



Avaya VisAbility™ Management Suite
Release 1.3
Configuring Red Hat Linux

555-233-152
Issue 2
May 2003

**Copyright 2003, Avaya Inc.
All Rights Reserved, Printed in U.S.A.**

Notice

Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following website:

<http://www.avaya.com/support>

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or working on your company's behalf). Be aware that there is a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you *suspect that you are being victimized* by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help

For additional support telephone numbers, go to the Avaya Web site:

<http://www.avaya.com/support/>

If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional Centers of Excellence.

Providing Telecommunications Security

Telecommunications security of voice, data, and/or video communications is the prevention of any type of intrusion to, that is, either unauthorized or malicious access to or use of, your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or working on your company's behalf. Whereas, a "malicious party" is Anyone, including someone who may be otherwise authorized, who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company, including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you – an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure your:

- Avaya provided telecommunications systems and their interfaces
- Avaya provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

To order copies of this and other documents

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
Fax 1.800.457.1764 or 1.207.626.7269

Write: GlobalWare Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

Email: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya Web site:

<http://www.avaya.com/support/>

Table of Contents

| | |
|---|----------|
| Chapter 1 — Welcome | 3 |
| Purpose | 3 |
| Prerequisites | 3 |
| Intended Audience | 3 |
| Conventions Used in This Book | 3 |
| Additional Resources | 4 |
| Tell Us What You Think! | 4 |
| How to Get This Book (and Others) on the Web | 5 |
| How to Order More Copies of This Book | 6 |
| Chapter 2 — Linux Server Installation | 7 |
| Installing Red Hat Linux 7.3 | 8 |
| Installing Additional Software | 9 |
| Installing RPM files | 9 |
| Determining whether RPM files are already installed | 10 |

1 Welcome

Purpose

This book explains how to set up Red Hat Linux on the server that runs components of the Avaya VisAbility™ Management Suite.

Prerequisites

Configuring Linux requires familiarity with Linux operating systems. Experience using Red Hat is highly desirable.

Intended Audience

We wrote this book for system administrators who are responsible for installing software on Linux-based systems.

Conventions Used in This Book

In this book, we use the following typographical conventions:

- We use bold type for emphasis and for any information that you should type; for example: **save translation**.
- We use Courier font for any information that the computer screen displays; for example: `login`.
- We use arrows to indicate options that you should select on cascading menus; for example: “Select File>Open” means choose the “Open” option from the “File” menu.

Additional Resources

The following additional book exists to help you during installation and configuration of selected applications in the suite: *Avaya VisAbility™ Management Suite Release 1.3 Advanced Converged Management Installation and Upgrade Procedures*, 555-233-149.

Tell Us What You Think!

Let us know how this book measured up to your expectations. Your opinions are crucial to helping us meet your needs! Please send us your comments by mail, fax, or e-mail, as follows:

Mail: Avaya Inc.
Avaya VisAbility Management Suite Documentation Team
Room 3C-313
307 Middletown Lincroft Rd.
Lincroft, NJ 07738
USA

Fax: Avaya VisAbility Management Suite Documentation Team
+ 1 732 852-2469

E-mail: document@avaya.com

How to Get This Book (and Others) on the Web

You can view or download the latest version of this book from the Avaya, Inc. web site. You must have access to the Internet, an Internet browser, and Adobe Acrobat Reader (version 5.0 or later) with Search. Adobe Acrobat Reader is available from <http://www.adobe.com>.

To view or download the latest version of the Avaya VisAbility Management Suite documentation:

1. Access <http://www.avaya.com/support>.
2. Click **Product Documentation**.
3. Click **System and Network Management**.
4. Locate the heading “Avaya VisAbility Management Suite,” and click the link corresponding to the software release.
5. Locate the title of the book, and click the link corresponding to the book.

2 Linux Server Installation

This document specifies the options that you must select during the installation of Red Hat Linux 7.3 to support Avaya MultiVantage Fault & Performance Manager, Avaya MultiVantage Proxy Agent, and Avaya MultiVantage Configuration Manager. This document is copied from the appendix of the Avaya VisAbility Management Suite Implementation Guidelines, which is available from your Avaya client executive.

If an option is not specified in this document, select the default response.

*** Note:** Make sure a modem is attached to COM 1 (ttyS0) of the Linux server for dial-in access and turned on while you install Red Hat Linux.

Installing Red Hat Linux 7.3

1. At the “Install Type” prompt (screen #5), choose the ‘Install’ and ‘Server’ options.
2. At the “Disk Partitioning Setup” prompt (screen #6), choose ‘Manually Partition with Disk Druid.’
3. At the “Disk Setup” prompt (screen #7), use the DELETE button to delete any partitioning that appears for the hard drive.
4. At the “Disk Setup” prompt (screen #7), use the ADD button to add partitions as shown in the following table.

The precise partition sizes are shown for a 40GB hard drive. If the hard drive is bigger than 40GB, use the proportion column to partition the hard drive.

| Mount Point | Partition Size (40MB HD) | Proportion of Disk Space (>40MB HD) | File System Type |
|-------------|--------------------------|-------------------------------------|------------------|
| / | 800 MB | 2% | ext3 |
| /boot | 100 MB | 1% | ext3 |
| /home | 7000 MB | 18% | ext3 |
| /usr | 13000 MB | 33% | ext3 |
| /var | 13000 MB | 33% | ext3 |
| swap | 2048 MB | 5% | swap |
| /tmp | 3000 MB | 8% | ext3 |
| Total | 38948 MB | 100% | |

5. At the “Network Configuration” prompt (screen #10), clear the ‘Configuration using DHCP’ checkbox and instead select ‘static IP.’
6. Then, enter the static IP address; subnet mask; Fully Qualified Domain Name; gateway; and primary, secondary, and tertiary DNS addresses.
7. At the “Firewall Configurations” prompt (screen #12), select ‘No firewall’ with ‘Use default firewall rules.’

*** Note:** The VisAbility Management Suite installation process will override the setting and select the default firewall rules.

8. At the “Account Configuration” prompt (screen #15), enter the password for the root user, and then add users including one for Avaya remote services.
9. At the “Package Group Selection” prompt (screen #16), select ‘Classic X window System,’ ‘GNOME,’ ‘KDE,’ and ‘Anonymous FTP Server.’

Installing Additional Software

1. After you install Red Hat, you must install the following individual RPM (Red Hat Package Manager) files from the Red Hat CD:
 - a. mgetty (install 1st)
 - b. mgetty-sendfax
 - c. uucp
2. In addition, verify that the following RPM files were loaded during the Red Hat installation:
 - a. ppp
 - b. vnc
 - c. vnc-server

If you need to install an RPM, perform the following procedures.

Installing RPM files

1. Insert the Red Hat installation CD in the CD-ROM drive.
 2. Open the Terminal Emulation program.
 3. Type **cd /mnt/cdrom/RedHat/RPMS**.
- * **Note:** If Linux responds “directory does not exist,” you may have to manually mount the CD-ROM drive. To do so, perform the following steps:
- a. Type **mount /dev/cdrom**.
 - b. Type **cd /dev/cdrom/RedHat/RPMS**.
4. At the command prompt, type **rpm -iv <name of RPM package>**.

Determining whether RPM files are already installed

1. In the terminal emulation window, at the command prompt, type **rpm -q <name of RPM package>**.
2. To search for RPM files using a partial RPM package name, at the command prompt type:

rpm -qa | grep <partial name>,

For example, **rpm -qa | grep vnc** to determine if any RPM packages beginning with “vnc” have been installed.