Performance Endpoints 5.1

Linux

April 2006

Legal Notice

Contents

Index

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, "Linux," explains the installation, configuration, and operation of the Performance Endpoint software for Linux.

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 67 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 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

Linux

This chapter explains the installation, configuration, and operation of the Performance Endpoint software for Linux.

We have concentrated our testing on the most popular Linux operating systems. The Performance Endpoint software requires kernel 2.0 with threading support. Our Linux endpoints run on the following Linux platforms:

- Red Hat Linux (version 6.1 and later ships with a current version of the Performance Endpoint) for x86 processors
- Slackware Version 2.0 and later (x86 processors)
- Cobalt Web Server RaQ 3 (x86 processors)
- Other Linux systems that incorporate the Linux 2.0 kernel (or later) with threading support on x86 processors. This includes Caldera Systems, for example.

If you are using a Linux system other than Red Hat or the Cobalt Web Server, use the instructions listed for TAR-based (Slackware) installation and operation.

The following topics installation and configuration instructions for the supported Linux configurations:

Installation Requirements for Linux Endpoints

Here is what you need to run the endpoint program with Linux:

- A computer capable of running Linux well.

- For Cobalt servers, the RaQ 3 system, which uses an Intel x86 processor, 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.

- 16 MBytes of random access memory (RAM).

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

- A hard disk with at least 8 MBytes of space available

- Linux kernel 2.0 with "pthreads support" (which is at least version 2.0.6 of glibc). TCP/IP networking and corresponding networking hardware must be installed and configured, plus ELF support. Some older installations of Linux may not have this installed. At the Web site www.linuxdoc.org/HOWTO/Glibc2-HOWTO.html, you can find information about Linux, as well as download the file glibc-2.0, which you need to have loaded to install the endpoint. We have

changed our installation procedures to check for this file, as it is required to run the endpoint.

We have tested with Red Hat (kernel 2.0.32). Red Hat 5.0 or higher is required for IP Multicast. Red Hat 8.0 or higher is required for IPv6. We have also tested with Slackware 3.6.

- 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

For Linux endpoints, there are three types of installation procedures. The basic procedure uses TAR files, which should be used for Slackware and Linux systems other than Red Hat or Cobalt. These systems have made changes to application installations that are described in later sections of this guide.

Installing the RPM-Based Endpoint for Linux

Use the RPM-based (x86 processor) installation if you are installing the endpoint on Red Hat Linux. 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

Installing from a CD-ROM

First, ensure that you are logged in as a "root" user. Also, remember that all commands and parameters discussed here are case-sensitive. Use the combination of uppercase and lowercase letters as shown in the following procedure.

To install the endpoint from a CD-ROM:

1 Put the CD-ROM in your CD-ROM drive.

2 Enter the following commands, assuming your CD-ROM drive device name is /dev/cdrom and you are able to create a temporary directory named cdrom:

```
mkdir /cdrom
mount /dev/cdrom /cdrom
```

3 Copy the endlnxr.rpm file from the CD-ROM to a local directory (like tmp, for example).

```
cp /cdrom/endpoint/linux/endlnxr.rpm /tmp
```

4 Use the RPM command to install the endpoint:

```
rpm -Uvh /tmp/endlnxr.rpm
```

During installation, you will see several status messages. Pay close attention to the output. When the installation is successful, you see the message "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 After the installation is complete, use the UMOUNT command to unmount the file system from the CD-ROM.

```
umount /cdrom
```

This is a good time to read the README file, installed with the endpoint in /usr/local/NetIQ, for the latest information about the endpoint program. Enter the more command to view the README file:

```
more /usr/local/NetIQ/README
```

When you've completed installation, refer to "Configuring Linux Endpoints" on page 25 to make sure your endpoint is ready to be used in testing and monitoring.

Installing from the Web

First, ensure that you are logged in as a "root" user. Also, remember that all commands and parameters discussed here are case-sensitive. Use the combination of uppercase and lowercase letters as shown in the following procedure.

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).

2   Save the `endlnxr.rpm` file to the `/tmp` directory.

3   Use the `RPM` command to install the endpoint:

```
cd /tmp
rpm -Uvh endlnxr.rpm
```

During installation, you will see several status messages. Pay close attention to the output. When the installation is successful, you see the message "`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.

This is a good time to read the `README` file, installed with the endpoint in `/usr/local/NetIQ`, for the latest information about the endpoint program. Enter the `more` command to view the `README` file:

```
more /usr/local/NetIQ/README
```

When you've completed installation, refer to to make sure your endpoint is ready to be used in testing and monitoring.

Removing the RPM Endpoint Package

Use the following command to remove the endpoint (you must be logged in as root to run this program):

```
rpm -e endpoint
```

If the removal is successful, you will see the following: "`Removal of endpoint was successful.`" This removes the files from `/usr/local/NetIQ`, except for any files that were added to this directory that were not present at installation, such as the `endpoint.ini` file. This command does not delete the directory. The remove program does not automatically delete files added to the directory that you may need if you reinstall the product.

If anything goes wrong during the process of uninstalling the endpoint, a reinstalled endpoint may not run. You may need to do some extra cleanup. Check for the hidden file `/usr/local/NetIQ/.NETIQ.ENDPOINT.PID`. You can use the command `ls -a` to view hidden files. Then enter the following command to delete it:

```
rm /usr/local/NetIQ/.NETIQ.ENDPOINT.PID
```

Installing the Cobalt-Based Endpoint for Linux

Use the Cobalt installation if you are installing the endpoint for x86 (RaQ 3) on a Cobalt Web server. There are some prerequisite levels of Cobalt software that are needed to operate the Performance Endpoint on a Cobalt Web server.

Typically, when you install an endpoint, you can automatically upgrade from the previous version of the endpoint. However, when you're upgrading the endpoint on a Cobalt RaQ 3 (x86) computer, you must first remove the previous version of the endpoint, following the directions in "Removing the Cobalt Endpoint Package" on page 19. Then install the new version of the endpoint.

If you attempt to install Endpoint 5.1 without first removing a previous version, you get a message stating, "`Error uninstalling RPM.`" This means that the upgrade failed.

Following are instruction for installing the endpoint from a CD-ROM and from the Internet.

Installing from a CD-ROM

The following instructions are for installing on the Cobalt Web server (x86 processors) from a Web browser running on a Linux computer. You can, however, install the endpoint from computers running other platforms. In these cases, proceed with the following instructions, but do not mount the CD-ROM.

To install the endpoint from a CD-ROM:

1 Put the CD-ROM in your CD-ROM drive.

2 Enter the following commands, assuming your CD-ROM drive device name is /dev/cdrom and you are able to create a temporary directory named cdrom:

```
mkdir /cdrom
mount /dev/cdrom /cdrom
```

3 Access the "Welcome to Cobalt" page on the Cobalt Web Server and click on the link to the **RaQ Server Management** section. The Username and Password Required dialog box is displayed.

4 Enter the **username** and **password** for Administrator.

5 Click **Maintenance** on the Server Management dialog box and then click **Install Software**.

6 In the **Software to install** field, enter the location of the package. If you are using the Browse function, make sure that the filename and extension are in lowercase.

```
/cdrom/endpoint/linux/endcbl3.pkg
```

7 If prompted, enter the password for Administrator. Click **Install a '.pkg' package**. After the endpoint is installed, a message stating that

the endpoint has been installed is shown. If you do not get this message, please go to the server management panel and browse the box labeled "Software on the Cobalt Server." This contains a list of products installed on the Cobalt computer. You should see a line that reads, "`Performance Endpoint X.X`," where `X.X` is the release number of the Performance Endpoint.

8 After the installation is complete, use the `UMOUNT` command to unmount the file system from the CD-ROM:

`umount/cdrom`

The installation script and temporary directory are not removed automatically if the installation is successful. If you need the disk space after installing the endpoint, you may delete the temporary directory and installation script.

This is a good time to read the `README` file, installed with the endpoint in `/usr/local/NetIQ/`, for the latest information about the endpoint program. Enter the `more` command to view the `README` file:

`more /usr/local/NetIQ/README`

When you've completed installation, refer to to make sure your endpoint is ready to be used in testing and monitoring.

Installing from the Web

Installing 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).

2 Save the file appropriate for your operating system to the `/tmp` directory.

3 Access the "Welcome to Cobalt" page on the Cobalt Web Server and click on the link to the **RaQ Server Management** section. The Username and Password Required dialog box is displayed.

4 Enter the **username** and **password** for Administrator.

5 Click **Maintenance** on the Server Management dialog box and then click **Install Software**.

6 In the **Software to install** field, enter the location of the package. If you are using the Browse function, make sure that the filename and extension are in lowercase.

`/tmp/endcbl3.pkg`

7 If prompted, enter the password for Administrator. Click **Install a '.pkg' package**. After the endpoint is installed, a message stating that the endpoint has been installed is shown. If you do not get this message, go to the server management panel and browse the box labeled "Software on the Cobalt Server." This contains a list of products installed on the Cobalt computer. You should see a line that reads, "`Performance Endpoint X.X`," where `X.X` is the release number of the Performance Endpoint software.

When you've completed installation, refer to "Configuring Linux Endpoints" on page 25 to make sure your endpoint is ready to be used in testing and monitoring.

Removing the Cobalt Endpoint Package

You must be logged in as the root user to remove the endpoint package. Do not use the `RPM` command to remove the Cobalt endpoint. First, stop the endpoint program (if it's running).

Next, enter the following command at a command prompt:

`/bin/sh /var/lib/cobalt/uninstallers/endpoint-5.1.uninst`

Note The actual command depends on the version of the endpoint installed. If you have a different version installed, for instance version 5.0, run the `endpoint-5.0.uninst` command instead.

After the script removing the endpoint package has completed, enter the following command:

`/usr/admserv/cgi-bin/.cobalt/install/install.cgi`

At the prompt, press the [Ctrl] + [D] keys. The endpoint has been removed.

If anything goes wrong during the process of uninstalling the endpoint, a reinstalled endpoint may not run. You may need to do some extra cleanup. Check for the hidden file /usr/local/NetIQ/ .NETIQ.ENDPOINT.PID by using the ls -a command. Enter the following:

```
rm /usr/local/NetIQ/.NETIQ.ENDPOINT.PID
```

Installing the TAR-Based Endpoint for Linux

Use the TAR-based installation if you are installing the endpoint on any x86 Linux platform other than Red Hat or Cobalt RaQ 3 Web Server.

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

- "Installing from a CD-ROM" on page 20
- "Installing from the Web" on page 22
- "Unattended Installation for TAR-Based Linux" on page 23

Installing from a CD-ROM

To install the endpoint from a CD-ROM:

1 Put the CD-ROM in your CD-ROM drive.

2 Enter the following commands, assuming your CD-ROM drive device name is /dev/cdrom and you are able to create a temporary directory named cdrom:

```
mkdir /cdrom
mount /dev/cdrom /cdrom
```

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:

```
cd /tmp
rm -fr temp
tar -xvf /cdrom/endpoint/linux/endlnxr.tar
```

4 Next, run the endpoint installation script to install the endpoint:

```
./endpoint.install
```

5 You will see the license agreement, presented with the `more` 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`.

The endpoint installs itself in `/usr/local/NetIQ`. During installation you will see several status messages. When the installation is successful, you see the message "`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.

6 After the installation is complete, use the `UMOUNT` command to unmount the file system from the CD-ROM:

```
umount /cdrom
```

The installation script and temporary directory are not removed automatically if the installation is successful. If you need the disk space after installing the endpoint, you may delete the temporary directory and installation script.

To remove the temp files, enter:

```
rm -fr temp
rm endpoint.install
```

This is a good time to read the README file, installed with the endpoint in /usr/local/NetIQ, for the latest information about the endpoint program. Enter the more command to view the README file:

```
more /usr/local/NetIQ/README
```

When you've completed installation, refer to "Configuring Linux Endpoints" on page 25 to make sure your endpoint is ready to be used in testing and 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).

2 Save the endpoint to the /tmp directory.

3 Uncompress the endpoint by using the uncompress command:

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

4 From the directory where you've downloaded the endpoint, run the endpoint's installation script:

```
./endpoint.install
```

The endpoint installs itself in /usr/local/NetIQ. During installation, you will see several status messages. When the installation is successful, you see the message "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.

The installation script and temporary directory are not removed automatically if the installation is successful. If you need the disk space after installing the endpoint, you may delete the temporary directory and installation script.

To remove the temp files, enter:

```
rm -fr temp
rm endpoint.install
```

This is a good time to read the README file, installed with the endpoint in /usr/local/NetIQ, for the latest information about the endpoint program. Enter the more command to view the README file:

```
more /usr/local/NetIQ/README
```

When you've completed installation, refer to "Configuring Linux Endpoints" on page 25 to make sure your endpoint is ready to be used in testing and monitoring.

Unattended Installation for TAR-Based Linux

You can install the endpoint silently, that is, without providing any additional user input.

Complete the steps, as described in "Installing the TAR-Based Endpoint for Linux" on page 20, through the tar command. Next, run the endpoint installation, adding the accept_license parameter:

```
./endpoint.install accept_license
```

Removing the TAR-Based Endpoint Package

Use the following command to remove the TAR-based (x86) Linux endpoint (you must be logged in as root to run this program):

```
/usr/local/NetIQ/endpoint.remove
```

If the removal is successful, you will see the following message: "`Removal of endpoint was successful.`" This removes the files from `/usr/local/NetIQ`, except for any files that were added to this directory that were not present at installation, such as the `endpoint.ini` file. This command does not delete the directory. The remove program does not automatically delete files added to the directory that you may need if you reinstall the product.

If anything goes wrong during the process of uninstalling the endpoint, a reinstalled endpoint may not run. You may need to do some extra cleanup. Check for the hidden file `/var/local/NetIQ/.NETIQ.ENDPOINT.PID` by using the `ls -a` command. This file should be manually removed. Enter the following command:

```
rm /var/local/NetIQ/.NETIQ.ENDPOINT.PID
```

What Happens During Installation

Here is what happens during the installation steps. The endpoint is installed into the directory `/usr/local/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 currently running and starts a copy of the newly installed endpoint. You can run tests immediately, without restarting your computer.

Our software displays information on how to update your system to have the endpoint start automatically upon restarting.

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

Configuring Linux 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. Take the following steps to verify that your network is ready for testing and/or monitoring:

1 Determine the network addresses of the computers for use in tests.

2 Verify the network connections.

See the following topics for details about accomplishing these tasks.

- "Configuration for TCP/IP" on page 26
- "Determining the IP Address for TAR and RPM Linux" on page 26
- "Determining the IP Address for Cobalt" on page 26
- "Testing the TCP Connection" on page 26
- "Sockets Port Number" on page 27

Configuration for TCP/IP

The 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 for TAR and RPM Linux

To determine the IP address of the local computer you are using, enter the following at a command prompt:

```
/sbin/ifconfig
```

Determining the IP Address for Cobalt

Access the Welcome to Cobalt page on the Cobalt Web Server and click the link to the **RAQ Server Management** section. The Username and Password Required dialog box is displayed.

After you enter the Administrator username and password, the IP address is shown on the Server Management Page.

Testing the TCP Connection

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

```
ping xx.xx.xx.xx -c 1
```

Replace the x's with the IP address of the target computer. If Ping returns a message that says

```
1 packets transmitted, 1 packets received, 0% packet loss
```

then the Ping worked. Otherwise, there will be a delay, and you'll see

```
1 packets transmitted, 0 packets received, 100% packet loss
```

This means that the Ping failed, and you cannot 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 Linux 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 Linux Endpoint

The endpoint program is installed so that it starts automatically each time Linux is rebooted.

- On Slackware, it sends its screen output to the `/var/adm/endpoint.console` file.

- On Red Hat and Cobalt, it sends its screen output to the `/var/local/endpoint.console` file.

If you want to see any error messages generated at this endpoint, enter one of the following:

for Slackware:

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

for Red Hat or Cobalt:

```
tail -f /var/local/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 the following:

```
/usr/local/NetIQ/endpoint &
```

The "&" parameter indicates to Linux 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 or stopped.

If the endpoint program is already running, you get the following message, "`CHRO183: The endpoint program is already running. Only one copy is allowed at a time.`"

Use the `ps` command to check all running processes and make sure the endpoint is running (see "How to Tell If a Linux Endpoint Is Active" on page 30 for more information). If you repeatedly get error message **CHR0183** but it appears that the endpoint is not running, you may need to do some extra cleanup. Check for the hidden file `/usr/local/NetIQ/NETIQ.ENDPOINT.PID` by using the `ls -a` command. This file should be manually removed.

Stopping a Linux Endpoint

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

```
/usr/local/NetIQ/endpoint -k
```

The `-k` command-line option has the purpose of stopping any endpoint process 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 correctly by the running endpoint program, you may need to use the UNIX `kill -TERM` command. Avoid using `kill -9` to stop the running endpoint program — it doesn't clean up what's been created (so you'll need to do the steps outlined in Cleanup after Unexpected Errors).

Cleanup after Unexpected Errors

If the endpoint should fail or stop abnormally (or encounter assertion conditions), you may also 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 the endpoint using the UNIX `kill` command.

Then enter the following command:

```
rm /usr/local/NetIQ/.NETIQ.ENDPOINT.PID
```

How to Tell If a Linux Endpoint Is Active

Use traditional UNIX commands to determine whether a Linux endpoint is active. At a command prompt, enter:

```
ps axf | grep endpoint
```

If the endpoint program is running, you will see output similar to this:

```
366 p0 S 0:00  \_ /usr/local/NetIQ/endpoint
367 p0 S 0:00  |      \_ /usr/local/NetIQ/endpoint
368 p0 S 0:00  |              \_/usr/local/NetIQ/endpoint
369 p0 S 0:00  |              \_ /usr/local/NetIQ/endpoint
```

Autostarting the Endpoint

For the endpoint to automatically start when your computer restarts, you must update your system `rc` scripts.

If your Linux system uses `rc.local`, which is used by older Linux systems, such as Slackware, add the following line to the `rc.local` file:

```
/usr/local/NetIQ/endpoint 1>>/var/local/endpoint.console 2>&1 &
```

Don't forget the ampersand (&) at the end of the line. If this character is not included, the boot process does not continue, and you may be unable to log in at the Console.

If you have previously installed the endpoint in a `Ganymede` directory, the install script displays the following message:

```
The endpoint install directory now uses $installPath instead of
```

```
$oldInstallPath. If your rc.local referenced $oldInstallPath, you
should change it to use the new directory.
```

If your Linux system is more recent, it probably supports System V init rc scripts. Red Hat software uses this type of init rc files. Copy usr/local/NetIQ/rc2exec.lnx to the appropriate places. For example, with Red Hat Linux 5.0, you may run these commands:

```
cp /usr/local/NetIQ/rc2exec.lnx /etc/rc.d/init.d/endpoint

ln -fs /etc/rc.d/init.d/endpoint /etc/rc.d/rc2.d/S81endpoint

ln -fs /etc/rc.d/init.d/endpoint /etc/rc.d/rc3.d/S81endpoint

ln -fs /etc/rc.d/init.d/endpoint /etc/rc.d/rc6.d/K81endpoint
```

For Red Hat Linux 5.2 or later, or for Cobalt, the recommended commands are the following:

```
cp /usr/local/NetIQ/rc2exec.lnx /etc/rc.d/init.d/endpoint

/sbin/chkconfig endpoint reset
```

Disabling Automatic Startup

If you run a Linux system that uses rc.local to invoke applications, remove the invocation of /usr/local/NetIQ/endpoint from /etc/rc.d/rc.local.

If you use a Linux system that supports System V init rc scripts, remove /etc/rc.d/rc2.d/S81endpoint from /etc/rc.d/rc2.d.

If you are using Red Hat Linux versions 5.2 or later, or Cobalt Web server, and have enabled automatic startup through the CHKCONFIG utility, you can also disable automatic startup through the CHKCONFIG utility. Here is the syntax to use the CHKCONFIG utility to disable the automatic startup:

```
/sbin/chkconfig -del endpoint
```

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 the following file:

- On Slackware, file `/var/adm/endpoint.log`

- On Red Hat or Cobalt, file `/var/local/endpoint.log`

To view an error log, use the program named `FMTLOG`. `FMTLOG` reads from a binary log file, and writes its formatted output to `stdout`. Use the following `FMTLOG` command(s):

    /usr/local/NetIQ/fmtlog /var/adm/endpoint.log >output_filename

or

    /usr/local/NetIQ/fmtlog /var/local/endpoint.log >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:

- On Slackware, file `/var/adm/assert.err`

- On Red Hat or Cobalt, file `/var/local/assert.err`

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 Linux computer, it says that the endpoint program on Linux has run out of system semaphores. Each instance of Endpoint 1 requires a system semaphore. The maximum number of semaphores is not configurable on Linux, which is hard-coded to a large value (128). To avoid this problem, stop other programs that use semaphores or decrease the number of tests that use the computer as Endpoint 1.

Increasing the Number of Concurrent Connections

Some parameters are tuned in Linux by rebuilding the Linux kernel. If you're adventurous and skilled enough, you can change the number of concurrent endpoint connections. Consult your Linux documentation for information about increasing the maximum open files allowed per process (this probably involves redefining `NR_FILES` and other macros). Alternatively, search Linux newsgroups on the Internet (using DejaNews, for example) for something like "`max open files per process.`"

Updates for Linux

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.

Check the following Web sites for code and driver updates:

- www.redhat.com/
- for Cobalt, wwws.sun.com/software/linux/index.html
- www.slackware.com/
- www.calderasystems.com/
- www.linux.org/
- www.ibiblio.org/

We've found the following site good for ordering Linux software: www.linuxmall.com/

Index

P

S

U

uninstall