on the other protocols.

See the discussion of the `ALLOW` keyword on page 6 for information about support of the datagram protocols, RTP, and UDP.

Configuring Endpoints for Large-Scale Customization

To customize features such as automatic upgrades, you must edit the `endpoint.ini` file for each endpoint. For obvious reasons, you may not want to undertake such a potentially lengthy procedure. You can extract the files located in `gsendw32.exe` if you need to perform a large-scale customization of endpoint.ini. In addition to WinZip, you'll need the WinZip command-line support add-on and WinZip Self-Extractor. Here's how to use it:

1. Open the file `gsendw32.exe` using WinZip. See "Using WinZip" on page 15 for more information.
2. Extract the files to a temporary directory.
3. Edit or replace the `endpoint.ini` that is now in the temporary directory.
4. Using WinZip, create a new archive that contains all the files in the temporary directory.
5. Using the WinZip Self-Extractor, create a self-extracting executable; for the command line to run, enter the following:

   ```
   SETUP.EXE replace_ini
   ```

Now, anyone who executes the new executable you've created will automatically have the endpoint installed using the `endpoint.ini` file that you've customized.

To create a file that silently self-installs with a custom endpoint.ini:

1. Open the file `gsendw32.exe` using WinZip. See "Using WinZip" on page 15 for more information.
2. Extract the files to a temporary directory.
3. Edit or replace the `endpoint.ini` that is now in the temporary directory.
4. Create a custom response file (say, `customer.iss`); enter

   ```
   i. SETUP -noinst -r -f1.\customer.iss
   ```

5. Using WinZip, create a new archive that contains all the files in the temporary directory.
6. Using the WinZip Self-Extractor, create a self-extracting executable; for the command line to run, enter the following:

   ```
   SETUP.EXE replace_ini -s -f1.\CUSTOMER.ISS
   ```

Now, anyone who executes the file you've created will automatically have the endpoint installed using `customer.iss` as the response file, and the `endpoint.ini` file installed will also be the customized version you created.

Chapter 3

Sun Solaris

This chapter explains the installation, configuration, and operation of the Performance Endpoint software for Sun Solaris version 2.4 (or later). The endpoints operate on the "SPARC" and "x86" versions of Solaris.

- SPARC computers contain CPUs made by Sun Microsystems and others.
- x86 computers are commonly known as "Intel-compatible PCs"; they contain CPUs made by Intel, AMD, Cyrix, or others.

Consult the following topics for details on working with the Performance Endpoints for Sun Solaris:

Installation Requirements for Sun Solaris Endpoints

Here's what you need to run the endpoint program with Sun Solaris:

- A computer capable of running Sun Solaris well.

  For SPARC computers, any system seems to give good performance.

  For x86 computers, this implies a CPU such as an Intel 80386, 80486, a member of the Pentium family, or equivalent. A Pentium or better is recommended.

- At least 32 MBytes of random access memory (RAM).

  The total RAM requirement depends on the RAM usage of the underlying protocol stack and the number of concurrent connection pairs. For large tests involving hundreds of connections through a single endpoint, additional memory may be required.

- A hard disk with at least 4 MBytes of space available.
- Sun Solaris version 2.4 or later, with TCP/IP networking and corresponding networking hardware installed and configured. This version also supports IP Multicast.
- Acrobat Reader to view the .PDF files.

  Acrobat readers are loaded on most computers for viewing other documents, but if you do not have one, they are available at the Adobe Web site: www.adobe.com/prodindex/acrobat/readstep.html.

Installing the Endpoint for Sun Solaris

First, make sure that you are logged in as a "root" user. Also, remember that all the commands and parameters discussed here are case-sensitive; use the combination of uppercase and lowercase letters as shown. The following instructions explain how to install an endpoint from a CD-ROM and from the Internet.

- "Installing from a CD-ROM" on page 13
- "Installing from the Web" on page 15
- "Installation Defaults File for Solaris" on page 16

- "Unattended Installation for Solaris" on page 17
- "What Happens During Installation" on page 18

Note To install version 5.1 of the Endpoint for Sun Solaris over a previous version of the endpoint, you need to modify the admin file to contain "`instance=overwrite`" and "`conflict=nocheck`."

Installing from a CD-ROM

To install the endpoint from a CD-ROM:

1. Put the CD-ROM in your CD-ROM drive.
2. Next, enter the `VOLCHECK` command, which tells Solaris that the CD-ROM is inserted in the drive and is readable. `VOLCHECK` returns quickly to the command prompt, without a message.

   ```
   volcheck
   ```

3. The CD-ROM contains an archive of the endpoint package. First use the `rm` command to ensure a clean temporary install directory. Then use the `tar` command to extract the archive contents from the CD-ROM.

   For SPARC systems, enter:

   ```
   cd /tmp
   rm -fr endpoint
   tar -xvf /cdrom/endpoint/solaris/endsunr.tar
   ```

   For x86 systems, enter:

   ```
   cd /tmp
   rm -fr endpoint
   tar -xvf /cdrom/endpoint/s86/ends86r.tar
   ```

4. Next, install the endpoint package using the `pkgadd` command:

   ```
   pkgadd -d /tmp endpoint
   ```

   The `pkgadd` command is not part of the endpoint installation. It is part of the standard Solaris installation and can be found in the `/usr/bin` directory.

5 You will see the license agreement, presented with the `pg` command. Press the spacebar until the end of the agreement is displayed. You are asked whether you accept the terms and conditions of the agreement. If you do, enter `accept_license` and press `Return`.

6 Next, you are asked the following question:

```
This package contains scripts which will be executed with super user
permission during the process of installing this package.

Do you want to continue with the installation of this package [y,n,?]
```

Enter a lowercase "`y`" to complete the installation script. About 20 lines of text give the status of the installation. When it's finished, the last line reads:

```
Installation of <endpoint> was successful.
```

You may instead see the following message:

```
Notice! There were potential problems with migrating from
$oldInstallPath to $installPath. Review the warnings displayed above
for further explanation.
```

If you see this message, please review the entire output from the install script for an explanation of the warnings and further instructions.

To delete the archive contents from the temporary working directory:

```
cd /tmp
rm -fr endpoint
```

Remove the CD-ROM by entering `eject` at a command prompt.

This is a good time to read the `README` file, installed with the endpoint in `/opt/NetIQ`, for the latest information about the endpoint program.

When you've completed installation, refer to "Configuring Solaris Endpoints" on page 19 to make sure your endpoint is ready to be used in monitoring.

Installing from the Web

To install an endpoint you've downloaded from the Web:

1 First, use the `rm` command to ensure a clean temporary install directory (we'll use tmp in this example).

For SPARC systems:

- Download the `endsunr.tar.Z` file to the `/tmp` directory.
- Uncompress the endpoint file by using the `uncompress` command:

```
cd /tmp
uncompress endsunr.tar
tar -xvf endsunr.tar
```

For x86 systems:

- Download the `ends86r.tar.Z` file to the `/tmp` directory.
- Uncompress the endpoint file by using the `uncompress` command:

```
cd /tmp
uncompress ends86r.tar
tar -xvf ends86r.tar
```

2 Next, install the endpoint package using the `pkgadd` command:

```
pkgadd -d /tmp endpoint
```

The `pkgadd` command is not part of the endpoint installation. It is part of the standard Solaris installation and can be found in the `/usr/bin` directory.

3 You will see the license agreement, presented with the `pg` command. Press the spacebar until the end of the agreement is displayed. You are asked whether you accept the terms and conditions of the agreement. If you do, enter `accept_license`.

4 You are next asked the following question:

```
This package contains scripts which will be executed with super user
permission during the process of installing this package. Do you want
to continue with the installation of this package [y,n,?]
```

Enter a lowercase "`y`" to complete the installation script. About 20 lines

of text give the status of the installation. When it's finished, the last line reads, "`Installation of <endpoint> was successful.`"

You may instead see the following message:

```
Notice! There were potential problems with migrating from
$oldInstallPath to $installPath. Review the warnings displayed above
for further explanation.
```

If you see this message, please review the entire output from the install script for an explanation of the warnings and further instructions.

5 Use the following commands to delete the archive contents from the temporary working directory:

```
cd /tmp
rm -fr endpoint
rm ends86r.tar
```

This is a good time to read the `README` file, installed with the endpoint in `/opt/NetIQ`, for the latest information about the endpoint program.

When you've completed installation, refer to "Configuring Solaris Endpoints" on page 19 to make sure your endpoint is ready to be used in monitoring.

Installation Defaults File for Solaris

The admin file defines default installation actions to be taken when administrative input is required during install, for example, whether to allow a new package to overwrite an older version, whether an installation can be run with super user authority, and so on. The admin file is found in `/var/sadm/install/admin/default`. The `man` pages ("`man -s 4 admin`") describe its format and content; please read the `man` pages if you are unfamiliar with the admin file.

To install version 5.1 of the Endpoint for Sun Solaris over a previous version of the endpoint, you need to modify the admin file to contain "`instance=overwrite`" and "`conflict=nocheck`."

If you want non-interactive install capability, modify the admin file to contain "`action=nocheck`" so that the endpoint package scripts can be run with super user authority.

Unattended Installation for Solaris

Unattended installation is available for the Sun Solaris endpoint. You install an endpoint once, manually, while the install facility saves your input in a response file. You can then install that same endpoint silently on other computers, that is, without providing input other than the response file.

First, complete the steps described in Installing the Endpoint for Sun Solaris using the `tar` command. Next create a response file, using the `pkgask` command:

```
pkgask -r /tmp/endpoint.response -d /tmp endpoint
```

The endpoint license agreement is displayed with the `pg` command. Press the spacebar until the end of the agreement is displayed. Next, you are asked whether you accept the terms and conditions of the agreement. If you do, enter `accept_license`.

You should see the following displayed:

```
Response file </tmp/endpoint.response> was created.
Processing of request script was successful.
```

Use the following command to install other Solaris endpoints in unattended mode (this single command is split over two lines):

```
pkgadd -n -a /tmp/endpoint/root/opt/NetIQ/admin
       -r /tmp/endpoint.response -d /tmp endpoint
```

The `pkgadd` command is not part of the endpoint installation. It is part of the standard Solaris installation and can be found in the `/usr/bin` directory.

When `pkgadd` is finished, the last line reads, "`Installation of <endpoint> was successful.`"

You may instead see the following message:

```
Notice! There were potential problems with migrating from
$oldInstallPath to $installPath. Review the warnings displayed above
for further explanation.
```

If you see this message, review the entire output from the install script for an explanation of the warnings and further instructions.

The response file may be used to install the endpoint on each of your Sun Solaris computers.

What Happens During Installation

Here's what happens during the installation steps. The endpoint is installed into the directory `/opt/NetIQ`. A directory is created with the following contents:

- The executable programs
- The `README` file
- Various install and uninstall programs
- The directory `cmpfiles`. This directory contains files with the `.cmp` file extension. These are files containing data of different types, such as typical text or binary data. These files are used by the endpoint as data on `SEND` commands. The different data types can be used to vary the data compression performance of your network hardware and software.
- The `endpoint.ini` file. See "Endpoint Initialization File" on page 5 for information about tailoring this file for individual endpoints.

The installation program stops any copy of the endpoint program that may currently be running and starts a copy of the newly installed endpoint. You can run tests immediately, without a reboot.

Our software copies an S81endpoint initialization script to the `/etc/rc2.d` directory so the endpoint is started every time your system boots.

No changes are made to the `PATH` environment variable of the root user.

Removing the Endpoint Package

Use the following command to remove the endpoint package (you must be logged in as root to run `pkgrm`):

```
pkgrm endpoint
```

Enter a lowercase "`y`" when you're asked if you want to remove this package. About 10 lines of text give the status of the uninstallation. When it's finished, the last line reads, "`Removal of <endpoint> was successful.`"

This removes the files from `/opt/NetIQ`, except for any files that were added to this directory that were not present at installation, such as the `endpoint.ini` file, and does not delete the directory. The removal program does not automatically delete files that have been added to the directory that you may need if you reinstall the product.

Configuring Solaris Endpoints

The endpoint dynamically configures its own programs, so you do not have to update the configuration files for your communications software. However, your communications software must be configured and running correctly. The following steps guide you through this verification.

1. Determine the network addresses of the computers to be used in tests.
2. Verify the network connections.

The following topics describe how to accomplish these tasks.

- "Configuration for TCP/IP" on page 20
- "Determining the IP Address" on page 20
- "Testing the TCP/IP Connection" on page 20
- "Sockets Port Number" on page 21

Configuration for TCP/IP

The RTP, TCP, and UDP protocols use TCP/IP software for network communications. TCP/IP offers two forms of network addresses: IP addresses and domain names. An IP address is a 32-bit numeric address. It is represented in dotted notation as a set of four numbers separated by periods, such as `199.72.46.202`. The alternative, domain names, are in a format that is easier to recognize and remember, such as www.netiq.com. To use domain names, you need either a Domain Name Server (DNS) set up in your network or an `/etc/hosts` file on each computer.

Determining the IP Address

Here are two ways to determine the IP address of the local computer you're using:

1. If you're using the Sun OpenWindows graphical user interface, right-click on the outer desktop background. One of the options in this **Workspace** menu that pops up is **Workstation Info**. Click on it to display Workstation Information about your computer, including your local Internet address.

2. As an alternative, enter the following at a command prompt:

   ```
   netstat -in
   ```

   Your local IP address is shown in the left-hand column, if there are active connections.

Testing the TCP/IP Connection

Ping is a simple utility program, included in all TCP/IP implementations. To check the connection from one computer to another, enter:

```
ping xx.xx.xx.xx
```

Replace the x's with the IP address of the target computer. If Ping returns a message that says "`xx.xx.xx.xx is alive`," the Ping worked.

Otherwise, there will be a delay, and then you'll see "`no answer from xx.xx.xx.xx`." This means that the Ping failed, and you can't reach the target computer.

Make sure that you can run Ping successfully from the AppManager, Vivinet Assessor, or Vivinet Diagnostics Console to each computer serving as Endpoint 1, and between each pair of endpoints involved in a test, before starting your testing with TCP/IP.

Sockets Port Number

TCP/IP applications use their network address to decide which computer to connect to in a network. They use a *Sockets port number* to decide which application program to connect to within a computer.

The TCP/IP sockets port for endpoints is `10115`. This port number is used during the initialization of a test; during the actual running of the test, other port numbers are used.

Running Solaris Endpoints

The following sections describe how to manually start and stop the endpoint program, and how to examine error log files if a problem occurs.

Starting a Solaris Endpoint

The endpoint program is installed so it will start automatically each time Solaris is rebooted. It sends its screen output to file `/var/adm/endpoint.console`. If you want to see any error messages generated at this endpoint, enter the following command:

```
tail -f /var/adm/endpoint.console
```

The detailed information about the start and stop of each individual connection pair is written to file `endpoint.aud`. The contents of this file vary depending on how you've set the `SECURITY_AUDITING` keyword in your `endpoint.ini` file.

See "Endpoint Initialization File" on page 5 for more information about `endpoint.aud` and `SECURITY_AUDIT` settings.

Instead of automatic startup, you can choose to manually start the endpoint program at a command prompt. Ensure that you are logged in as a "root" user. To start the endpoint, enter:

```
/opt/NetIQ/endpoint &
```

The "`&`" parameter indicates to Solaris that the endpoint program should run in the background. The screen output from the endpoint program is interleaved with other UNIX commands. Just press `Return` to enter more commands.

If you choose to manually start the endpoint, consider redirecting its output to the `endpoint.console` file. You can tell by the time stamp of the file when the endpoint program was started and stopped.

If the endpoint program is already running, you get the following message, "`CHR0183: The endpoint program is already running. Only one copy is allowed at a time.`"

Stopping a Solaris Endpoint

The endpoint program has a special command-line option, `-k`. If you have an endpoint program you'd like to stop, go to a command prompt on the same computer and enter the following (you must be logged in as root to run this program):

```
/opt/NetIQ/endpoint -k
```

The `-k` command-line option has the purpose of stopping any endpoint program running on that computer. You should see the message "`Sent exit request to the running endpoint`," which indicates that the endpoint program has been sent a request to stop.

If for some reason the request to stop is not handled by the running endpoint program correctly, you may need to use the UNIX `kill -TERM` command.

Cleanup after Unexpected Errors

If the endpoint should fail or stop abnormally (or encounter assertion conditions), you may need to do additional cleanup. If the endpoint is still running, try to stop it using the command `endpoint -k`. If that does not stop the endpoint, stop it using the UNIX `KILL` command.

Next, enter the following command:

```
rm /var/adm/.NETIQ.ENDPOINT.PID
```

How to Tell If a Solaris Endpoint Is Active

You can use traditional UNIX commands to determine whether the endpoint program is active. At a command prompt, enter:

```
ps -ef | grep endpoint
```

If the endpoint program is running, it shows up with the following string in the rightmost column of the output, "`/opt/NetIQ/endpoint`."

Disabling Automatic Startup

To disable automatic startup, remove the `/etc/rc2.d/S81` endpoint file.

Logging and Messages

Although most error messages encountered on an endpoint are returned to the AppManager, Vivinet Assessor, or Vivinet Diagnostics Console, some may be logged to disk. Errors are saved in a file named `endpoint.log`, in the `/var/adm` directory. To view an error log, use the NetIQ program named `FMTLOG`. `FMTLOG` reads from a binary log file, and writes its formatted output to `stdout`. Use the following `FMTLOG` command:

```
/opt/NetIQ/fmtlog log_filename >output_filename
```

The endpoint code does a lot of internal checking on itself. Our software captures details related to the problem in an ASCII text file named `assert.err` in the `/var/adm` directory. Save a copy of the file and send it to us via email for problem determination.

Message CHR0181 You may receive message **CHR0181** while running a test. If the error was detected at the Sun Solaris computer, it says that the endpoint program on Sun Solaris has run out of system semaphores. Each instance of Endpoint 1 requires a system semaphore. The maximum number of semaphores is not configurable on Sun Solaris; it is hard-coded to a large value. To avoid this problem, stop other programs that use semaphores or decrease the number of tests that use the computer as Endpoint 1.

Updates for Sun Solaris

We've found that communications software is often fragile. Its developers are constantly working to make it more robust, as the software gets used in an ever-wider set of situations.

We therefore recommend working with the very latest software for the underlying operating system and communications software.

Sun posts code and driver updates directly to the following Web sites:

- www.sun.com/
- Anonymous FTP to ftp://ftp.sun.com/

Index

U