

Performance Endpoints 5.1

IBM AIX

April 2006



Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 1995-2006 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, Provider-1, SiteManager-1, and VPN-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, AppAnalyzer, AppManager, ConfigurationManager, the cube logo design, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Knowing is Everything, Knowledge Scripts, MailMarshal, Marshal, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, NetIQ Change Guardian, NetIQ Firecall Administrator, NetIQ Firewall Suite, NetIQ Group Policy Administrator, NetIQ Group Policy Guardian, the NetIQ Partner Network design, Patch Manager, NetIQ Security Analyzer, NetIQ Security Manager, NetIQ Security Reporting Center, NetIQ Vulnerability Manager, WebMarshal, PSAudit, PSDetect, PSPasswordManager, PSSecure, RecoveryManager, Server Consolidator, SQLcheck, VigilEnt, Vivinet, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Contents

About This Guide

| | |
|--|-----|
| Intended Audience | iii |
| Using This Guide | iii |
| Conventions Used in this Guide | iv |
| Complementary NetIQ Products | iv |
| Contacting NetIQ | v |

Chapter 1 Introduction to Performance Endpoints

| | |
|---|---|
| Operating System and Protocol Stack Support | 2 |
| Endpoint Capabilities | 2 |

Chapter 2 Endpoint Initialization File

| | |
|---|---|
| ALLOW | 6 |
| SECURITY_AUDITING | 7 |
| AUDIT_FILENAME | 7 |
| ENABLE_PROTOCOL | 8 |
| Configuring Endpoints for Large-Scale Customization | 9 |

Chapter 3 IBM AIX

| | |
|---|----|
| Installation Requirements for AIX Endpoints | 11 |
| Installing the Endpoint for AIX | 12 |
| Installation from CD | 12 |
| Installation from the Web | 14 |
| Unattended Installation for AIX | 15 |

| | |
|--|----|
| What Happens During Installation | 16 |
| Removing the Endpoint Package | 16 |
| Configuring AIX Endpoints | 17 |
| Configuration for TCP/IP | 17 |
| Determining the IP Address | 18 |
| Testing the TCP/IP Connection | 18 |
| Sockets Port Number | 19 |
| Running AIX Endpoints | 19 |
| Starting an AIX Endpoint | 19 |
| Stopping an AIX Endpoint | 20 |
| Cleanup after Unexpected Errors | 21 |
| How to Tell If an AIX Endpoint Is Active | 21 |
| Disabling Automatic Startup | 21 |
| Logging and Messages | 22 |
| Updates for AIX | 22 |

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, “IBM AIX,” explains the installation, configuration, and operation of the Performance Endpoint software for IBM AIX on the RISC System/6000 (RS/6000).

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

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 contains 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 |

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:

| | |
|-----------------------|---|
| <code>NONE</code> | Writes nothing to the audit file |
| <code>PASSED</code> | Logs only access attempts that passed the <code>ALLOW</code> address check. |
| <code>REJECTED</code> | Logs only access attempts that failed the <code>ALLOW</code> address check. |
| <code>ALL</code> | 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 [“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** 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.

IBM AIX

This chapter explains the installation, configuration, and operation of the Performance Endpoint software for IBM AIX on the RISC System/6000 (RS/6000).

- [“Installation Requirements for AIX Endpoints”](#) on page 11
- [“Installing the Endpoint for AIX”](#) on page 12
- [“Removing the Endpoint Package”](#) on page 16
- [“Configuring AIX Endpoints”](#) on page 17
- [“Running AIX Endpoints”](#) on page 19
- [“Logging and Messages”](#) on page 22
- [“Updates for AIX”](#) on page 22

Installation Requirements for AIX Endpoints

Here’s what you need to run the endpoint program with AIX:

- An IBM RS/6000 computer capable of running AIX.
- 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. Large tests involving hundreds of connections through a single endpoint may require additional memory.

- A hard disk with at least 4 MBytes of space available.
- AIX version 4.1 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 AIX

The following topics walk you through the process of installing the endpoint for IBM AIX:

- “Installation from CD” on page 12
- “Installation from the Web” on page 14
- “Unattended Installation for AIX” on page 15
- “What Happens During Installation” on page 16

Installation from CD

First, ensure 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.

To install the endpoint from a CD-ROM:

- 1 Put the endpoint CD-ROM in your CD-ROM drive.
- 2 Enter the following commands, assuming your CD-ROM drive device name is cd0 and you’re able to create a temporary directory named cdrom:

```
mkdi r /cdrom  
mount -v cdrfs -r /dev/cd0 /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/ai x/endai xr. tar
```

- 4 Next, run the endpoint's installation script to install our software:

```
./endpoint. install
```

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

The endpoint installs itself in `/usr/lib/NetIQ`. During installation, you will see several status messages. Pay close attention to the output. If 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 unmount command to unmount the file system from the CD-ROM:

```
umount /cdrom
```

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

To remove the temp files, enter:

```
rm -fr temp
rm endpoint.install
rm endai xr. tar
```

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

```
more /usr/lpp/NetIQ/README
```

See [“Configuring AIX Endpoints” on page 17](#) for information about your network connections.

If all connections are in order, you’re ready to use this endpoint in testing and monitoring.

Installation from the Web

First, ensure 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.

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

- 1 First, use the `rm` command to ensure a clean temporary install directory. Then save the endpoint to that directory (we’ll use `/tmp` in this example).
- 2 Download the `endai.xr.tar.Z` file to the `/tmp` directory.
- 3 Uncompress the endpoint file by using the `uncompress` command:

```
cd /tmp
uncompress endai.xr.tar
tar -xvf endai.xr.tar
```
- 4 From the directory where you’ve downloaded the endpoint, run the endpoint’s installation script to install our software:

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

The endpoint installs itself in `/usr/lpp/NetIQ`. During installation, you will see several status messages. Pay close attention to the output. If 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.

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

To remove the temp files, enter:

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

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

```
more /usr/lpp/NetIQ/README
```

See [“Configuring AIX Endpoints” on page 17](#) for information about your network connections.

If all connections are in order, you’re ready to use this endpoint in testing and monitoring.

Unattended Installation for AIX

Unattended installation is available for the AIX endpoint. You can install the endpoint silently, that is, without providing any additional user input.

Complete the steps, as described in [“Installing the Endpoint for AIX” on page 12](#) through the tar command. Next, run the endpoint installation, adding the accept_license parameter:

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

What Happens During Installation

Here's 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.
- 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.
- File `endpoint.ini`. 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 does the following so the endpoint is started every time your system boots:

- Copies the `rc.netiq` initialization script to the `/etc` directory.
- Updates `/etc/inittab` to invoke `/etc/rc.netiq`

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 (you must be logged in as root to run this program):

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

If the removal is successful, you see the following: “Removal of endpoint was successful.”

This removes the files from `/usr/lib/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 `remove` program does not automatically delete files that have been added to the directory that you may need if you reinstall the product.

Configuring AIX 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.

See the following topics for details about accomplishing these tasks.

- [“Configuration for TCP/IP” on page 17](#)
- [“Determining the IP Address” on page 18](#)
- [“Testing the TCP/IP Connection” on page 18](#)
- [“Sockets Port Number” on page 19](#)

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:

- If you're using IBM System Management Interface Tool (SMIT), first open the **Communications Applications and Services** menu, then the **TCP/IP** menu, and then the **Minimum Configuration & Startup** menu. Next, select the network interface used to reach other endpoints (for example, en0 or tr0). SMIT displays the network interface's configuration; your host's IP address is in the **Internet ADDRESS** field.
- Alternatively, enter the following at a command prompt:

```
netstat -in
```

You may have several network interfaces. If you are using a LAN network, for example, look at the output for the en0 interface; your local IP address is shown in the "Address" column.

Testing the TCP/IP Connection

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

```
ping xx.xx.xx.xx 64 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," the Ping worked. Otherwise, there will be a delay, and then you'll see the following:

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

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 Operator 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 AIX 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 an AIX Endpoint” on page 19](#)
- [“Stopping an AIX Endpoint” on page 20](#)
- [“Cleanup after Unexpected Errors” on page 21](#)
- [“How to Tell If an AIX Endpoint Is Active” on page 21](#)
- [“Disabling Automatic Startup” on page 21](#)

Starting an AIX Endpoint

The endpoint program is installed so that it starts automatically each time AIX 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 the following:

```
/usr/lpp/NetIQ/endpoint &
```

The “&” parameter indicates to AIX 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 an AIX 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):

```
/usr/lpp/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 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 be stopped 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 `endpoi nt -k`. If that does not stop the endpoint, stop the endpoint using the UNIX `ki ll` command.

Next, enter the following command:

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

How to Tell If an AIX 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 endpoi nt
```

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

```
root 9888 1 0 19:19:54 - 0:00 /usr/lpp/NetIQ/endpoi nt -G 7477 -T 3
root 7477 1 0 18:37:47 - 0:00 /usr/lpp/NetIQ/endpoi nt
```

Disabling Automatic Startup

To disable automatic startup, comment out or remove the following lines from the `/etc/rc.netiq` script:

```
if test -f $instal lPath/endpoi nt; then
echo "Starting the NetIQ Endpoint."
$instal lPath/endpoi nt 1>$outputPath/endpoi nt console 2>&1 &
fi
```

Logging and Messages

Although most error messages encountered on an endpoint are returned to the AppManager Operator 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 program named `FMTLOG`. `FMTLOG` reads from a binary log file, and writes its formatted output to `stdout`. Use the following `FMTLOG` command:

```
/usr/lpp/NetIQ/fmtlog /var/adm/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 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 AIX computer, it says that the endpoint program on AIX has run out of system semaphores. Each instance of Endpoint 1 requires a system semaphore. The maximum number of semaphores is not configurable on AIX; it is hard-coded to a large value (4096). To avoid this problem, stop other programs that use semaphores, or decrease the number of connection pairs that use the AIX computer as Endpoint 1.

Updates for AIX

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 site for code and driver updates:

www-03.ibm.com/servers/eserver/support/unixservers/othermodels/downloadingwaix.html

Index

A

ALLOW 6
AUDIT_FILENAME 7

C

CHR0181
 IBM AIX 22
CHR0183
 IBM AIX 20
CMPFILES directory
 AIX 16
conventions, documentation iv

D

documentation, conventions iv

E

ENABLE_PROTOCOL 8
endpoint
 capabilities 2
 initialization file 5
 installing IBM AIX 12, 14
 removing IBM AIX 16
 running IBM AIX 19
endpoint.aud
 description 7
 IBM AIX 19
endpoint.console
 IBM AIX 19
endpoint.ini
 ALLOW 6

AUDIT_FILENAME 7
ENABLE_PROTOCOL 8
IBM AIX 16, 19
keywords 5
SECURITY_AUDITING 7

endpoint.log
 IBM AIX 22
error messages
 IBM AIX 22

G

gsendw32.exe 9

I

IBM AIX endpoint 11
 CHR0181 22
 CHR0183 20
 configuring 17
 determining IP address 18
 disabling auto startup 21
 error cleanup 21
 error messages 22
 installation requirements 11
 installing 12, 14
 is it active? 21
 removing 16
 running 19
 SMIT 18
 sockets port number 19
 starting 19
 stopping 20

- TCP/IP configuration 17
- unattended installation 15
- installation requirements
 - IBM AIX endpoint 11

K

- keyword
 - ALLOW 6
 - AUDIT_FILENAME 7
 - ENABLE_PROTOCOL 8
 - SECURITY_AUDITING 7

P

- protocol support 2

S

- SECURITY_AUDITING 7
- silent installation
 - IBM AIX 15
- SMIT 18
- software requirements 2

U

- uninstall
 - IBM AIX 16