



N1 Grid Service Provisioning System 5.0 Installation Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 817-6500-10
December 2004

Copyright 2004 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. JVM is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Netscape is a trademark or registered trademark of Netscape Communications Corporation in the United States and other countries. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. Netscape Navigator is a trademark or registered trademark of Netscape Communications Corporation in the United States and other countries.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2004 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, Java sont des marques déposées ou enregistrées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. JVM sont des marques déposées ou enregistrées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. et Solaris sont des marques de fabrique ou des marques déposées, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. Netscape est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays. UNIX est une marque enregistrée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company Ltd. Netscape Navigator est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



041203@10536



Contents

Preface	13
1 N1 Grid Service Provisioning System 5.0 Overview	17
Installing the N1 Grid Service Provisioning System 5.0 – Process Overview	17
Overview of N1 Grid Service Provisioning System 5.0 Applications	19
Master Server	19
Local Distributor	19
Remote Agent	20
Command Line Interface Client	20
Network Protocols	21
Raw TCP/IP	21
Secure Shell	22
Secure Sockets Layer	22
Introduction to Plug-Ins	22
Acquiring Plug-Ins	23
2 System Requirements for the N1 Grid Service Provisioning System 5.0	25
General System Requirements	25
Supported Operating Systems	25
Supported Web Browsers	26
Required Operating System Patches	26
Requirements for SSH	28
Requirement for Jython	28
Requirements for Locales	28
Application Requirements	29
System Requirements for Applications on Solaris OS Systems	29

	System Requirements for Applications on Red Hat Linux	30
	System Requirements for Applications on IBM AIX	31
	System Requirements for Applications on Windows 2000	31
3	Gathering Information Before Installation	33
	Configuration Decisions	33
	The Java Runtime Environment	33
	User Ownership of Applications	34
	Host Names and IP Addresses	35
	Network Protocol	35
	Jython	36
	Worksheet for All Applications	36
	Worksheet for the Master Server	37
	Worksheet for Local Distributors	38
	Worksheet for Remote Agents	38
	Worksheet for CLI Clients	39
4	Installing the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems	41
	Installing the N1 Grid Service Provisioning System 5.0	41
	▼ How to Install the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems	42
	Non-Interactive Installation of a Remote Agent on Solaris OS, Red Hat Linux, and IBM AIX Systems	44
	▼ How to Non-Interactively Install a Remote Agent on Solaris OS, Red Hat Linux, and IBM AIX Systems	44
	Remote Installation of Remote Agents on Solaris OS, Red Hat Linux, and IBM AIX Systems	46
	▼ How to Remotely Install Remote Agents on Solaris OS, Red Hat Linux, and IBM AIX	46
	Starting Applications on Solaris OS, Red Hat Linux, and IBM AIX Systems	49
5	Installing the N1 Grid Service Provisioning System 5.0 on Windows Systems	51
	Installing the Master Server	51
	▼ How to Install the N1 Grid Service Provisioning System 5.0 Master Server on Windows	51
	▼ How to Create a Scheduled Task to Optimize the Database	53
	Installing the Remote Agent, Local Distributor, and CLI Client	54

	▼ How to Install the Remote Agent, Local Distributor, and CLI Client on Windows	54
	Non-Interactive Installation of a Remote Agent on Windows	55
	▼ How to Non-Interactively Install Remote Agents on Windows	55
	Remote Installation of Remote Agents on Windows	57
	▼ How to Remotely Install Remote Agents on Windows	57
	Remote Agent Variable Values	59
	Starting Applications on Windows Systems	60
6	Configuring the N1 Grid Service Provisioning System 5.0 to Use Secure Shell	63
	Overview of SSH and Requirements	64
	ssh-agent or Empty Password Keys	64
	SSH Requirements	65
	Additional SSH Security	66
	Configuring SSH – Process Overview	67
	Preparing the Keys	67
	▼ How to Generate Key Pairs	68
	▼ How to Set Up Keys for the ssh-agent	68
	▼ How to Set Up Keys for Empty Password Files When Using One Key Pair	69
	▼ How to Set Up Keys for Empty Password Files When Using Multiple Key Pairs	70
	Setting Up and Testing the Connectivity on the Master Server	71
	▼ How to Start the ssh-agent on the Master Server	71
	▼ How to Set Up and Test the Connectivity on the Master Server	72
	Configuring SSH for the Applications	73
	▼ How to Configure SSH for Local Distributors and Remote Agents	73
	▼ How to Configure SSH for the CLI Client With the ssh-agent	74
	▼ How to Configure SSH for the CLI Client With Empty Passwords	76
	SSH Advanced Parameters and Command Reference	77
	Advanced Parameters Reference	77
	OpenSSH 2.0 Command Reference	78
7	Configuring the N1 Grid Service Provisioning System 5.0 for SSL	81
	Overview of SSL Support in the N1 Grid Service Provisioning System 5.0	81
	Cipher Suites: Encryption and Authentication Overview	82
	Authentication Keystores	83
	Using Passwords With SSL	84

Limitations of SSL on the N1 Grid Service Provisioning System 5.0	84
Configuring SSL – Process Overview	85
Enabling HTTPS Connections from the Master Server Browser Interface	85
▼ How to Generate SSL Certificates	86
▼ How to Obtain a Signature for an SSL Certificate	86
▼ How to Enable HTTPS Connections from the Master Server Browser Interface	87
Requiring Users to Connect to the Master Server Browser Interface Using SSL	88
▼ How to Require Users to Connect to the Master Server Browser Interface Using SSL	88
▼ How to Revert to the Original Configuration	89
Creating Keystores	89
▼ How to Create Keystores	89
Configuring SSL	91
▼ How to Configure SSL	92
Sample Configuration Scenarios	93
SSL Cipher Suites	97
Cipher Suites for Solaris OS, Red Hat Linux, and Windows	97
Cipher Suites for IBM AIX	98
8 Configuring the Java Virtual Machine Security Policy	99
Configuring the JVM Security Policy	99
▼ How to Configure the JVM Policy for the Master Server	100
▼ How to Configure the JVM Policy for the Remote Agent	100
▼ How to Configure the JVM Policy for the Local Distributor	101
Postgres Security	101
9 Upgrading to the N1 Grid Service Provisioning System 5.0	103
Upgrading Overview	103
Upgrading Requirements	103
Upgrading – Process Overview	104
Upgrading the Master Server	105
▼ How to Migrate Master Server Data From Supported Operating Systems	105
▼ How to Upgrade a Master Server From an Operating System That Is No Longer Supported	107
Master Server Data Migration Details	109
Upgrading Remote Agents and Local Distributors	111

	▼ How to Upgrade Remote Agents and Local Distributors	111
	▼ How to Manually Upgrade Remote Agents and Local Distributors From an Operating System That Is No Longer Supported	112
10	Uninstalling the N1 Grid Service Provisioning System 5.0	115
	Uninstalling Applications on Solaris OS, Red Hat, and IBM AIX Systems	115
	▼ How to Uninstall a Solaris OS Master Server or CLI Client	115
	▼ How to Uninstall File-Based Applications on Solaris OS, Red Hat Linux, and IBM AIX Systems	116
	▼ How to Disable Automatic Database Optimization	117
	Uninstalling Applications on Windows Systems	118
A	Installation and Configuration Reference	119
	Reference Data for the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems	119
	Directory Structure of the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX	120
	Database Optimization on Solaris OS, Red Hat Linux, and IBM AIX Systems	122
	Sample Remote Agent Parameters File for Solaris OS, Red Hat Linux, and IBM AIX Systems	123
	Reference Data for the N1 Grid Service Provisioning System 5.0 on Windows	125
	Directory Structure of the N1 Grid Service Provisioning System 5.0 on Windows	125
	Cygwin	128
	Actions Performed by the Windows Installation Scripts	128
B	Troubleshooting	131
	Issues During Installation on Solaris OS, Red Hat Linux, and IBM AIX	131
	Warning When Installing the JRE on IBM AIX	131
	Issues During Installation on Microsoft Windows	132
	Error When Installing on Windows	132
	SSH Connectivity	132
	Master Server Unable to Connect to Local Distributor Through an Intermediate Local Distributor	132
	Unable to Connect to an Application Using SSH	133
	▼ How to Troubleshoot SSH Connectivity Issues	133

Glossary 135

Index 141

Tables

TABLE 2-1	Web Browser Requirements for the Browser Interface	26
TABLE 2-2	Required Patches for Supported Operating Systems	27
TABLE 2-3	Solaris <code>/etc/system</code> Settings	30
TABLE 2-4	Red Hat System Settings	31
TABLE 3-1	Information Requested for All Applications	36
TABLE 3-2	Information Requested for the Master Server	37
TABLE 3-3	Information Requested for Local Distributors	38
TABLE 3-4	Information Requested for Remote Agents	38
TABLE 3-5	Information Requested for CLI Clients	39
TABLE 4-1	Start Commands for Solaris OS, Red Hat Linux, and IBM AIX Applications	49
TABLE 5-1	Remote Agent Variable Values	59
TABLE 5-2	Names of Services to Start for the Windows Master Server, Local Distributor, and Remote Agent	60
TABLE 5-3	Start Commands for the Windows CLI Client	61
TABLE 6-1	OpenSSH 2.0 Commands	79
TABLE 9-1	Migration Overview	110
TABLE A-1	Directories Common to All Applications	120
TABLE A-2	Directories Installed for the Master Server	120
TABLE A-3	Directories Installed for the Local Distributor	121
TABLE A-4	Directories Installed for the Remote Agent	121
TABLE A-5	Directories Installed for the CLI Client	122
TABLE A-6	Directories Common to All Applications	126
TABLE A-7	Directories Installed for the Master Server	126
TABLE A-8	Directories Installed for the Local Distributor	126
TABLE A-9	Directories Installed for the Remote Agent	127
TABLE A-10	Directories Installed for the CLI Client	127

Examples

EXAMPLE 5-1	Non-Interactive Installation of a Remote Agent on Windows	56
EXAMPLE 5-2	Remote Installation of a Remote Agent On Windows	59
EXAMPLE 6-1	cprefix Example	77
EXAMPLE 6-2	sshpath Example	78
EXAMPLE 6-3	sshargs Example	78
EXAMPLE 7-1	crkeys Command Syntax	91
EXAMPLE 7-2	How to Configure SSL Without Authentication Between the Master Server, Local Distributor, and Remote Agent	93
EXAMPLE 7-3	How to Configure SSL Server Authentication	93
EXAMPLE 7-4	How to Configure SSL Server and Client Authentication	95
EXAMPLE 7-5	How to Configure SSL Authentication Between a CLI Client and Master Server	96

Preface

The N1 Grid Service Provisioning System 5.0 Installation Guide describes how to install and upgrade the N1™ Grid Service Provisioning System 5.0 on the Solaris™ Operating System (OS), Red Hat Linux, IBM AIX, and Windows 2000.

Note – In this document the term “x86” refers to the Intel 32-bit family of microprocessors and compatible 64-bit and 32-bit microprocessors made by AMD.

Who Should Use This Book

This book is intended for system administrators responsible for installing and configuring the N1 Grid Service Provisioning System 5.0.

How This Book Is Organized

The N1 Grid Service Provisioning System 5.0 Installation Guide describes the following topics.

- [Chapter 1](#) provides an overview of the tasks required to install and configure the software. This chapter also contains an overview of the software and supported network protocols.
- [Chapter 2](#) describes the system requirements for installing and using the software.
- [Chapter 3](#) contains worksheets to help you gather the information you need to install the software.

- [Chapter 4](#) describes the steps to install the software on Solaris OS, Red Hat Linux, and IBM AIX servers.
- [Chapter 5](#) describes the steps to install the software on Windows.
- [Chapter 6](#) describes the tasks necessary to configure the software to communicate using SSH.
- [Chapter 7](#) describes the tasks necessary to configure the software to communicate using SSL.
- [Chapter 8](#) describes how to configure the JVM™¹ security policy.
- [Chapter 9](#) describes the steps to upgrade the software.
- [Chapter 10](#) describes the steps to uninstall the software.
- [Appendix A](#) contains reference material related to installing and configuring the software.
- [Appendix B](#) describes steps to troubleshoot installation and configuration issues.

Related Books

You might need to refer to the following manuals when you install and use the N1 Grid Service Provisioning System 5.0.

- *N1 Grid Service Provisioning System 5.0 Release Notes*
- *N1 Grid Service Provisioning System 5.0 System Administration Guide*
- *N1 Grid Service Provisioning System 5.0 Command-Line Interface Reference Manual*

Accessing Sun Documentation Online

The docs.sun.comSM Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is <http://docs.sun.com>.

¹ The terms “Java Virtual Machine” and “JVM” mean a Virtual Machine for the Java™ platform.

Ordering Sun Documentation

Sun Microsystems offers select product documentation in print. For a list of documents and how to order them, see “Buy printed documentation” at <http://docs.sun.com>.

Typographic Conventions

The following table describes the typographic changes that are used in this book.

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name% you have mail.</code>
AaBbCc123	What you type, contrasted with onscreen computer output	<code>machine_name% su</code> <code>Password:</code>
<i>AaBbCc123</i>	Command-line placeholder: replace with a real name or value	The command to remove a file is <code>rm filename</code> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . Perform a <i>patch analysis</i> . Do <i>not</i> save the file. [Note that some emphasized items appear bold online.]

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	machine_name%
C shell superuser prompt	machine_name#
Bourne shell and Korn shell prompt	\$
Bourne shell and Korn shell superuser prompt	#

N1 Grid Service Provisioning System 5.0 Overview

This chapter provides an overview of the tasks required to install and configure the N1 Grid Service Provisioning System 5.0. This chapter also contains an overview of the applications included in the N1 Grid Service Provisioning System 5.0 and the types of network protocols that you can use for additional security.

This chapter discusses the following topics:

- “Installing the N1 Grid Service Provisioning System 5.0 – Process Overview” on page 17
- “Overview of N1 Grid Service Provisioning System 5.0 Applications” on page 19
- “Network Protocols” on page 21
- “Introduction to Plug-Ins” on page 22

Installing the N1 Grid Service Provisioning System 5.0 – Process Overview

The process overview below describes the tasks necessary to properly install and configure the N1 Grid Service Provisioning System 5.0.

1. Determine whether your server meets the minimum requirements to install.
See [Chapter 2](#).
2. Gather the information that you need to install the product.
See [Chapter 3](#).
3. (Optional) You can create a special, operating system group and user account to be used by N1 Grid Service Provisioning System 5.0.

If you create a new user and a new group, be sure to include the new user in the group. For more information about creating user accounts, see the documentation for your operating system.

4. (Optional) Install Jython on CLI Client machines.
You might choose to install Jython on any machine from which you want to run the CLI Client. Jython is not required to run the CLI Client. Jython is available from <http://www.jython.org>.
For more information about using the CLI Client with Jython, see Chapter 1, "Using the Command-Line Interface," in *N1 Grid Service Provisioning System 5.0 Command-Line Interface Reference Manual*.
5. Install each of the N1 Grid Service Provisioning System 5.0 applications individually using the appropriate installation script provided on the product media.
For installation instructions, see [Chapter 4](#) or [Chapter 5](#).
6. (Optional) If you plan to access the Master Server on the Internet, you can increase the Master Server security by configuring the N1 Grid Service Provisioning System 5.0 to use SSH to communicate with that server.
See [Chapter 6](#).
7. (Optional) If you want to provide the maximum security for communication among the applications, configure the applications to use SSL when communicating.
See [Chapter 7](#).
8. (Optional) If you do not use SSL to provide security for communication among applications, you can configure the JVM security policy so that the applications accept only connections from `localhost`. This setup provides a minimum level of security.
See [Chapter 8](#).
9. (Optional) Start the applications.
The installation program prompts you to start the applications upon successful installation. If you choose not to start the applications at that time, start the applications by following the instructions in "[Starting Applications on Solaris OS, Red Hat Linux, and IBM AIX Systems](#)" on page 49 or "[Starting Applications on Windows Systems](#)" on page 60.
10. Complete the initial setup.
See "[Configuring the N1 Grid Service Provisioning System – Process Overview](#)" in *N1 Grid Service Provisioning System 5.0 System Administration Guide* for more initial setup instructions.

Overview of N1 Grid Service Provisioning System 5.0 Applications

The N1 Grid Service Provisioning System 5.0 is a distributed software platform. The provisioning system includes the following special-purpose applications that you install on the servers in your network. These applications interact to allow you to deploy software to the servers in your network.

- [“Master Server” on page 19](#) – A central server that stores components and plans, and provides an interface for managing application deployments.
- [“Local Distributor” on page 19](#) – Optional servers that act as a proxy for the Master Server to optimize network communications across data centers and through firewalls.
- [“Remote Agent” on page 20](#) – A management application that performs operations on a host. Every server that you want to be controlled by the N1 Grid Service Provisioning System 5.0 must have the Remote Agent application.
- [“Command Line Interface Client” on page 20](#) – Optional applications that accept commands to be executed on the Master Server.

Master Server

The Master Server runs on Solaris OS, Red Hat Linux, Microsoft Windows 2000 Server, or Microsoft Windows 2000 Advanced Server servers. The Master Server is a central server that does the following:

- Manages a database that identifies all of the hosts that are registered in the provisioning software
- Stores components and plans in a repository
- Performs version control on the objects that are stored in the repository
- Authenticates provisioning system users and ensures that only authorized users perform specific operations
- Includes special-purpose engines for performing tasks such as dependency tracking and deployments
- Provides both a browser interface and a command-line interface for users

Local Distributor

A Local Distributor is a proxy that optimizes the distribution and management of Remote Agents. Data centers can use Local Distributors to do the following:

- Minimize network traffic during deployments. The Master Server sends one copy of a component to a Local Distributor, which replicates the component for installation on other servers.
- Minimize firewall reconfigurations. If a firewall stands between the Master Server and a collection of servers, administrators can open the firewall only for the Local Distributors, rather than for every server involved in a deployment.
- Minimize the load to the Master Server during large scale deployments.

Remote Agent

The Remote Agent is an application that runs on every server being managed by the N1 Grid Service Provisioning System 5.0. Remote Agents perform the tasks requested by the Master Server. The Remote Agents are supported on the Solaris OS, Red Hat Linux, IBM AIX, and Microsoft Windows 2000 platforms. Remote agents can do the following:

- Report server hardware and software configurations to the Master Server
- Start and stop services
- Manage directory contents and properties
- Install and uninstall software
- Run operating system commands and native scripts specified by components and plans

Command Line Interface Client

The Command Line Interface (CLI) Client provides a communication path to the Master Server to enable the execution of commands from local and remote servers. The CLI Client enables commands to be executed in the following environments:

- Windows command line
- UNIX shell such as bash

To execute these commands, the CLI Client establishes a connection to the Master Server through TCP/IP or securely using SSL, or SSH.

The CLI Client operates in the following two modes:

- Single-command mode, which enables you to submit one command at a time
- Interactive mode, which prompts you for commands, maintains a command history and allows for Jython scripting

When operating in interactive mode, the CLI Client uses the Jython programming language. Jython is a Java implementation of the high-level, dynamic, object-oriented language Python.

Note – Install Jython on any server on which you plan to run the CLI Client in interactive mode. For more information about Jython and to download Jython, visit <http://www.jython.org>.

Network Protocols

The N1 Grid Service Provisioning System 5.0 supports a variety of network protocols for communication among the software applications. You select the protocol to apply to each of the following types of network communication:

- Communication between the Master Server and Local Distributors or Remote Agents
- Communication between a particular Local Distributor and Remote Agents
- Communication between the Master Server and a CLI Client

The N1 Grid Service Provisioning System 5.0 supports the following protocols:

- Raw TCP/IP
- Secure Shell
- Secure Sockets Layer

You can tailor your network security to meet the needs of your particular network topology. For example, the communication within each of your data centers is secure, but your network connection to a remote data center passes through the public Internet. You might configure the Master Server to use SSL when communicating with a Local Distributor that is installed inside the firewall of the remote data center. Consequently, the communication over the Internet to the remote data center is secure. The Local Distributor might use raw TCP/IP to communicate with the Remote Agents because the communication over the local network is secure. For more information about the different protocols and about configuring the protocols, read [Chapter 6](#) and [Chapter 7](#).

Raw TCP/IP

Raw TCP/IP is standard TCP/IP without additional encryption or authentication. The advantage of raw TCP/IP is that it requires no additional set-up and configuration. If your data center network is protected by a firewall and secured from intrusion, using raw TCP/IP provides a convenient method for communication among N1 Grid Service Provisioning System 5.0 applications.

Secure Shell

Secure Shell (SSH) is a UNIX command suite and protocol for securely accessing a remote computer. SSH secures network client/server communications by authenticating both endpoints with a digital certificate and by encrypting passwords. SSH uses RSA public key cryptography to manage connections and authentication. SSH is more secure than telnet or other shell-based communication methods.

You can configure the N1 Grid Service Provisioning System 5.0 applications to communicate using SSH. The N1 Grid Service Provisioning System 5.0 supports OpenSSH which is a free version of SSH that has been primarily developed by the OpenBSD Project. For more details about OpenSSH, see <http://www.openssh.com>. The software can be configured to support other versions of SSH as well.

Secure Sockets Layer

Secure Sockets Layer (SSL) is a protocol for securing communication over IP networks. SSL uses TCP/IP sockets technology to exchange messages between a client and a server while protecting the message with a public-and-private key encryption system developed by RSA. Support for SSL is included in most web server products, as well as in the Netscape Navigator™ browser and Microsoft web browsers.

You can configure the N1 Grid Service Provisioning System 5.0 applications to use SSL for network communications to help prevent the software messages from being read or altered. Optionally, the applications can be configured to use SSL to authenticate each other before communicating, thereby increasing network security.

Introduction to Plug-Ins

In general usage, plug-in applications are programs that can easily be installed and used as part of your web browser. A plug-in application is recognized automatically by the browser and its function is integrated into the main HTML file that is being presented. Web browser plug-in applications generally play sound or motion video or perform some other functions.

In the N1 Grid Service Provisioning System environment, a plug-in differs only slightly in concept from the general usage. A plug-in for the N1 Grid Service Provisioning System product is a packaged solution that extends the provisioning capability of the product for a specific platform, application, or environment. For example, you might create a plug-in solution for a specific application, such as Oracle 8i, or for some feature of an operating system, such as Solaris Zones.

A plug-in includes all of the relevant data that is needed to support a new custom application. The contents of the plug-in are described in the plug-in descriptor file. This file is located in a standard place within the plug-in packaging structure.

Acquiring Plug-Ins

Several plug-ins have been created for use with the N1 Grid Service Provisioning System. The following plug-ins are available on the N1 Grid Service Provisioning System 5.0: Supplement CD and in the image downloaded from the Sun Download Center:

- N1 Grid Service Provisioning System 5.0 Solaris Plug-In
- N1 Grid Service Provisioning System 5.0 WebLogic Plug-In
- N1 Grid Service Provisioning System 5.0 Windows Plug-In
- N1 Grid Service Provisioning System 5.0 Linux Plug-In

Note – In previous versions of the N1 Grid Service Provisioning System, the WebLogic, Windows, and Linux component types, components, and plans were automatically installed with the provisioning system. In the N1 Grid Service Provisioning System 5.0, the plans, components, and component types associated with these solutions are now available only as plug-ins.

The plug-ins are packaged in Java archive files (.jar files). To make a given plug-in known to the N1 Grid Service Provisioning System product, you need to import the plug-in. For instructions to import a plug-in, see the user's guide associated with the plug-in that you want to import in the Plug-In User's Guide document collection at <http://docs.sun.com/db/coll/1223.1>.

System Requirements for the N1 Grid Service Provisioning System 5.0

This chapter lists the system requirements for installing and using the N1 Grid Service Provisioning System 5.0. This chapter discusses the following topics:

- “General System Requirements” on page 25
- “Application Requirements” on page 29

General System Requirements

This section lists requirements for installing and using the N1 Grid Service Provisioning System 5.0:

- “Supported Operating Systems” on page 25
- “Supported Web Browsers” on page 26
- “Required Operating System Patches” on page 26
- “Requirements for SSH” on page 28
- “Requirement for Jython” on page 28
- “Requirements for Locales” on page 28

Supported Operating Systems

You can install the N1 Grid Service Provisioning System 5.0 Master Server on servers that are running the following operating systems:

- Solaris 8 OS running on SPARC® based servers
- Solaris 9 OS running on SPARC and x86 based servers
- Red Hat Linux Advanced Server 2.1
- Microsoft Windows 2000 Server and Microsoft Windows 2000 Advanced Server

You can install the N1 Grid Service Provisioning System 5.0 Remote Agent, Local Distributor, and CLI Client on servers that are running the following operating systems:

- Solaris 7 and Solaris 8 OS running on SPARC based servers
- Solaris 9 and Solaris 10 OS running on SPARC and x86 based servers
- Red Hat Linux Advanced Server 2.1 and Red Hat Linux Advanced Server 3.0
- IBM AIX 5.1, 5.2
- Microsoft Windows 2000 Server and Microsoft Windows 2000 Advanced Server

Supported Web Browsers

The following table lists the web browser requirements for the N1 Grid Service Provisioning System 5.0 browser interface.

TABLE 2-1 Web Browser Requirements for the Browser Interface

Platform	Browser
Solaris	Netscape Navigator 6.2.2, Netscape Navigator 7.0
Red Hat	Netscape Navigator 6, Netscape Navigator 7.1
Windows	Internet Explorer 6, Netscape Navigator 6, Netscape Navigator 7.1

Note – Some web proxy servers are configured to block popup windows. The N1 Grid Service Provisioning System 5.0 relies on the ability to present popup windows to run properly. Do not run web proxy servers that block popup windows.

Required Operating System Patches

The following table lists the required patches for each supported operating system.

TABLE 2-2 Required Patches for Supported Operating Systems

OS Version	Required Patches
Solaris 7	106980-16 106541-16 107544-03 106950-13 106327-08 106300-09
Solaris 8, SPARC based servers	111310-01 109147-28 111308-04 112438-03 108434-15 108435-15 111111-04 112396-02 110386-03 111023-03 111317-05 113648-03 115827-01 116602-01 108987-13 108528-29 108989-02 108993-33 109326-14 110615-10
Solaris 9, SPARC based servers	None
Solaris 9, x86 based servers	None
Solaris 10, SPARC based servers	None
Solaris 10, x86 based servers	None

TABLE 2-2 Required Patches for Supported Operating Systems (Continued)

OS Version	Required Patches
IBM AIX 5.1	AIX 5100-04 maintenance level (APAR IY44478)
IBM AIX 5.2	AIX 5200-01 maintenance level (APAR IY 44479)
Red Hat Linux Advanced Server 2.1	None
Red Hat Linux Advanced Server 3.0	None
Windows 2000 Server or Windows 2000 Advanced Server	Service Pack 3

Requirements for SSH

If you want to use SSH for secure connections on Solaris OS, Red Hat Linux, or IBM AIX servers, you must have SSH protocol version 2 installed on each machine that you want to use SSH.

Requirement for Jython

If you want to use Jython with the CLI Client, install Jython version 2.0 or higher. For more information about Jython, see <http://www.jython.org>.

Requirements for Locales

The N1 Grid Service Provisioning System 5.0 has been internationalized to install and run in localized environment. Also, The N1 Grid Service Provisioning System 5.0 accepts non-ASCII characters. You will need to adhere to the following requirements if you require that the software support non-ASCII characters:

- All applications must be run in the same locale or in locales that are equivalent. The Remote Agent, Local Distributors, and CLI Client must run a locale that is compatible with the locale in which the Master Server is running.
- You must use Internet Explorer 5.5 or 6.0, or Netscape 7.0.
- Set the web browser Character Interface to use UTF-8, which is also known as Unicode or Universal Alphabet.
- In the configuration files, such as the `config.properties` file, all non-ASCII characters must be Unicode-encoded. You can create configuration files in any encoding. Then, use the `native2ascii` command that is available in the Java™ Development Kit (JDK) package to convert the file to Unicode-encoded ASCII

characters.

Application Requirements

This section lists the requirements for installing and using each of the N1 Grid Service Provisioning System 5.0 applications:

- “System Requirements for Applications on Solaris OS Systems” on page 29
- “System Requirements for Applications on Red Hat Linux” on page 30
- “System Requirements for Applications on IBM AIX” on page 31
- “System Requirements for Applications on Windows 2000” on page 31

System Requirements for Applications on Solaris OS Systems

Solaris Master Server

The Solaris Master Server requires the Solaris 8 or Solaris 9 operating system. The server must meet the following hardware requirements:

- SPARC hardware only for the Solaris 8 operating system.
- 450 MHz single or multiple CPU.
- At least 1 GByte RAM.
- 2 GBytes HD free space. The space required for the database is determined by the size of your deployed applications.

The following table lists the `/etc/system` settings that are required for a Solaris system that is running the Master Server.

Note – If you are using the Solaris 9 OS, you cannot change the values for `shmsys:shminfo_shmmin` and `shmsys:shminfo_shmseg`. The default values for these settings are acceptable.

TABLE 2-3 Solaris /etc/system Settings

Variable	Minimum Value
shmsys:shminfo_shmmax	0x20000000 ¹
shmsys:shminfo_shmmin	1
shmsys:shminfo_shmmni	2
shmsys:shminfo_shmseg	1
semsys:seminfo_semmni	32
semsys:seminfo_semmns	512
semsys:seminfo_semmsl	17
semsys:seminfo_sevmx	537

¹ 536870912 in decimal (512Mb), but this number must be specified in hex for the Solaris 8 Operating System.

Solaris Local Distributor, Remote Agent, and CLI Client

The Solaris Local Distributor requires the Solaris 7, Solaris 8, Solaris 9, or Solaris 10 operating system. The server must meet the following hardware requirements:

- SPARC hardware only for the Solaris 7 and Solaris 8 operating systems.
- 400 MHz single or multiple CPU.
- At least 256 MBytes RAM.
- 1 GBytes HD free space. The space required for cache is determined by the size of your deployed applications.

System Requirements for Applications on Red Hat Linux

The `bc` command must be in the user's path when the Red Hat Linux Master Server installation begins. Without the `bc` command, the installation exits and requests that `bc` be installed. Install the `bc-1.06-5.rpm` package or a later version of the package.

Red Hat Linux Master Server

The Red Hat Linux Master Server requires Red Hat Linux Advanced Server 2.1.

The server must meet the following hardware requirements:

- 1 GHz single or multiple CPU, Intel x86-compatible hardware only.
- At least 1 GByte RAM.

- 2 GBytes HD free space. The space required for the database is determined by the size of your deployed applications.

The Red Hat Linux Master Server installer checks the following system parameters and exits with an error if the minimum values are not met.

TABLE 2-4 Red Hat System Settings

System Parameter	Minimum Value
shmall in <code>/proc/sys/kernel/shmall</code>	536870912 (512Mb)
shmmax in <code>/proc/sys/kernel/shmmax</code>	536870912 (512Mb)

Red Hat Linux Local Distributor, Remote Agent, and CLI Client

The Red Hat Linux Local Distributor, Remote Agent, and CLI Client require one of the following versions of Red Hat Linux:

- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Advanced Server 3.0

The server must meet the following hardware requirements:

- 1 GHz single or multiple CPU, Intel x86-compatible hardware only.
- At least 1 GByte RAM.
- 1 GByte HD free space. The space that is required for cache is determined by the size of your deployed applications.

System Requirements for Applications on IBM AIX

The IBM AIX Local Distributor, Remote Agent, and CLI Client require the AIX 5.1, or 5.2 operating system. The server must meet the following hardware requirements:

- 400 MHz single or multiple CPU, pSeries hardware only.
- At least 256 MBytes RAM.
- 1 GByte HD free space. The space that is required for cache is determined by the size of your deployed applications.

System Requirements for Applications on Windows 2000

When running the Windows Master Server, Remote Agent, Local Distributor, or CLI Client, you must have enough space in the home directory for creating intermediate files. The space requirement is approximately equivalent to the size of the files that are installed to run the application.

Windows 2000 Master Server

The Windows Master Server requires one of the following versions of Windows:

- Windows 2000 Server
- Windows 2000 Advanced Server

The server must meet the following hardware requirements:

- 1 GHz single or multiple CPU, Intel x86-compatible hardware only.
- At least 1 GByte RAM.
- 2 GBytes HD free space The space required by the database is determined by the size of your deployed applications.

Windows 2000 Local Distributor, Remote Agent, and CLI Client

The Windows Local Distributor, Remote Agent, and CLI Client require one of the following versions of Windows:

- Windows 2000 Server
- Windows 2000 Advanced Server

The server must meet the following hardware requirements:

- 1 GHz single or multiple CPU, Intel x86-compatible hardware only.
- At least 1 GByte RAM.
- 1 GByte HD free space The space that is required for the database is determined by the size of your deployed applications.

Gathering Information Before Installation

This chapter contains information and worksheets to help you make decisions and gather all of the information that you need to install the N1 Grid Service Provisioning System 5.0. This chapter covers the following topics:

- “Configuration Decisions” on page 33
- “Worksheet for All Applications” on page 36
- “Worksheet for the Master Server” on page 37
- “Worksheet for Local Distributors” on page 38
- “Worksheet for Remote Agents” on page 38
- “Worksheet for CLI Clients” on page 39

Configuration Decisions

The installation program prompts you for configuration information for the N1 Grid Service Provisioning System 5.0. Use the sections below to make configuration decisions before you begin the installation.

The Java Runtime Environment

When installing on Solaris OS, Red Hat Linux, or IBM AIX servers, the installation program prompts you to install the JRE or to provide a valid path to a JRE. When installing on Windows, the installation program automatically installs the JRE without prompting you.

If you are installing on a Red Hat Linux server, the installation script searches your machine for an instance of the JRE in the default location.

- If the JRE is not installed in the default location, you must install the JRE.

- If the installation program finds the JRE in the default location, you can choose whether or not to reinstall the JRE.

If you are installing on Solaris OS or IBM AIX servers and you chose not to install the JRE, the installation script prompts you to provide a path to a valid JRE. Then the installation script verifies that the JRE is supported.

- If the JRE is not supported but has a higher version number than the versions that are supported, the installer warns you that the JRE is not supported and asks if you want to continue.
- If you specified a version of the JRE that is supported by the N1 Grid Service Provisioning System 5.0, the installation script sets the `JRE_HOME` variable to the JRE that you specified. The installation script also creates a symbolic link, `N1SPS5.0-home/common/jre`, which points to the JRE directory. `N1SPS5.0-home` is the home directory of the N1 Grid Service Provisioning System 5.0. By creating a symbolic link, the N1 Grid Service Provisioning System 5.0 applications use the JRE without changing its location, which other applications might depend upon.

Note – You should install the bundled JRE only once for each machine. For example, if you are installing the Master Server, a Local Distributor, and the CLI Client on the same machine, you should install the JRE with the Master Server, but not with the Local Distributor or the CLI Client.

User Ownership of Applications

The installation program prompts you to select a user and group to own the application that you are installing. If you want to configure the applications to communicate using SSH, install the Master Server, Local Distributors, and Remote Agents as the same user.

The root user cannot own the Master Server. You can install the Master Server as the user that owns the Master Server or you can install the application as root and, when you are prompted, specify which user owns the Master Server .

Note – If you are installing the Master Server or the CLI Client on a Solaris server, you must login as root.

If you want the Remote Agent to have root privileges on the machine where it is running, then you must run the installation program as the root user. Even though you may specify a user other than root to own the Remote Agent, if you want the Remote Agent to have root privileges on the machine where it is running, start the installation program as the root user.

Host Names and IP Addresses

The N1 Grid Service Provisioning System 5.0 applications require all servers to have a static IP address because the N1 Grid Service Provisioning System 5.0 application installed on a server uses the IP address to listen for network requests. The installation program prompts you to supply either a host name or an IP address. If the host name on a server does not resolve to that server's IP address, you will not be able to configure that server to connect within the N1 Grid Service Provisioning System.

If you supply a host name during the installation, the host name must resolve to the actual IP address of the server. Some servers are configured so that the host name does not resolve to the IP address or so that the host name resolves to the loopback address, 127.0.0.1. If the N1 Grid Service Provisioning System application is configured with the host name on a server with this configuration, the application might fail to start. Or, connections to this server from other N1 Grid Service Provisioning System applications also might fail.

When installing an N1 Grid Service Provisioning System application, specify the IP address of the server, not the host name. If you choose to specify the host name, ensure that the host name resolves to the actual IP address of the server.

Network Protocol

The installation program prompts you to choose a network protocol for communication among the software applications. For the Master Server, you can choose TCP/IP or SSL. For Local Distributors, Remote Agents, and CLI Clients, you can choose TCP/IP, SSH, or SSL.

TCP/IP is an insecure communication protocol. When using this connection protocol with the provisioning system, anyone with network access to a server that has an N1 Grid Service Provisioning System 5.0 application installed on it can connect to the provisioning system and issue commands. If you choose TCP/IP, you can secure the provisioning system by configuring the security policy file to only accept connections from servers that have N1 Grid Service Provisioning System 5.0 applications. For more details, see [Chapter 8](#).

SSL is more secure than TCP/IP. If you select SSL, you must also specify which cipher suite to use, encryption with no authentication or encryption with authentication. Encryption with no authentication is similar to using TCP/IP in that anyone with network access to a server that has a provisioning system application installed on it can connect to the provisioning system and issue commands. The encryption with authentication mode is the most secure choice when using SSL. You can further secure the provisioning system by configuring the security policy file to only accept connections from servers that have N1 Grid Service Provisioning System 5.0 applications. For more details, see [Chapter 8](#). For more information about SSL, see [Chapter 7](#).

Note – When you use SSL with a Local Distributor on an AIX server, the SSL cipher suite is set to encryption with authentication. Encryption with no authentication is not available for Local Distributors that are running on AIX servers.

SSH is the most secure network protocol and supported on only Solaris OS, Red Hat Linux, and IBM AIX platforms. To use SSH with the N1 Grid Service Provisioning System 5.0, you must install SSH software on your servers. For more information, see [Chapter 6](#).

Jython

When you install the CLI Client, the installation program prompts you to specify whether or not Jython is installed on the machine. The CLI Client uses the Jython programming language to run in interactive mode. However, Jython is not required to use the CLI Client. For more information about Jython and the CLI Client, see [“Command Line Interface Client” on page 20](#).

Worksheet for All Applications

The installation scripts for each of the N1 Grid Service Provisioning System 5.0 applications begin by performing the same set of preparatory tasks and asking the same questions about directories and files. Use the following worksheet to gather the information that you need to install each of the N1 Grid Service Provisioning System 5.0 applications.

TABLE 3–1 Information Requested for All Applications

Description	Value
The base directory in which to install the software. Example: <code>/opt/SUNWn1sps</code>	_____
If the JRE is already installed on the machine, the path to the JRE. Example: <code>/usr/local/jre</code> or the value of your <code>JAVA_HOME</code> environment variable	_____
The user that you want to own the application that you are installing.	_____

TABLE 3-1 Information Requested for All Applications (Continued)

Description	Value
On Solaris OS, Red Hat Linux, and IBM AIX servers, the group that you want to own the application that you are installing.	_____

Worksheet for the Master Server

Use the following worksheet to gather the information that you need to install the Master Server.

TABLE 3-2 Information Requested for the Master Server

Description	Value
IP address or host name for the Master Server machine.	_____
IP port number that the CLI Client should use to connect to the Master Server. Example: 1130	_____
IP address or host name of the SMTP mail server for the software to use to send notification mail messages.	_____
The subject line of email notifications from the software. Example: N1 Grid Service Provisioning System notification	_____
The name of the user account (user name) from which email notifications are sent. The installation program does not verify the validity of the user account name that you type.	_____
The name of the user account that the software should use when executing native commands. The installation program does not verify the validity of the user account name that you type.	_____
The port number on which the Postgres database will listen. Example: 5432	_____
The password for the admin user to access the Master Server browser interface after installation is complete.	_____
The port number on which the browser interface will be available. Example: 8080	_____

TABLE 3-2 Information Requested for the Master Server (Continued)

Description	Value
Whether you want to automate the optimization of your Postgres database.	_____
If yes, specify the time of day you want the Master Server database to be optimized by using the HH:MM format. Example: 23:00	
An entry will be made in your <code>crontab</code> file to optimize the database every day. Before installing, verify that a <code>crontab</code> file exists. If not, create one.	

Worksheet for Local Distributors

Use the following worksheet to gather the information that you need to install Local Distributors.

TABLE 3-3 Information Requested for Local Distributors

Description	Value
IP address or host name for the Local Distributor machine.	_____
The port number on which this Local Distributor will listen. Example: 1132	_____

Worksheet for Remote Agents

Use the following worksheet to gather the information that you need to install Remote Agents.

TABLE 3-4 Information Requested for Remote Agents

Description	Value
IP address or host name on which the Remote Agent will run.	_____

TABLE 3-4 Information Requested for Remote Agents (Continued)

Description	Value
The port number on which this Remote Agent will listen. Example: 1131	_____

Worksheet for CLI Clients

Use the following worksheet to gather the information that you need to install CLI Clients.

TABLE 3-5 Information Requested for CLI Clients

Description	Value
IP address or host name of the Master Server for the command line user interface.	_____
The IP port number of the Master Server. Example: 1130	_____
If Jython is already installed on this machine, the path to Jython. Default Value: /usr/local/jython	_____

Installing the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems

This chapter describes the steps to install the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX servers. This chapter discusses the following topics:

- “Installing the N1 Grid Service Provisioning System 5.0” on page 41
- “Non-Interactive Installation of a Remote Agent on Solaris OS, Red Hat Linux, and IBM AIX Systems” on page 44
- “Remote Installation of Remote Agents on Solaris OS, Red Hat Linux, and IBM AIX Systems” on page 46
- “Starting Applications on Solaris OS, Red Hat Linux, and IBM AIX Systems” on page 49

Installing the N1 Grid Service Provisioning System 5.0

You will install each of the applications separately by using the appropriate installation script on the product media. The installation scripts for each of the N1 Grid Service Provisioning System 5.0 applications begin by performing the same set of preparatory tasks and asking the same questions about directories, files, and installing the Java™ runtime environment (JRE). Each script then asks specific configuration questions about the application that it will install.

▼ How to Install the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems

Before You Begin

Review the installation process overview in “Installing the N1 Grid Service Provisioning System 5.0 – Process Overview” on page 17. Complete any necessary tasks prior to installing the applications.

Steps 1. Log in as the user that you want to own the application.

You can log in as root and install the software as the root user. If necessary, the installation program prompts you for information about which user should own the software.

Note – If you are installing the Master Server or the CLI Client on a Solaris server, you must login as root.

2. Access the installation scripts.

- If you are installing from a CD, insert the appropriate CD:
 - To install the software on a Solaris OS, SPARC server, insert the N1 Grid Service Provisioning System 5.0: Solaris, SPARC CD.
 - To install the software on a Solaris OS, x86 server, insert the N1 Grid Service Provisioning System 5.0: Solaris, x86 CD
 - To install the software on IBM AIX or Red Hat Linux, insert the N1 Grid Service Provisioning System 5.0: IBM-AIX, Red Hat Linux CD.
- If you are installing from the image that you downloaded, change to the directory where you saved the downloaded image.

3. Change to the directory on the software CD or within the downloaded image where the installation script is located.

```
# cd /script-directory
```

script-directory is one of the following values:

- solaris_sparc
- solaris_x86
- aix
- linux

4. Start the installation script for the application that you want to install.

```
# cr_app_opsystem_5.0.sh [-allowForwardVersion]
```

app is one of the following values:

- ms – installs the Master Server

- ra – installs the Remote Agent
- ld – installs the Local Distributor
- cli – installs the CLI Client

opsystem is one of the following values:

- solaris_sparc – installs the application on SPARC based hardware that is running the Solaris OS. To install the Master Server or CLI client, use `solaris_sparc_pkg`.
- solaris_x86 – installs the application on x86 based hardware that is running the Solaris OS. To install the Master Server or CLI client, use `solaris_x86_pkg`.
- aix – installs the application on IBM AIX
- linux – installs the application on Red Hat Linux

The `-allowForwardVersion` option enables you to install an N1 Grid Service Provisioning System 5.0 application on a version of an operating system that is numerically higher than the highest version the N1 Grid Service Provisioning System 5.0 supports for that operating system. If you use the `-allowForwardVersion` option, the installation program does not verify that the operating system on which you are installing the application is supported. There is no standard Sun Services support for use of the N1 Grid Service Provisioning System 5.0 on unsupported operating systems.



Caution – Installing the N1 Grid Service Provisioning System 5.0 on unsupported operating systems might result in undefined and unexpected behavior. Install the N1 Grid Service Provisioning System 5.0 on unsupported operating systems only for testing purposes. Do not use the N1 Grid Service Provisioning System 5.0 on unsupported operating systems in a production environment.

5. Answer the configuration questions when prompted by the installation program.

The installation program completes the installation and asks if you want to start the application.

The installation program saves a log of events in the `/tmp/N1GridSPSInstaller.log.pidnumber` file.

Non-Interactive Installation of a Remote Agent on Solaris OS, Red Hat Linux, and IBM AIX Systems

You can install the Remote Agent non-interactively by providing a parameters file to indicate your configuration selections. When you provide a parameters file to the installation program, the installation program does not prompt you for configuration selections during the installation. Instead, the installation program uses the configuration information that is provided in the parameters file.

▼ How to Non-Interactively Install a Remote Agent on Solaris OS, Red Hat Linux, and IBM AIX Systems

Before You Begin You must install a Master Server before you install a Remote Agent. The Master Server does not need to be installed on the machine on which you want to install the Remote Agent.

Steps 1. **On the machine where you want to install the Remote Agent, log in as the user that you want to own the Remote Agent.**

You can log in as root and install the software as the root user. If necessary, the installation program prompts you for information about which user should own the software.

2. **Access the installation scripts.**

- If you are installing from a CD, insert the appropriate CD:
 - To install the Remote Agent on a Solaris OS, SPARC server, insert the N1 Grid Service Provisioning System 5.0: Solaris, SPARC CD.
 - To install the Remote Agent on a Solaris OS, x86 server, insert the N1 Grid Service Provisioning System 5.0: Solaris, x86 CD.
 - To install the Remote Agent on IBM AIX or Red Hat Linux, insert the N1 Grid Service Provisioning System 5.0: IBM-AIX, Red Hat Linux CD.
- If you are installing from the image that you downloaded, change to the directory where you saved the downloaded image.

3. **Change to the directory on the software CD or within the downloaded image where the installation script is located.**

⌘ `cd /script-directory`

script-directory is one of the following values:

- solaris_sparc
- solaris_x86
- aix
- linux

4. Copy the installation script to the machine on which you want to install the Remote Agent.

```
% cp cr_ra_opsystem_5.0.sh RA-machine/
```

RA-machine is a directory on the machine on which you want to install the Remote Agent. *opsystem* is one of the following values:

- solaris_sparc – installs the Remote Agent on SPARC based hardware running the Solaris OS
- solaris_x86 – installs the Remote Agent on x86 based hardware running the Solaris OS
- aix – installs the Remote Agent on IBM AIX
- linux – installs the Remote Agent on Red Hat Linux

5. Copy a parameters file into the same directory as the installation script.

A sample parameters file is installed on the Master Server in the *N1SPS5.0-MasterServer-home/server/bin* directory when you install the Master Server. You can use the default values that are provided in this file or edit the file and add your custom values. The contents of the *cr_ra_remote_params.sh* sample parameters file are in “[Sample Remote Agent Parameters File for Solaris OS, Red Hat Linux, and IBM AIX Systems](#)” on page 123.

You can also create a new parameters file to use. The parameters file must be an executable file.

N1SPS5.0-MasterServer-home is the directory where you installed the Master Server.

6. Start the installation script.

```
% cr_ra_opsystem_5.0.sh -paramfile parameters-file.sh [-allowForwardVersion]
```

opsystem is one of the following values:

- solaris_sparc – installs the Remote Agent on SPARC based hardware running the Solaris OS
- solaris_x86 – installs the Remote Agent on x86 based hardware running the Solaris OS
- aix – installs the Remote Agent on IBM AIX
- linux – installs the Remote Agent on Red Hat Linux

parameters-file is the name of the parameters file that you want the installation program to use to obtain the configuration information. The parameters file must be an executable file.

The *-allowForwardVersion* option enables you to install an N1 Grid Service Provisioning System 5.0 Remote Agent on a version of an operating system that is

numerically higher than the highest version the N1 Grid Service Provisioning System 5.0 supports for that operating system. If you use the `-allowForwardVersion` option, the installation program does not verify that the operating system on which you are installing the Remote Agent is supported. There is no standard Sun Services support for use of the N1 Grid Service Provisioning System 5.0 on unsupported operating systems.



Caution – Installing the N1 Grid Service Provisioning System 5.0 on unsupported operating systems might result in undefined and unexpected behavior. Install the N1 Grid Service Provisioning System 5.0 on unsupported operating systems only for testing purposes. Do not use the N1 Grid Service Provisioning System 5.0 on unsupported operating systems in a production environment.

Remote Installation of Remote Agents on Solaris OS, Red Hat Linux, and IBM AIX Systems

You can install a Remote Agent remotely from another machine across the network. When you install the Master Server, the scripts needed to remotely install a Remote Agent are installed in the `N1SPS5.0-MasterServer-home/server/bin` directory. The installation is a non-interactive installation and uses environment variables to manage the installation and configuration of the Remote Agents. You can set the environment variables in a parameters file, at the command line, or use the default values provided by the installation script.

▼ How to Remotely Install Remote Agents on Solaris OS, Red Hat Linux, and IBM AIX

The installation scripts for the Remote Agent are specific to the operating system of the target machine. You need to complete these steps for each operating system running on your target machines.

Before You Begin

The target machine must meet the following requirements:

- The UNIX utility `sshd` must be running and have direct IP connectivity to the source machine.
- Support for the UNIX `hostname` command must exist, so that the remote installation script can call this command. The Remote Agent must be configured to listen on the IP address of the host name returned by the `hostname` command.

The Master Server machine must have the UNIX utilities `ssh` and `scp` installed and in the path at the time of execution.

The remote installation program uses environment variables to manage the installation and configuration of the Remote Agent. You can set the environment variables in a parameters file, at the command line, or use the default values provided by the installation script. Following are the required environment variables and their default values:

- `CR_RA_CTYPE=raw` – The Remote Agent connects to the Master Server or Local Distributor using no encryption. Other values for this variable are `ssh` and `ssl`.
- `CR_RA_SUID=y` – Installs the Remote Agent with `setuid` root privilege. To specify a value of `yes`, you must run the installation script as the root user.
- `CR_RA_INSTALLER_HOSTS=host1,host3.enterprise.com,10.10.0.207` – If you do not supply host names on the command line or as an environment variable, the installation script exits with an error.

Steps 1. On the Master Server machine, access the installation scripts.

- If you are installing from a CD, insert the appropriate CD:
 - To install the Remote Agent on a Solaris OS, SPARC server, insert the N1 Grid Service Provisioning System 5.0: Solaris, SPARC CD.
 - To install the Remote Agent on a Solaris OS, x86 server, insert the N1 Grid Service Provisioning System 5.0: Solaris, x86 CD.
 - To install the Remote Agent on IBM AIX or Red Hat Linux, insert the N1 Grid Service Provisioning System 5.0: IBM-AIX, Red Hat Linux CD.
- If you are installing from the image that you downloaded, change to the directory where you saved the downloaded image.

2. Change to the directory on the software CD or within the downloaded image where the installation script is located.

```
% cd /script-directory
```

script-directory is one of the following values:

- `solaris_sparc`
- `solaris_x86`
- `aix`
- `linux`

3. Copy the installation script to the Master Server.

```
% cp cr_ra_opsystem_5.0.sh N1SPS5.0-MasterServer-home/server/bin
```

N1SPS5.0-MasterServer-home is the directory where you installed the Master Server and *opsystem* is one of the following values:

- `solaris_sparc` – installs the Remote Agent on SPARC based hardware running the Solaris OS

- `solaris_x86` – installs the Remote Agent on x86 based hardware running the Solaris OS
- `aix` – installs the Remote Agent on IBM AIX
- `linux` – installs the Remote Agent on Red Hat Linux

4. Change directories to where the scripts are located.

```
% cd N1SPS5.0-MasterServer-home/server/bin
```

`N1SPS5.0-MasterServer-home` is the directory where you installed the Master Server.

5. Determine how to provide configuration information to the installation script.

- Create a new parameters file or edit the sample parameters file that was installed by the N1 Grid Service Provisioning System 5.0. When you install the Master Server, a parameters file is installed. The file is named `N1SPS5.0-MasterServer-home/server/bin/cr_ra_remote_params.sh`. You can use the default values that are provided in this file or edit the file and add your custom values. You can also create a new parameters file to use. The contents of the sample parameters file are in [“Sample Remote Agent Parameters File for Solaris OS, Red Hat Linux, and IBM AIX Systems”](#) on page 123. The parameters file must be an executable file.

- Set the environment variables.

```
% export CR_RA_INSTALLER_USER=username
% export CR_RA_INSTALLER_WORKDIR=/working_directory
% export CR_RA_INSTALLER_LEAVEFILES=yes_or_no
% export CR_RA_INSTALLER_HOSTS=hostnames.enterprise.com,10.10.0.207
```

6. Start the remote installation.

```
% cr_ra_remote.sh -paramfile path-to-file/parameters-file.sh -f
cr_ra_opsystem_5.0.sh hostnames
```

- `cr_ra_opsystem_5.0.sh` is the installation script that you copied from the N1 Grid Service Provisioning System 5.0 CD or downloaded image.
- `path-to-file/parameters-file` is the path to the parameters file and the name of the parameters file that you want the installation program to use to obtain the configuration information. If you set the environment variables or you want the installation script to use the default values, you do not need to specify a parameters file.
- `hostnames` are the host names of the machines on which to perform the installation. Separate the hostnames by a space. If you specified the host names in the `CR_RA_INSTALLER_HOSTS` parameter, either in the parameters file or as an environment variable, you do not need to specify the hostnames on the command line. If you specify host names on the command line, those hosts are installed and any hosts specified in the `CR_RA_INSTALLER_HOSTS` parameter are not be installed.

7. Make a note of the location of the log file.

The installation program notifies you that it is creating a log file and displays the location of the log file. Note the location of the file so that you can view it later.

8. If prompted by the installation program, provide passwords for the remote machine.

The installation script generates log files on the remote machine.

Starting Applications on Solaris OS, Red Hat Linux, and IBM AIX Systems

The following table lists the commands to start the N1 Grid Service Provisioning System 5.0 applications on Solaris OS, Red Hat Linux, and IBM AIX servers. *N1SPS5.0-home* is the home directory of the application.



Caution – Do not use the Bourne shell to start the Master Server or other N1 Grid Service Provisioning System 5.0 applications. If you start the Master Server process using the `cr_server start` command in a Bourne shell, and if a `^C` command is issued to any subsequent command in the same shell that started the Master Server, then the database and Master Server processes stop.

In the *N1SPS5.0-home/server/bin/roxdb.out* file, the following messages appear as the most recent entries:

```
DEBUG: fast shutdown request
DEBUG: aborting any active transactions
```

TABLE 4–1 Start Commands for Solaris OS, Red Hat Linux, and IBM AIX Applications

Application	Path to Command	Command to Start
Master Server	<i>N1SPS5.0-home/server/bin/</i>	<code>cr_server start</code>
Local Distributor	<i>N1SPS5.0-home/ld/bin/</i>	<code>cr_ld start</code>
Remote Agent	<i>N1SPS5.0-home/agent/bin/</i>	<code>cr_ra start</code>
CLI Client	<i>N1SPS5.0-home/cli/bin/</i>	<code>cr_cli CLI-command</code>
Jython version of CLI Client	<i>N1SPS5.0-home/cli/bin/</i>	<code>cr_clij CLI-command</code>

Installing the N1 Grid Service Provisioning System 5.0 on Windows Systems

This chapter describes the steps to install the N1 Grid Service Provisioning System 5.0 on servers running Windows. You will install each of the applications separately by using the appropriate Microsoft Installer (MSI) package on the product media. The MSI packages for each of the N1 Grid Service Provisioning System 5.0 applications begin by performing the same set of preparatory tasks and asking the same questions about directories and files. Each MSI package then asks specific configuration questions about the application that it will install.

This chapter discusses the following topics:

- “Installing the Master Server” on page 51
- “Installing the Remote Agent, Local Distributor, and CLI Client” on page 54
- “Non-Interactive Installation of a Remote Agent on Windows” on page 55
- “Remote Installation of Remote Agents on Windows” on page 57
- “Remote Agent Variable Values” on page 59
- “Starting Applications on Windows Systems” on page 60

Installing the Master Server

▼ How to Install the N1 Grid Service Provisioning System 5.0 Master Server on Windows

Before You Begin

Review the installation process overview in “Installing the N1 Grid Service Provisioning System 5.0 – Process Overview” on page 17. Complete any necessary tasks prior to installing the Master Server.

If you want to install the Master Server remotely, use the Virtual Network Computing (VNC) software to access the server. If you use Terminal Client Services to access the server, the installation fails.

Ensure that you have write permissions on the folder in which the MSI packages are saved.

Steps 1. **Access the MSI packages.**

- If you are installing from a CD, insert the N1 Grid Service Provisioning System 5.0: Windows CD.
- If you are installing from the image that you downloaded, change to the directory where you saved the downloaded image.

2. **Use the Windows File Manager or a Command Prompt to access the windows directory on the CD or in the directory where you saved the downloaded image.**

3. **Start the Master Server installation.**

- If you are using the File Manager, double-click the `cr_ms_win32_5.0.msi` file.
- If you are at a Command Prompt, type the name of the installation file at the prompt.

```
E:\N1GSPS5.0\windows> cr_ms_win32_5.0.msi [ALLOWFORWARDVERSION=true]
```

The `ALLOWFORWARDVERSION=true` option enables you to install an N1 Grid Service Provisioning System 5.0 Master Server on a version of an operating system that is numerically higher than the highest version the N1 Grid Service Provisioning System 5.0 supports for that operating system. If you use the `ALLOWFORWARDVERSION=true` option, the installation program does not verify that the operating system on which you are installing the Master Server is supported. There is no standard Sun Services support for use of the N1 Grid Service Provisioning System 5.0 on unsupported operating systems.



Caution – Installing the N1 Grid Service Provisioning System 5.0 on unsupported operating systems might result in undefined and unexpected behavior. Install the N1 Grid Service Provisioning System 5.0 on unsupported operating systems only for testing purposes. Do not use the N1 Grid Service Provisioning System 5.0 on unsupported operating systems in a production environment.

4. **Answer the configuration questions when prompted by the installation program.**

The installation program prompts you to answer a series of configuration questions and then displays the Ready to Install screen.

5. **Click Install to begin the installation.**

The installation program installs the program files. When the installation completes, the installation program prompts you to restart the machine.

6. Restart the machine to complete the installation.

You must restart the machine to complete the installation of the N1 Grid Service Provisioning System 5.0.

7. Log in to the server.

After you log in, the installation program displays a Welcome screen.

8. Click Next to complete the installation.

Note – The installer opens Command Prompt windows and executes commands. Some of the commands might take several minutes to run. Do not close the Command Prompt windows or cancel the operations. The operations complete automatically after a few minutes.

9. Click Finish to exit the installation program.

The Master Server is installed. Access the Master Server by using your web browser and the browser interface address that you specified during the installation.

10. (Optional) Create a scheduled task to optimize the database.

To optimize the performance of your database, create a scheduled task that runs the `vacuumdb` utility daily. To create the scheduled task, follow the instructions in [“How to Create a Scheduled Task to Optimize the Database”](#) on page 53.

▼ How to Create a Scheduled Task to Optimize the Database

Steps 1. **Open the Windows 2000 Scheduled Tasks Folder.**

You can open the Scheduled tasks folder by clicking the Start menu, then clicking Programs -> Accessories -> System Tools -> Scheduled Tasks.

2. **To create a new task, right click in the folder and select New -> Scheduled Task.**

3. **Name the task.**

4. **Double-click on the task to edit it.**

5. **In the Run field, type the following command on a single line:**

```
bash -c "%cygdrive/c/Program Files/N1\ Grid\ Service\ Provisioning\ System/5.0/server/bin/roxdbcmd vacuumdb -h localhost -a -z"
```

c:/Program\ Files/N1\ Service\ Provisioning\ System/5.0 is the directory in which you installed the Master Server.

6. In the **Schedule** tab, configure the task to run once a day.

Installing the Remote Agent, Local Distributor, and CLI Client

▼ How to Install the Remote Agent, Local Distributor, and CLI Client on Windows

Before You Begin Review the installation process overview in [“Installing the N1 Grid Service Provisioning System 5.0 – Process Overview”](#) on page 17. Complete any necessary tasks prior to installing the Master Server.

Ensure that you have write permissions on the folder in which the MSI packages are saved.

- Steps**
1. **Access the installation MSI packages.**
 - If you are installing from a CD, insert the N1 Grid Service Provisioning System 5.0: Windows CD.
 - If you are installing from the image that you downloaded, change to the directory where you saved the downloaded image.
 2. **Use the Windows File Manager or a Command Prompt to access the `windows` directory on the CD or in the directory where you saved the downloaded image.**
 3. **Start the installation for the application you want to install.**
 - If you are using the File Manager, double-click the `cr_app_win32_5.0.msi` file.
 - If you are in a Command Prompt, type the name of the installation file at the prompt.

```
E:\N1GSPS5.0\windows> cr_app_win32_5.0.msi [ALLOWFORWARDVERSION=true]
```

`app` is one of the following values:

 - `ra` – installs the Remote Agent
 - `ld` – installs the Local Distributor

- `cli` – installs the CLI Client

The `ALLOWFORWARDVERSION=true` option enables you to install an N1 Grid Service Provisioning System 5.0 application on a version of an operating system that is numerically higher than the highest version the N1 Grid Service Provisioning System 5.0 supports for that operating system. If you use the `ALLOWFORWARDVERSION=true` option, the installation program does not verify that the operating system on which you are installing the application is supported. There is no standard Sun Services support for use of the N1 Grid Service Provisioning System 5.0 on unsupported operating systems.



Caution – Installing the N1 Grid Service Provisioning System 5.0 on unsupported operating systems might result in undefined and unexpected behavior. Install the N1 Grid Service Provisioning System 5.0 on unsupported operating systems only for testing purposes. Do not use the N1 Grid Service Provisioning System 5.0 on unsupported operating systems in a production environment.

4. **Answer the configuration questions when prompted by the installation program.**
The installation program prompts you to answer a series of configuration questions and then displays the Ready to Install screen.
5. **Click Install to begin the installation.**
The installation program installs the program files.
6. **Click Finish to exit the installation program.**

Non-Interactive Installation of a Remote Agent on Windows

You can install the Remote Agent by using variables on a command line to indicate your configuration selections. The non-interactive installation for Remote Agents is accomplished by using the `msiexec` command that is installed as part of the Windows Installer Service.

▼ How to Non-Interactively Install Remote Agents on Windows

Before You Begin

Ensure that you have write permissions on the folder in which the MSI packages are saved.

- Steps**
1. On the machine where you want to install the Remote Agent, open a Command Prompt window.
 2. Insert the N1 Grid Service Provisioning System 5.0: Windows CD.
 3. Change to the directory where the MSI package is located, either on the software CD or from the directory where you saved the downloaded image.
 4. Copy the installation MSI package to the machine on which you want to install the Remote Agent.

```
% copy cr_ra_win32_5.0.msi RA-machine\
```

RA-machine is a directory on the machine on which you want to install the Remote Agent.

5. Start the installation.

```
C:RA-machine\> msisexec /i cr_ra_win32_5.0.msi /qn  
VARIABLE=value VARIABLE=value [ALLOWFORWARDVERSION=true]
```

You may include as many variables as necessary. Variable values that contain spaces, such as directory names, must be included in quotation marks. For the variables and values accepted by the non-interactive installation program, refer to [Table 5-1](#). If you do not include any variables or values, the installation program installs the Remote Agent using the default values.

The `ALLOWFORWARDVERSION=true` option enables you to install an N1 Grid Service Provisioning System 5.0 Remote Agent on a version of an operating system that is numerically higher than the highest version the N1 Grid Service Provisioning System 5.0 supports for that operating system. If you use the `ALLOWFORWARDVERSION=true` option, the installation program does not verify that the operating system on which you are installing the Remote Agent is supported. There is no standard Sun Services support for use of the N1 Grid Service Provisioning System 5.0 on unsupported operating systems.



Caution – Installing the N1 Grid Service Provisioning System 5.0 on unsupported operating systems might result in undefined and unexpected behavior. Install the N1 Grid Service Provisioning System 5.0 on unsupported operating systems only for testing purposes. Do not use the N1 Grid Service Provisioning System 5.0 on unsupported operating systems in a production environment.

Example 5-1 Non-Interactive Installation of a Remote Agent on Windows

The following example is a sample of the command to install the Remote Agent non-interactively on Windows.

```
C:\> msisexec /i cr_ra_win32_5.0.msi /qn  
INSTALLDIR="C:\Program Files\N1 Grid Service Provisioning System\  
RA_PARENT_CONNECTION=false
```

Remote Installation of Remote Agents on Windows

The Remote Agent MSI package facilitates remote installation in a non-interactive mode. The installation is accomplished by using a .wsh script used by the Windows Scripting Host. The script file contains VB script code that does the following:

- Attaches to the Remote Systems WMI DCOM interface
- Uses WMI to create a temporary Windows file share on the target server
- Copies `cr_ra_win32_5.0.msi` from the local location to the target share
- Uses WMI remotely to run the silent MSI on the target machine

▼ How to Remotely Install Remote Agents on Windows

Before You Begin Ensure that you have write permissions on the folder in which the MSI packages are saved.

- Steps**
1. **On the Master Server machine, open a Command Prompt window.**
 2. **Access the MSI packages.**
 - If you are installing from a CD, insert the N1 Grid Service Provisioning System 5.0: Windows CD.
 - If you are installing from the image that you downloaded, change to the directory where you saved the downloaded image.
 3. **Change to the directory where the MSI package is located, either on the software CD or from the directory where you saved the downloaded image.**

4. **Copy the MSI package to the Master Server.**

```
C:\> copy cr_ra_win32_5.0.msi MS-machine\  
MS-machine is a directory on the Master Server machine.
```

5. **Change to the Master Server home directory.**

```
C:\> cd N1SPS5.0-home\server\bin\WinInstaller  
N1SPS5.0-home is the directory in which you installed the Master Server.
```

6. **Start the installation.**

```
C:\MS-machine> cscript WinInstaller.wsf [ALLOWFORWARDVERSION=true] parameters Hostname
```

The `ALLOWFORWARDVERSION=true` option enables you to install an N1 Grid Service Provisioning System 5.0 Remote Agent on a version of an operating system

that is numerically higher than the highest version the N1 Grid Service Provisioning System 5.0 supports for that operating system. If you use the `ALLOWFORWARDVERSION=true` option, the installation program does not verify that the operating system on which you are installing the Remote Agent is supported. There is no standard Sun Services support for use of the N1 Grid Service Provisioning System 5.0 on unsupported operating systems.



Caution – Installing the N1 Grid Service Provisioning System 5.0 on unsupported operating systems might result in undefined and unexpected behavior. Install the N1 Grid Service Provisioning System 5.0 on unsupported operating systems only for testing purposes. Do not use the N1 Grid Service Provisioning System 5.0 on unsupported operating systems in a production environment.

Hostname is the hostname of the machine on which to install the Remote Agent.

If you do not include values for any of the following *parameters* on the command line, the installation program installs the Remote Agent using the default values as shown below.

The Remote Agent non-interactive installation program accepts the parameters that are listed in the following table.

Parameter	Description	Default
-user	User to connect to WMI on the target machine.	None
-password	Password to connect to the WMI on the target machine.	None
variables	The Windows variable for the <code>cscript WinInstaller.wsf</code> command found in Table 5-1 . All variables and values must be contained in a string that is enclosed by quotation marks.	None
-msiLocation	Paths to the <code>.msi\input</code> files to install.	Current working directory
-shareLocation	An existing directory on the target machine in which to create a temporary Windows file share. The file share directory must be at least the size of the MSI package.	C:\WINNT\Temp

The exit code is 0 for a successful installation and 1 for a failure.

Example 5-2 Remote Installation of a Remote Agent On Windows

The following example is a sample of the command to remotely install a Remote Agent on Windows.

```
C:\> cscript WinInstaller.wsf -shareLocation C:\installs -options  
"INSTALLDIR='C:\Program Files\N1 Grid Service Provisioning System'" targetHost
```

Remote Agent Variable Values

The Remote Agent non-interactive and remote installation programs accepts the following variables.

TABLE 5-1 Remote Agent Variable Values

Variable Name	Description	Default	Values
INSTALLDIR	Specify the directory in which to install the Remote Agent.	C:\Program Files\N1 Grid Service Provisioning System	Any valid directory.
REMOTE_AGENT_HOSTNAME	Specify the hostname or IP address for the machine on which to install the Remote Agent.	The Windows computer name	Any valid hostname or IP address.
RA_PORT_NUMBER	Specify the IP Port number to use for this Remote Agent.	1131	Any valid port number.
RA_PARENT_CONNECTION	Specify that the parent application connects to this Remote Agent by using unencrypted (raw) or SSL connections.	true	true specifies to use SSL. false specifies to use raw.
RA_SSL_CIPHER	If you selected SSL, specify the type of SSL cipher suite to use.	1	0 specifies to use encryption with authentication. 1 specifies to use encryption without authentication.

TABLE 5-1 Remote Agent Variable Values (Continued)

Variable Name	Description	Default	Values
RA_SERVICE_USERNAME RA_SERVICE_PASSWORD	Specify which user account the Remote Agent is to run as.	system user	Use a prefix of .\ for local user names. If you define these variables, you must set RA_SERVICE_CONTROL to other.
RA_SERVICE_AUTOSTART	Specify whether to start the Remote Agent automatically on server restart. The variable also determines whether the Remote Agent is started at the time of the installation.	1	1 specifies to start automatically. 0 specifies to not start automatically.

Starting Applications on Windows Systems

On Windows servers, you start the Master Server, Local Distributor, and Remote agent in the Services Panel. You start the CLI Client from a Command Prompt window.

To start the Master Server, Local Distributor, or Remote Agent, click the Start menu, then Programs -> Administrative Tools -> Services. In the Services panel, find the name of the application and start it.

TABLE 5-2 Names of Services to Start for the Windows Master Server, Local Distributor, and Remote Agent

Application	Name of Service to Start
Master Server	N1 Grid Service Provisioning System 5.0 Server
	N1 Grid Service Provisioning System 5.0 PostgreSQL Server
	N1 Grid Service Provisioning System 5.0 IPC Daemon
	N1 Grid Service Provisioning System 5.0 Database Preparer
Local Distributor	N1 Grid Service Provisioning System 5.0 Distributor
Remote Agent	N1 Grid Service Provisioning System 5.0 Agent

To start the CLI Client on a Windows server, type one of the following commands at a Command Prompt. *N1SPS5.0-home* is the home directory of the application.

TABLE 5-3 Start Commands for the Windows CLI Client

Application	Path to Command	Command to Start
CLI Client	<i>N1SPS5.0-home\cli\bin\</i>	<i>cr_cli.cmd CLI-command</i>
Jython version of CLI Client	<i>N1SPS5.0-home\cli\bin\</i>	<i>cr_clij.cmd CLI-command</i>

Configuring the N1 Grid Service Provisioning System 5.0 to Use Secure Shell

This chapter contains instructions for configuring the N1 Grid Service Provisioning System 5.0 to communicate using Secure Shell (SSH).

The N1 Grid Service Provisioning System 5.0 supports OpenSSH 2.0 explicitly. OpenSSH 2.0 is a free version of SSH that has primarily been developed by the OpenBSD Project. For more details, see <http://www.openssh.com>. The software can be configured to support other versions of SSH.

Using the same implementation of SSH on each server in your network ensures that the keys are compatible and that the servers communicate properly. You may choose to use different implementations of SSH on servers in your network, but you must test to verify that the various implementations are compatible and interoperable.

Note – The commands and interface examples in this chapter apply to OpenSSH 2.0. If you are using a different version of SSH, refer to the documentation provided with that version of SSH to determine the commands and options that are equivalent to the commands used in OpenSSH 2.0. For details about the OpenSSH 2.0 commands and options used, refer to [“OpenSSH 2.0 Command Reference”](#) on page 78.

This chapter discusses the following topics:

- [“Overview of SSH and Requirements”](#) on page 64
- [“Configuring SSH – Process Overview”](#) on page 67
- [“Preparing the Keys”](#) on page 67
- [“Setting Up and Testing the Connectivity on the Master Server”](#) on page 71
- [“Configuring SSH for the Applications”](#) on page 73
- [“SSH Advanced Parameters and Command Reference”](#) on page 77

Overview of SSH and Requirements

SSH is a UNIX-based command suite and protocol for securely accessing a remote computer. SSH secures network client/server communications by authenticating both endpoints with a digital certificate and by encrypting passwords. SSH uses RSA public key cryptography to manage connections and authentication. SSH is more secure than telnet and other shell based communication methods, and is used to manage web servers and other remote servers.

Unlike the other connection types, when an SSH connection is set up between two N1 Grid Service Provisioning System 5.0 applications, the downstream application does not need to be manually started. The upstream application automatically starts the downstream application when it is needed. The downstream application remains running for the duration necessary and shuts down automatically when it is not used for a configurable period of time.

Do not manually start the downstream application for an SSH connection. For example, if you set up a Local Distributor to connect to a Remote Agent using SSH, do not manually start the Remote Agent. The Local Distributor automatically starts the Remote Agent when necessary. The Remote Agent continues to run for as long as it is being used. The Local Distributor will automatically shut down the Remote Agent when it has not been used for a configurable period of time.

ssh-agent or Empty Password Keys

You can configure SSH to use the `ssh-agent` or to use empty password keys. If you use empty password keys, the generated SSH private key is stored with an empty password. As a result, you do not need a password to access the key. When you use SSH to communicate with another machine that trusts its public key, you are not prompted for a password. When using the `ssh-agent`, the generated private key is stored with a secure password and saved on secure media. You communicate with another machine by starting the `ssh-agent`, uploading the private key from the secure media, and supplying the password. The private key is not stored on the file system, but is stored in the memory of the `ssh-agent` process.

When using the `ssh-agent`, the private key is stored with the `ssh-agent` that is running only on the Master Server. The public key is distributed to other machines on the network. When an SSH application requires authentication, it communicates with the `ssh-agent` to authenticate. You must turn on `ssh-agent` forwarding when making intermediate SSH connections to enable Local Distributors to proxy to the `ssh-agent` that is running on the Master Server for authentication. `ssh-agent` forwarding allows Local Distributors to authenticate to Local Distributors and Remote Agents that are downstream. This approach provides more security. Also, configuring the `ssh-agent` for use with the N1 Grid Service Provisioning System 5.0 is less complicated than configuring empty passwords.

When using empty passwords, the private key is stored on the file system of the machine without a password. Also, the private key must be present on all machines that initiate SSH communications. In the case of the N1 Grid Service Provisioning System 5.0, all Master Servers and Local Distributors that are connecting to applications downstream using SSH are required to have a private key. This approach provides less security.

SSH Requirements

The N1 Grid Service Provisioning System 5.0 requires the following SSH capabilities:

- Remote command invocation through `ssh`
- Public-private key authentication
- Support for `BatchMode yes` interaction, which is the ability to invoke the `ssh` command without interaction from an operator

If you are using the `ssh-agent`, the following SSH capabilities are required:

- Support for `ssh-agent`.
- Support for `ssh-agent` forwarding in SSH. Use the `-A` option in OpenSSH.

The following capabilities are helpful when configuring machines for SSH connectivity, but are not requirements:

- Force allocate a `tty` when doing remote command invocation. Use the `-t` option in OpenSSH.
- Kill the `ssh-agent`. Use the `-k` option for the `ssh-agent` command in OpenSSH.
- Generate an RSA key for higher security. Use the `-t rsa` in OpenSSH.

Review the following checklist to determine whether an implementation of SSH meets the requirements of the N1 Grid Service Provisioning System 5.0.

- The `ssh-keygen` command must generate a public-private key pair that can be used for authenticating SSH invocations.
- On the specified host, without prompting for any extra information to exchange host keys, obtain a password, etc., when the private key used for authentication was created without a password or with an empty password, the `ssh` command must be able to execute the following:

```
% ssh -o 'BatchMode yes' hostname
```

- After hopping from the current host to `host1` to `host2` to `host3`, on `host3` with the `ssh-agent` running on the current host, uploaded with a private key created with a non-empty password, without prompting for any extra information to exchange host keys, obtain a password, etc., the `ssh` command must be able to execute the following:

```
% ssh -o 'BatchMode yes' -A host1 ssh -o 'BatchMode yes' -A host2
ssh -o 'BatchMode yes' host3
```

- The `ssh` command must be able to correctly pipe its own standard input, output, and error streams to the command being executed on the remote machine.
- The `ssh-add` command must be able to upload private keys with non-empty passwords into the `ssh-agent` so that the private keys can be used for authentication.

Additional SSH Security

When you invoke the Remote Agent through SSH, the Remote Agent uses the `jexec` wrapper to invoke the Java Virtual Machine. This wrapper is a native executable that is owned by root and that has the `setuid` bit set. This file has the same group ID as the user that you used to install the Remote Agent and it gives execute permission to the group. Additionally, the file is stored in a directory that is called `protect` that is owned by the user you used to install the Remote Agent. The file gives execute permission only to the user that owns the Remote Agent. This prevents any other user from being able to execute the `jexec` wrapper.

You must ensure that the file permissions on `jexec` and `protect` are not accidentally changed at any point.

To further tighten security for `jexec`, make any or all of the following changes:

- The JVM executables, usually shell scripts, must be owned by root or the user that owns the application and do not give write permissions to any other users or groups. If you install the JRE with the N1 Grid Service Provisioning System 5.0, ensure that all the files in `N1SPS5.0-home/common/jre` are owned by the user that owns the application and do not give write access to any other users or groups.
- The user ID of the user that owns the application must only be allowed to log in using SSH. When logging in using SSH, only public-key authentication should be allowed. The `/N1SPS5.0-home/.ssh` directory should not give any permissions to any other users or groups.
- The SSH server can be configured to allow only public key authentication by ensuring that the `etc/sshd_config` file contains the following line to disable password authentication.

```
PasswordAuthentication no
```

- Ensure that the `etc/sshd_config` file does not have lines that contain `RhostsRSAAuthentication`, because this is not allowed by default. Also, ensure that `RSAAAuthentication`, if present, is set to `yes`, the default.
- You can further tighten security on the Remote Agent by editing the `/N1SPS5.0-home/.ssh/authorized_keys2` file and prefixing the following text to the line that contains the public key of the Master Server.

```
no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty
```

The `sshd(1M)` man page offers additional details.

Configuring SSH – Process Overview

The following process overview describes the tasks necessary to configure the N1 Grid Service Provisioning System 5.0 to use SSH.

1. Determine whether you want to use empty password keys or the `ssh-agent`.
For more information about choosing an SSH security level, see [“ssh-agent or Empty Password Keys” on page 64](#).
2. Generate the keys on the applications that initiate SSH connections.
See [“How to Generate Key Pairs” on page 68](#).
3. Copy the generated keys to the Local Distributors and the Remote Agents.
From the following list, choose the appropriate task based on whether you are using empty password keys or the `ssh-agent`:
 - [“How to Set Up Keys for the ssh-agent” on page 68](#)
 - [“How to Set Up Keys for Empty Password Files When Using One Key Pair” on page 69](#)
 - [“How to Set Up Keys for Empty Password Files When Using Multiple Key Pairs” on page 70](#)
4. Set up the SSH connectivity. Then, test the connectivity before you start the Master Server.
See [“Setting Up and Testing the Connectivity on the Master Server” on page 71](#).
5. Configure the Local Distributors and Remote Agents to use SSH.
See [“How to Configure SSH for Local Distributors and Remote Agents” on page 73](#).
6. (Optional) If you have any CLI Clients, configure the clients to use SSH.
See [“How to Configure SSH for the CLI Client With the ssh-agent” on page 74](#).

Preparing the Keys

Generate the public-private key pair that will be used to authenticate communication from the Master Server to the Local Distributors and the Remote Agents. Then, copy the generated keys to the Local Distributors and Remote Agents. Choose the appropriate task to complete based on whether you are using the `ssh-agent` or empty password keys.

Note – The following instructions describe how to create keys with the default key lengths. For maximum security, create keys with the longest possible key lengths.

▼ How to Generate Key Pairs

If you are using the `ssh-agent`, you only need to generate one key pair. If you are using empty passwords, you may generate a key pair for each SSH connection that the software makes between two machines. Alternatively, you may generate one single key pair for use by all the connections. Complete this task for each key pair that you want to generate.

Before You Begin Ensure that the user ID and group ID that you are using for the N1 Grid Service Provisioning System 5.0 are the same on all of the servers in the network.

Steps 1. **On the Master Server, or if you are using empty passwords and are generating key pairs for each connection, on the machine that is upstream, generate the keys.**

```
% ssh-keygen -t rsa
```

The server prompts you to save the keys.

2. **Save the keys in the default locations by pressing Return.**

The private key is saved in `/User-home/.ssh/id_rsa`. The public key is saved in `/HOME/.ssh/id_rsa.pub`.

User-home is the home directory of the currently logged in user on the Master Server machine.

The server prompts you for a password.

3. **Determine whether you need to supply a password.**

- If you are using empty password keys, do not supply a password. Press Return to continue.
- If you are using the `ssh-agent`, supply a password for the keys.

▼ How to Set Up Keys for the `ssh-agent`

If you are using the `ssh-agent`, complete this task to copy the keys to the Local Distributors and Remote Agents.

Steps 1. **On the Master Server, copy the private key file, `~/.ssh/id_rsa`, to a secure media.**

```
% cp /User-home/.ssh/id_rsa path_to_file/
```

User-home is the home directory of the currently logged in user on the Master Server machine. *path_to_file/* is the path to the secure media where you want to save the private key file.

2. Delete the private key file from the local file system.

```
% rm /User-home/.ssh/id_rsa
```

3. Copy the public key to each Local Distributor and Remote Agent that you want to set up to use SSH. Save the key in the `~/ .ssh/authorized_keys2` file.

```
% cp /User-home/.ssh/id_rsa.pub /User-home-APP/.ssh/authorized_keys2
```

User-home is the home directory on the Master Server machine. *User-home-APP* is the home directory of the currently logged in user on the Local Distributor or the Remote Agent machine.

4. Ensure that the `.ssh/` directory and any parent directories are not world writable.
5. Change the permissions for the `.ssh/authorized_keys2` file to 600.

6. Edit the following line in the `config.properties` files on the Master Server and the Local Distributors to enable `ssh-agent` forwarding.

Current configuration:

```
net.ssh.args=-o|BatchMode yes
```

Edit the line to include the `-A` option:

```
net.ssh.args=-o|BatchMode yes|-A
```

▼ How to Set Up Keys for Empty Password Files When Using One Key Pair

If you are using empty password files and you generated only one key pair, complete this task to copy the keys to the Local Distributors and Remote Agents.

- Steps**
1. From the Master Server, copy the private key to each machine that is upstream. Save the key in the home directory.

```
% cp /User-home/.ssh/id_rsa /User-home-upstream/.ssh/id_rsa
```

User-home is the home directory of the currently logged in user on the Master Server machine. *User-home-upstream* is the home directory on the machine that is upstream. The upstream machine is the machine that initiates the SSH connection with the machine that is downstream.

Each Local Distributor can have a unique private key, or you can use the same private key for all Local Distributors.

2. Copy the public key to each machine that is downstream. Save the key in the `.ssh/authorized_keys2` file.

```
% cp /HOME-MS/.ssh/id_rsa.pub /HOME-downstream/.ssh/authorized_keys2
```

User-home is the home directory on the Master Server machine.

User-home-downstream is the home directory on the Local Distributor or the Remote Agent machine to which the machine that you set up in the previous step will connect. Copy the public key to all Local Distributors and Remote Agents that connect using SSH.

3. Ensure that the `.ssh/` directory and any parent directories are not world writable.
4. Ensure that the private key file, `.ssh/id_rsa`, is not accessible by other users or groups.
5. Change the permissions for the `.ssh/authorized_keys2` file to 600.

▼ How to Set Up Keys for Empty Password Files When Using Multiple Key Pairs

If you are using empty password files and you generated a key pair for each SSH connection, complete this task to copy the keys to the Local Distributors and Remote Agents.

Before You Begin Complete this task for every SSH connection, therefore every key pair, that is made on the network.

- Steps**
1. From the machine that is upstream, copy the public key to each machine that is downstream. Save the key in the `User-home/.ssh/authorized_keys2` file.

```
% cp /User-home-upstream/.ssh/id_rsa.pub /User-home-downstream/.ssh/authorized_keys2
```

User-home-upstream is the home directory on the machine that is upstream.

User-home-downstream is the home directory on the Local Distributor or the Remote Agent machine to which the upstream machine will connect.

2. Ensure that the `.ssh/` directory and any parent directories are not world writable.
3. Ensure that the private key file, `.ssh/id_rsa`, is not accessible by other users or groups.
4. Change the permissions for the `.ssh/authorized_keys2` file to 600.

Setting Up and Testing the Connectivity on the Master Server

This section describes the initial setup and testing of SSH that must be done before you use SSH with the N1 Grid Service Provisioning System 5.0. If you are using the `ssh-agent`, you will need to start the `ssh-agent` before you begin the setup and testing task.

▼ How to Start the `ssh-agent` on the Master Server

Complete this task only if you are using the `ssh-agent`. Complete this task before you start the Master Server

Note – You must execute all the SSH setup commands in the following setup tasks, `ssh`, `ssh-add`, and `cr_server start`, in the same session as the session that you used to start the `ssh-agent`. If this session is terminated, you must kill the `ssh-agent` program that is running and start a new `ssh-agent` program.

Steps 1. Start the `ssh-agent`.

```
% eval `ssh-agent`
```

The `ssh-agent` starts and sets two environment variables. `SSH_AUTH_SOCK` and `SSH_AGENT_PID` are used by `ssh` and `ssh-add` to connect to the `ssh-agent`.

2. Upload the private key that you generated.

```
% ssh-add path-to-file/
```

path-to-file/ is the path to the secure media where you saved the private key file.

You are prompted to provide a password.

3. Provide the password that you created when you generated the keys.

More Information

Shutting Down the `ssh-agent`

You can shut down the `ssh-agent` by running the command `eval `ssh-agent -k``.

This command uses the `SSH_AGENT_PID` variable to send a signal to the `ssh-agent` process to shut it down. The command also unsets the environment variables that were set when you started the `ssh-agent`.

▼ How to Set Up and Test the Connectivity on the Master Server

Before You Begin

If you are using the `ssh-agent`, be sure to start the `ssh-agent` by following the instructions in “How to Start the `ssh-agent` on the Master Server” on page 71.



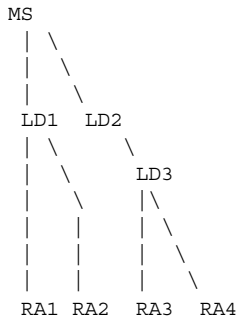
Caution – The setup is session sensitive, so you must execute all the SSH commands, `ssh`, `ssh-add`, and `cr_server start`, in the same session as the session that you used to start the `ssh-agent`. If this session is terminated, you must kill the `ssh-agent` program that is running and start a new `ssh-agent` program. You will also need to upload the private key.

Steps 1. Test the SSH connection paths.

```
% ssh target-host-IP set
% ssh -A -t target-host-IP ls -l
```

Use the `-A` option only if you are using the `ssh-agent`. *target-host-IP* is the IP address for the machine to which this machine will connect.

For example, you might have a network setup with the following Master Server (MS), Local Distributors (LD1, LD2, and LD3), and Remote Agents (RA1, RA2, RA3, and RA4).



For this example network, executing the following commands on the Master Server, substituting the IP addresses of the Local Distributors and Remote Agents on the network for LD1, LD2, RA1, RA2, RA3, and RA4 to test the SSH connection paths.

```
% ssh -A -t LD1 ssh -t RA1 set
% ssh -A -t LD1 ssh -t RA2 set
% ssh -A -t LD2 ssh -A -t LD3 ssh -t RA3 set
% ssh -A -t LD2 ssh -A -t LD3 ssh -t RA4 set
```

These commands follow the paths that the Master Server uses when using SSH to connect to the machines that are downstream. Each command enables SSH to exchange the host keys required for communicating to the machines specified as arguments.

SSH prompts you to allow the host key exchange.

2. **Answer yes to each of the prompts.**
3. **Verify the output of all of the commands to ensure that the environment variables are correctly set up.**
The `PATH` variable should have `/bin`, `/usr/bin`, and any other directories that are part of your environments.
4. **Test the SSH connection paths again.**
Use the same command that you used in Step 1 to test the connection paths again to ensure that the server does not prompt you for any information.

More Information

Repeating Set Up and Testing

If you change any of the keys, you might need to perform this task again. Depending upon your server setup, you also might need to complete this task again whenever you reboot any of the machines.

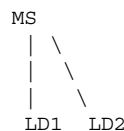
Configuring SSH for the Applications

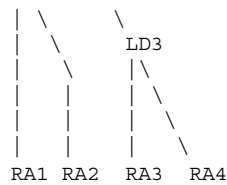
After you set up and test SSH on the Master Server, configure the other machines in the N1 Grid Service Provisioning System 5.0 so that the Master Server can connect to them using SSH.

▼ How to Configure SSH for Local Distributors and Remote Agents

The SSH configuration has must be completed by following the N1 Grid Service Provisioning System 5.0 network from the Master Server to the Remote Agents and configuring the intermediate Local Distributors in the order in which you encounter them. Essentially, this is a preorder traversal of the tree network.

For example, you might have a network setup with the following Master Server (MS), Local Distributors (LD1, LD2, and LD3), and Remote Agents (RA1, RA2, RA3, and RA4).





Configure your network in the following order: LD1, RA1, RA2, LD2, LD3, RA3, RA4. Follow this order strictly and complete the configuration of one machine before moving on to the next machine.

- Steps**
1. Use the Master Server browser interface to view the Host Details page for the machine you want to configure.
 2. Add the connection details in the Local Distributor or the Remote Agent section depending on what application you are configuring on that machine.
 3. Specify the connection type as ssh.
 4. Add the following text in the Advanced Parameters field.

```
cprefix=/N1SPS5.0-Home/application
```

N1SPS5.0-Home is the home directory of the application. *application* is agent if you are configuring a Remote Agent or ld if you are configuring a Local Distributor.

For example, if the N1 Grid Service Provisioning System 5.0 is installed in `/opt/SUNWn1sps/N1_Grid_Service_Provisioning_System_5.0/` and you are configuring a Remote Agent, the text you add to the Advanced Parameters field is:

```
cprefix=/opt/SUNWn1sps/N1_Grid_Service_Provisioning_System_5.0/agent
```

5. Save the Host Details.
6. Ensure that you do not have a Remote Agent or Local Distributor instance running on this machine.
7. Click Test Connection on the Host Details page for this application instance.
8. Repeat this task for each machine in your network.

▼ How to Configure SSH for the CLI Client With the ssh-agent

Complete this task if you want to use SSH connectivity for the CLI Client with the ssh-agent.

- Steps**
1. Create a new operating system user account on the Master Server and the machine on which the CLI Client is installed.

This account should be different from the account that you specified during the installation of the Master Server, Local Distributor, or Remote Agent.

2. **Log in to the Master Server as the new user that you created in the previous step.**
3. **Generate public and private keys for the new user by following the instructions in “How to Generate Key Pairs” on page 68.**

Do not reuse the keys that you generated for communication between the Master Server, Local Distributors, and Remote Agents.

4. **On the Master Server, copy the private key file to a secure media.**

```
% cp /User-home/.ssh/id_rsa path-to-file/.ssh/id_rsa
```

User-home is the home directory of the currently logged in user on the Master Server machine. *path-to-file/* is the path to the secure media where you want to save the private key file.

5. **Delete the private key file from the local file system.**

```
% rm /User-home/.ssh/id_rsa
```

6. **On the Master Server, concatenate the public key to the `.ssh/authorized_keys2` file for that user.**

```
% cat /User-home/.ssh/id_rsa.pub >> /HOME-MS/.ssh/authorized_keys2
```

User-home is the home directory on the Master Server machine.

7. **Log in to the CLI Client machine as the new user that you created.**

8. **Start the `ssh-agent`.**

```
% ssh-agent > /User-home/.ssh/agent_vars
```

User-home is the home directory of the currently logged in user on the CLI Client machine.

9. **Add the following line to the `.profile`, the `.cshrc`, or the `.bash_profile` file.**

```
. /User-home/.ssh/agent_vars
```

User-home is the home directory on the CLI Client machine.

10. **Log out of the Master Server and log back in.**

11. **Upload the private key that you generated.**

```
% ssh-add path-to-file/
```

path-to-file/ is the path to the secure media where you saved the private key file.

The CLI Client now uses SSH and the `ssh-agent` for authentication when connecting to the Master Server.

12. **Configure the Master Server to accept only connections from localhost. For instructions, see “Configuring the JVM Security Policy” on page 99.**

**More
Information**

Stopping the ssh-agent

Note – If you want to stop the ssh-agent, on the CLI Client, use the following command:

```
% eval `ssh-agent -k >User-home/.ssh/agent_vars`
```

User-home is the home directory of the currently logged in user on the CLI Client machine.

▼ How to Configure SSH for the CLI Client With Empty Passwords

Complete this task if you want to use SSH connectivity for the CLI Client with empty passwords.

- Steps**
- 1. Create a new operating system user account on the Master Server and the machine on which the CLI Client is installed.**
This account should be different from the account that you specified during the installation of the Master Server, Local Distributor, or Remote Agent.
 - 2. Log in to the CLI Client machine as the new user that you created in the previous Step.**
 - 3. Generate public and private keys for the new user by following the instructions in “How to Generate Key Pairs” on page 68.**
Do not reuse the keys that you generated for communication between the Master Server, Local Distributors, and Remote Agents.
 - 4. On the CLI Client, copy the public key file to the new user’s `authorized_keys2` file on the Master Server machine.**

```
% cp User-home-CLI/.ssh/id_rsa.pub User-home-MS/.ssh/id_rsa.pub
```

User-home-CLI is the home directory on the CLI Client machine. *User-home-MS* is the home directory on the Master Server machine.
 - 5. On the Master Server, concatenate the public key to the `/.ssh/authorized_keys2` file for that user.**

```
% cat /User-home/.ssh/id_rsa.pub >> /User-home/.ssh/authorized_keys2
```

User-home is the home directory of the currently logged in user on the Master Server machine.
 - 6. Log in to the CLI Client machine as the new user that you created.**

7. Test the SSH connection.

```
% ssh IP-Address-MS set
```

IP-Address-MS is the IP address of the Master Server machine.

You might be prompted to exchange keys.

8. If you are prompted to exchange keys, answer yes.

9. Verify that the `PATH` variable is set correctly.

The `PATH` variable must contain `/bin`, `/usr/bin`, and any other directories that are part of your environment.

10. Configure the Master Server to accept only connections from localhost. For instructions, see [“Configuring the JVM Security Policy” on page 99](#).

SSH Advanced Parameters and Command Reference

Advanced Parameters Reference

On the Host Details page in the Advanced Parameters field, you can specify additional SSH configuration information. The Advanced Parameters that are accepted are as follows. If you want to use more than one parameter, separate the parameters with a comma. Do not add any unnecessary spaces in the Advanced Parameters field.

`cprefix`

The `cprefix` parameter is required for all Local Distributors and Remote Agents. The syntax of the parameter in the Advanced Parameters field is as follows:

```
cprefix=/N1SPS5.0-Home/application
```

N1SPS5.0-Home is the home directory of the application. *application* is agent if you are configuring a Remote Agent or `ld` if you are configuring a Local Distributor.

EXAMPLE 6-1 `cprefix` Example

If the N1 Grid Service Provisioning System 5.0 is installed in `/opt/SUNWn1sps/` and you are configuring a Remote Agent, the text you add to the Advanced Parameters field is:

EXAMPLE 6-1 cprefix Example (Continued)

```
cprefix=/opt/SUNWn1sps/N1_Grid_Service_Provisioning_System/agent
```

ssopath

If you have not added and do not want to add the path to the SSH executable to the PATH on the target server, you can specify the path to the SSH executable with this parameter. The syntax of the parameter in the Advanced Parameters field is as follows:

```
ssopath=path-to-SSH
```

path-to-SSH is the directory in which the SSH executable is installed.

EXAMPLE 6-2 ssopath Example

If the SSH executable is installed in the `/usr/local/bin/ssh` directory, the text that you add to the Advanced Parameters field is:

```
ssopath=/usr/local/bin/ssh
```

sshargs

If you want to supply additional command line arguments to the `ssh` command when it runs on a specific Host, you can supply those arguments in the Advanced Parameters field for that Host. The syntax of the parameter in the Advanced Parameters field is as follows:

```
sshargs=-option | -option
```

option is the command line option that you want supplied to the `ssh` command. Add more than one option by separating the options with a `|`.

EXAMPLE 6-3 sshargs Example

If you want the `ssh` command to enable authentication agent forwarding, supply the `-A` option in the Advanced Parameters field:

```
sshargs=-o|BatchMode yes|-A
```

OpenSSH 2.0 Command Reference

This section describes the OpenSSH 2.0 commands and options that are used in the instructions in this chapter. If you are using a different version of SSH, determine the commands and options that are available in that version of SSH that are equivalent to the following commands. Then, use the equivalent commands when following the instructions to configure SSH.

TABLE 6-1 OpenSSH 2.0 Commands

Tool	Description
<code>ssh</code>	Enables the calling application to invoke another application remotely. When configured to use SSH for communications, the software uses the <code>ssh</code> command to invoke the remote application, either a Remote Agent or a Local Distributor, and uses the standard input and output streams of SSH to communicate with it.
<code>ssh-agent</code>	Used when you want to use private keys with passwords. Upload your keys with the <code>ssh-agent</code> so that SSH invocations of the applications communicate with the <code>ssh-agent</code> for authentication.
<code>ssh-add</code>	Uploads private keys into <code>ssh-agent</code> .
<code>ssh-keygen</code>	Generates the public-private key pair to secure an SSH connection.

The following options can be used with the `ssh` command:

- `-A` Enables authentication agent forwarding
- `-o 'BatchMode yes'` Disables passphrase querying
- `-t` Allocates a `tty` even if a command is given

The following option can be used with the `ssh-keygen` command:

- `-t rsa` Specifies RSA as the type of key to generate.

The following option can be used with the `ssh-agent` command:

- `-k` Kills the agent using the `pid` set in the environment variable `SSH_AGENT_PID`. Other implementations might use a different environment variable.

Configuring the N1 Grid Service Provisioning System 5.0 for SSL

This chapter contains instructions for configuring the N1 Grid Service Provisioning System 5.0 to communicate using Secure Socket Layer (SSL). This chapter discusses the following topics:

- [“Overview of SSL Support in the N1 Grid Service Provisioning System 5.0” on page 81](#)
- [“Configuring SSL – Process Overview” on page 85](#)
- [“Enabling HTTPS Connections from the Master Server Browser Interface” on page 85](#)
- [“Creating Keystores” on page 89](#)
- [“Configuring SSL” on page 91](#)
- [“Sample Configuration Scenarios” on page 93](#)
- [“SSL Cipher Suites” on page 97](#)

Overview of SSL Support in the N1 Grid Service Provisioning System 5.0

SSL is a protocol for securing communication over IP networks. SSL uses TCP/IP sockets technology to exchange messages between a client and a server, while protecting the message with a public and private key encryption system developed by RSA. Support for SSL is included in most web server products, as well as in the Netscape Navigator and Microsoft web browsers.

N1 Grid Service Provisioning System 5.0 applications can be configured to use SSL for their network communications, preventing messages from being read or tampered with. Optionally, applications can be configured to use SSL to authenticate before communicating, further increasing network security.

Cipher Suites: Encryption and Authentication Overview

The SSL protocol supports a variety of different cryptographic algorithms, or ciphers, for use in operations such as authenticating the server and client to each other, transmitting certificates, and establishing session keys. The cipher suite that SSL uses to connect determines whether any authentication takes place.

Exercise caution when selecting cipher suites. Each application must enable only those cipher suites that provide the minimum security needed by the node. SSL uses the most secure cipher suites supported by both the client and server. If low security cipher suites are enabled, a third party client can force the server to use the less secure cipher suites by publishing support for only the least secure cipher suite during cipher suite negotiation.

SSL can be operated in the following modes:

- Encryption only, no authentication – Connections are encrypted. However, SSL does not authenticate the applications that are connecting.
- Server Authentication – Clients authenticate the server to which they are connecting.
- Server and Client Authentication – Both the client and server authenticate each other.

During the installation, when you select to use SSL to secure communications between applications, you are prompted to select the cipher suite to use. The cipher suite value is stored as the value of `net.ssl.cipher.suites` in the `config.properties` file. The cipher suite value is set to the following value based on the selection you make:

- If you select encryption, no authentication, the cipher suite is set to `SSL_DH_anon_WITH_3DES_EDE_CBC_SHA`.
- If you select encryption, with authentication, the cipher suite is set to `SSL_RSA_WITH_3DES_EDE_CBC_SHA`.

When you use SSL with a Local Distributor on an AIX server, the SSL cipher suite is set to encryption with authentication. Encryption with no authentication is not available for Local Distributors that are running on AIX servers.

For lists of SSL cipher suites that do and do not require server authentication, see [“SSL Cipher Suites” on page 97](#). You can configure client authentication only for cipher suites that require server authentication.

Note – The N1 Grid Service Provisioning System 5.0 applications allow you to configure SSL connections with encryption, no authentication or encryption with authentication. Encryption with authentication uses client and server authentication. Although the configurations described above are possible, encryption, with authentication is the most secure.

Authentication Keystores

The N1 Grid Service Provisioning System 5.0 supports self-signed certificates and certificates signed by a Certifying Authority. Two types of keystores exist:

- Private Keystore – The private keystore contains the public-private key pairs that the application uses to authenticate itself when connecting to other applications.
- Trust Keystore – The trust keystore contains the public key, in self-signed certificates, of other applications that the keystore trusts and allows them to connect to the application.

When enabling SSL for client-server authentication, each enabled application needs to be configured with two keystores that SSL will use to authenticate itself to other applications and to authenticate other applications.

When enabling SSL for server-only authentication, the application acting as the SSL server requires a private keystore and the application acting as the SSL client requires a public, or trusted, keystore. The public keystores are in the proprietary JKS format provided by the Java Secure Sockets Extension (JSSE) v1.0.3.

You must specify a password for both of the keystores. The password for both of the keystores must be the same.

For example, application A, an SSL client, and application B, an SSL server, want to connect with each other using SSL. Both are configured to use a cipher suite that requires server authentication. Application B must have a public-private key pair in its private keystore, and application A must have application B's public key in its trust keystore. When application A attempts to connect to application B, application B sends its public key down to application A. Application A is able to verify the public key by finding it in its trust keystore.

If application B is configured to require client authentication, application A must have a public-private key pair in its private keystore. Also, application B must have application A's public key in its trust keystore. After application A has authenticated application B, application B is able to verify application A's public key, as it finds the public key in its trust keystore.

Using Passwords With SSL

If you supply a password for trust keystore operations, the password is only used to verify the integrity of the keystore. The password does not prevent access to the contents of the trust keystore, but it does protect updates to the keystore. Users are not able to change the contents of the keystore without supplying the password.

If you supply a password for private keystore operations, the password is used to verify the integrity of the keystore, protect against modifications of the keystore contents, and to encrypt and protect access to the private key.

The `crkeys` script validates that you specified the same password for both the keystores. When creating a trust store for the first time by importing certificates, the `crkeys` script ensures that the trust store has the same password as the private store, if one exists. Similarly, when creating a private store for the first time, the `crkeys` script ensures that the private store has the same password as the trust store, if one exists.

Limitations of SSL on the N1 Grid Service Provisioning System 5.0

The SSL implementation on the N1 Grid Service Provisioning System 5.0 has the following limitations:

- Both the trust and the private keystores must be configured with the same password. Also, within the private keystore, the key password for each key in the store must be the same as the store password. The `crkeys` script used to create keys enforces this limitation.
- Although enabling client authentication for CLI Client applications is possible, this setup is not supported due to security limitations. The CLI Client applications do not prompt the user for keystore passwords. If the keystores have been created, the keystores must be provided in the CLI Client properties file.
- The N1 Grid Service Provisioning System 5.0 uses single trust keystore for both incoming and outgoing connections. Therefore, if a Master Server connects to a Remote Agent and trusts its public key and if that Remote Agent becomes compromised, that Remote Agent's keys could be used to authenticate the CLI Client to the Master Server, if the CLI Client were to use client authentication. Similarly, if a Local Distributor connects to a Remote Agent and the Remote Agent becomes compromised, the Local Distributor can be used to issue commands to the Master Server.

To secure the Master Server and the Local Distributor against such issues, configure the applications to accept connections only from servers that are expected to connect to them. Permit a Local Distributor to accept connections only from its parent node. Permit the Master Server to accept connections only from the designated CLI hosts. For instructions, see [Chapter 8](#).

- For SSH connections, the remote application, the Local Distributor or Remote Agent, is automatically started. The server does not prompt you for the keystore passwords to start these applications. If the applications are initialized with keystores, the passwords to their keystores must be specified in their properties file.
- When you configure the CLI Client to connect to the Master Server using SSH, the CLI Client connects to the Master Server using an SshProxy application that connects to the Master Server through sockets. The SshProxy can connect to the Master Server through SSL, but this configuration is not supported.

Configuring SSL – Process Overview

The following process overview describes the tasks necessary to configure the N1 Grid Service Provisioning System 5.0 to use SSL.

1. Determine the SSL connectivity that you want to use.
For more information, see [“Overview of SSL Support in the N1 Grid Service Provisioning System 5.0”](#) on page 81.
2. (Optional) Enable the Master Server browser interface to use HTTPS.
See [“Enabling HTTPS Connections from the Master Server Browser Interface”](#) on page 85.
3. Use the `crkeys` command to create keystores.
See [“Creating Keystores”](#) on page 89.
4. Edit the `config.properties` file to configure SSL.
See [“Configuring SSL”](#) on page 91.

Enabling HTTPS Connections from the Master Server Browser Interface

By default, the N1 Grid Service Provisioning System 5.0 browser interface does not use SSL. Requests are performed over HTTP rather than HTTPS. You can enable HTTPS with an SSL Certificate. You can choose whether to have a Certifying Authority sign the certificate or you can use a self-signed certificate.

A certificate signed by a Certifying Authority is trusted by browsers, therefore the browser does not issue a warning when a user connects to the browser interface on the Master Server. Generally, Certifying Authorities charge a fee to sign a certificate.

A self-signed certificate is available for use immediately after you generate the certificate because you do not have to wait for the Certifying Authority to sign it. However, a self-signed certificate is not trusted by the browser, so the browser issues a warning each time a user connects to the Master Server browser interface.

▼ How to Generate SSL Certificates

To enable the browser interface to use SSL, you must first generate an SSL Certificate.

Steps 1. Change to the directory in which you installed the JRE.

```
% cd JAVA-HOME/bin
```

JAVA-HOME is the directory where you installed the JRE. If you installed the JRE with the N1 Grid Service Provisioning System 5.0, the JRE is installed in the *N1SPS5.0-home/common/jre/bin* directory.

2. Generate the certificate.

```
% keytool -genkey -alias tomcat -keyalg RSA -keystore /keystore-location  
-storepass password
```

Set */keystore-location* to the location and filename where you want to store the generated key.

Set *password* to whatever password that you choose.

3. Follow the prompts to complete.

Do not include any punctuation in the name of your organization, otherwise the Java Certificate tool fails when attempting to generate the request. The Common Name (CN) must be set to the fully qualified host name, including the domain name, component of the URI.

▼ How to Obtain a Signature for an SSL Certificate

If you want to use a Certificate signed by a Certifying Authority, follow this procedure to submit the Certificate to the Certifying Authority to be signed.

Steps 1. Generate the Certificate Request.

```
% keytool -certreq -v -alias tomcat -keyalg RSA -keystore /keystore-location
```

/keystore-location is the location and filename where you stored the generated key.

2. Send the Certificate Request to the Certifying Authority.

Follow the instructions provided by the Certifying Authority. The Certifying Authority returns a Certificate Reply.

3. Save the Certificate Reply to a file.

4. Verify the Certificate Reply.

```
% keytool -printcert -file certificate-reply-file
```

certificate-reply-file is the filename of the Certificate Reply that you received from the Certifying Authority.

5. Import the Certificate Reply file to the keystore file.

```
% keytool -v -import -trustcacerts -keystore /keystore-location  
-file certificate-reply-file -alias tomcat
```

/keystore-location is the location and filename where you stored the generated key.
certificate-reply-file is the filename of the Certificate Reply that you received from the Certifying Authority.

6. Verify the imported Certificate Reply.

```
% keytool -v -list -keystore /keystore-location
```

/keystore-location is the location and filename where you stored the generated key.

▼ How to Enable HTTPS Connections from the Master Server Browser Interface

After you have generated an SSL Certificate, and obtained a signature from a Certifying Authority if you chose to do so, you must configure the Master Server browser interface to use SSL.

Steps 1. Stop the Master Server.

```
% N1SPS5.0-MasterServer-home/server/bin/cr_server stop
```

N1SPS5.0-MasterServer-home is the directory where you installed the Master Server.

2. Move the keystore file to the Master Server home directory.

```
%mv /keystore-location N1SPS5.0-MasterServer-home/server/tomcat/
```

/keystore-location is the location and filename where you stored the generated key.
N1SPS5.0-MasterServer-home is the directory where you installed the Master Server.

3. Change to the directory where you moved the keystore file.

```
% cd N1SPS5.0-MasterServer-home/server/tomcat/
```

N1SPS5.0-MasterServer-home is the directory where you installed the Master Server.

4. Set the ownership and permissions on the keystore file:

```
%chmod 600 /keystore-location
```

```
%chown MS_user:MS_group /keystore-location
```

MS_user is the user that owns the Master Server application. *MS_group* is the group that owns the Master Server application. */keystore-location* is the filename where you

stored the generated key.

5. Change to the directory where the Tomcat configuration files are located.

```
% cd /N1SP5.0-MasterServer-home/server/tomcat/conf
```

N1SP5.0-MasterServer-home is the directory where you installed the Master Server.

6. In the `server.xml` file, uncomment the following lines. XML comments begin with `<!--` and end with `-->`.

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
  port="8443" minProcessors="5" maxProcessors="75"
  enableLookups="true"
  acceptCount="10" debug="0" scheme="https" secure="true">
  <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
    clientAuth="false" protocol="TLS"/>
</Connector>
```

7. Edit the Factory element as follows.

```
<Factory className="org.apache.catalina.net.SSLServerSocketFactory"
  clientAuth="false" protocol="TLS"
  keystoreFile="N1SP5.0-MasterServer-home/server/tomcat/keystore-file" keystorePass="password"/>
```

N1SP5.0-MasterServer-home/server/tomcat/keystore-file is the path to the keystore file. *password* is the password that you used to create the original keystore.

Requiring Users to Connect to the Master Server Browser Interface Using SSL

After you have configured the Master Server browser interface to use SSL, you can configure it further so that users must use SSL to connect to the on the N1 Grid Service Provisioning System Master Server.

▼ How to Require Users to Connect to the Master Server Browser Interface Using SSL

Steps 1. Replace the Tomcat `web.xml` file with the secure `web.xml` file.

```
% cd /N1SP5.0-MasterServer-home/server/webapp/WEB-INF
```

```
% cp web.xml.secure web.xml
```

N1SP5.0-MasterServer-home is the directory where you installed the Master Server.

2. Restart the Master Server.

```
% N1SP5.0-MasterServer-home/server/bin/cr_server start
```


N1SPS5.0-MasterServer-home is the directory where you installed the Master Server.

▼ How to Revert to the Original Configuration

Steps 1. Stop the Master Server

```
% N1SPS5.0-MasterServer-home/server/bin/cr_server stop
```

N1SPS5.0-MasterServer-home is the directory where you installed the Master Server.

2. To return to the original configuration, replace the secure `web.xml` file with the default `web.xml` file.

```
% cd N1SPS5.0-MasterServer-home/server/webapp/WEB-INF
```

```
% cp web.xml.default web.xml
```

N1SPS5.0-MasterServer-home is the directory where you installed the Master Server.

3. Restart the Master Server.

```
% N1SPS5.0-MasterServer-home/server/bin/cr_server start
```

N1SPS5.0-MasterServer-home is the directory where you installed the Master Server.

Creating Keystores

The N1 Grid Service Provisioning System 5.0 uses the `keytool` utility provided with the JRE. The `keytool` utility is wrapped in a shell script, `crkeys`, to enable you to create keystores. The script ensures that the correct parameters are supplied to the `keytool` utility.

When you create a keystore, the X.509 Distinguished Name in the self-signed certificate is set to the following:

```
CN=application_name OU=Engineering O=Sun Microsystems Inc L=Menlo Park ST=CA C=US
```

▼ How to Create Keystores

Step ● Generate the keys.

```
% crkeys -options
```

Use the following options to create keystores based on the type of SSL connectivity you want to use.

<code>-alias <i>application_hostname</i></code>	Specifies an alias for the certificate or the key pair. Use the host name of the application as the alias. The alias names must be unique within a keystore.
<code>-cpass</code>	Changes the password of the keystore and all the keys within the keystore.
<code>-delete</code>	Specifies that the key pair or certificate for the specified entity should be deleted from keystore.
<code>-export</code>	Exports a self-signed certificate of the specified entity to the specified file.
<code>-file <i>cert_file</i></code>	Specifies the name of the file that the certificate is to be imported from or exported to.
<code>-generate</code>	Generates a new key pair for the specified alias.
<code>-help</code>	Lists all the options.
<code>-import</code>	Imports a self-signed certificate of an entity that is allowed to connect to this node. When importing the certificate, the host name of the node that this certificate represents should be used as the alias.
<code>-keyalg <i>keyalg</i></code>	The key generation algorithm. Defaults to RSA. Can be either RSA or DSA.
<code>-keysize <i>keysize</i></code>	The key size. Defaults to 1024. Can be any multiple of 64 in the range 512-1024 for DSA keys, and range 512-2048 for RSA keys.
<code>-list</code>	Lists all the entities contained in the keystore.
<code>-new <i>newpassword</i></code>	Specifies the new password for the keystore and all the keys in the keystore. The password must contain at least six characters.
<code>-password <i>password</i></code>	Specifies the password for the keystore. If a password is not specified, the user is prompted for a password. The password must contain at least six characters.
<code>-private</code>	Specifies the private keystore as the target of the operation.
<code>-validity <i>days_valid</i></code>	Number of days the self-signed certificate is valid.
<code>-trust</code>	Specifies the trust keystore as the target of the operation.

Example 7-1 crkeys Command Syntax

The following examples show how to use the `crkeys` command.

To generate a public-private key pair:

```
crkeys -private -generate -alias application_hostname [-keyalg keyalg]  
[-keysize keysize] [-validity days_valid] [-password password]
```

To export the self signed public key for a key pair to a file:

```
crkeys -private -export -file cert_file  
-alias application_hostname [-password password]
```

To import an exported, as shown in the previous example, self signed public key into the trust store:

```
crkeys -trust -import -file cert_file  
-alias application_hostname [-password password]
```

To delete a key or key pair:

```
crkeys {-private|-trust} -delete  
-alias application_hostname [-password password]
```

To list all of the public keys:

```
crkeys {-private|-trust} -list [-password password]
```

To change the SSL keystore, both the trust and the private store, password:

```
crkeys -cpass -password oldpassword  
-new newpassword
```

To print instructions for using the `crkeys` command:

```
crkeys -help
```

Configuring SSL

During the installation, each application is configured to do the following:

- Support cipher suites that require server authentication.
- Do not require client authentication.
- Find the private keystore in the `N1SPS5.0-home/app/data/private.store` file.
- Find the trust keystore in the `N1SPS5.0-home/app/data/trust.store` file.
- Supply empty passwords for each keystore.

You can change the SSL configuration of each application to perform the following security checks:

- Selectively enable cipher suites on each application
You can explicitly specify which cipher suites to enable. If unspecified, the reference implementation uses the cipher suites that are enabled by default. The default cipher suites enabled by the reference implementation require server authentication. For the list of supported cipher suites, see [“SSL Cipher Suites” on page 97](#).
- Specify that the application authenticates the SSL clients that are connecting to it
- Specify the location and password of the private and trust keystores

Note – To enable authentication, you must initialize the keystores after installation of the application.

▼ How to Configure SSL

- Step** ● (Optional) Manually edit the `config.properties` file to change the SSL configuration.

The following table lists the settings in the `config.properties` file that are related to SSL configurations. Change the parameters based on the type of SSL connectivity you want to use.

Parameter	Default Value	Description
<code>net.ssl.cipher.suites</code>	<code>SSL_RSA_WITH_3DES_EDE_CBC_SHA</code>	A comma separated list of SSL cipher suites to enable. For a list of supported SSL Cipher suite, see “SSL Cipher Suites” on page 97 .
<code>net.ssl.client.auth</code>	<code>false</code>	Specifies whether the SSL server should authenticate clients that are connecting to it.
<code>net.ssl.key.store.pass</code>		The keystore password. Required in some instances. See the following for more information.

Note – The `net.ssl.key.store.pass` parameter specifies the SSL keystore password for an N1 Grid Service Provisioning System 5.0 application. Use this parameter when you configure an application with SSL keystores and you do not want to be prompted for the passwords to the keystore when you start the application. You must specify this parameter in the following instances:

- When you setup the N1 Grid Service Provisioning System applications to start automatically when the system boots
 - On Windows servers, N1 Grid Service Provisioning System applications do not prompt for keystore passwords, so this parameter must be specified for any applications configured to use SSL on Windows servers.
 - The CLI application does not prompt for keystore passwords, so this parameter must be specified for any CLI Clients that you configure to use SSL.
 - If a Local Distributor is connected to its parent through an SSH connection, the Local Distributor cannot prompt for passwords.
-

Sample Configuration Scenarios

EXAMPLE 7-2 How to Configure SSL Without Authentication Between the Master Server, Local Distributor, and Remote Agent

1. Install the Master Server, Local Distributor, and Remote Agent and select SSL when the installation program prompts you to select a connection type. When prompted to select a cipher suite, select encryption with no authentication.
2. Add the following property to the `config.properties` file for each application.

```
net.ssl.cipher.suites=SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
```

More than one cipher suite or a different cipher suite can be enabled. To enable multiple cipher suites, set the parameter to a comma separated list of cipher suites.

3. From the browser interface, create a new host.
4. On the host that you just created, add a Local Distributor with the connection type SSL.
5. Test the connection to the Local Distributor.
6. Create a new host.
7. On the host that you just created, add a Remote Agent with the connection type SSL.
8. Test the connection to the Remote Agent.

EXAMPLE 7-3 How to Configure SSL Server Authentication

By default, cipher suites requiring server authentication are enabled, so no change is required in the `config.properties` file to enable cipher suites.

EXAMPLE 7-3 How to Configure SSL Server Authentication (Continued)

1. Generate a key pair for the Local Distributor and store it in the private keystore for the Local Distributor.

```
% ld/bin/crkeys -private -generate -alias ldhostname.cr.com -validity 365
```

2. Export the self-signed certificate from the private keystore on the Local Distributor into a file.

```
% ld/bin/crkeys -private -export -file ld.cert -alias ldhostname.cr.com
```

3. Copy the self-signed certificate for Local Distributor to the Master Server.
4. Import the self-signed certificate into the Master Server trust keystore.

```
% server/bin/crkeys -trust -import -file ld.cert -alias ldhostname.cr.com
```

5. Create a new host.
6. On the new host, add a Local Distributor with the connection type SSL.
7. For the Local Distributor, use the CLI `net .genconfg` command to manually generate the `transport.config` file.

8. Copy the `transport.config` file to the Local Distributor.
9. If already running, stop and the Master Server and the Local Distributor.
10. Start the Master Server and the Local Distributor.

11. Provide the keystore password for the Master Server and Local Distributor.
12. Test the connection to the Local Distributor.

13. Generate a key pair for the Remote Agent and store it in the private store for the Remote Agent.

```
% agent/bin/crkeys -private -generate -alias rahostname.cr.com -validity 365
```

14. Export the self-signed certificate from the private store on the Remote Agent into a file.

```
% agent/bin/crkeys -private -export -file ra.cert -alias rahostname.cr.com
```

15. Copy the self-signed certificate for the Remote Agent to the Local Distributor.
16. Import the self-signed certificate into the Local Distributor trust store.

```
% ld/bin/crkeys -trust -import -file ra.cert -alias rahostname.cr.com
```

17. Create a new host.
18. On the new host, add a Remote Agent with the connection type SSL.
19. For the Remote Agent, use the CLI `net .genconfg` command to manually generate the `transport.config` file.

20. Copy the `transport.config` file to the Remote Agent.
21. If already running, stop the Local Distributor and Remote Agent.
22. Start the Local Distributor and the Remote Agent.
23. Provide the keystore password for the Local Distributor and Remote Agent.

EXAMPLE 7-3 How to Configure SSL Server Authentication (Continued)

24. Test the connection to the Remote Agent.

EXAMPLE 7-4 How to Configure SSL Server and Client Authentication

1. Install the Master Server, Local Distributor, and Remote Agent and select SSL when the installation program prompts you to select a connection type. When prompted to select a cipher suite, select encryption with authentication.
2. Generate a key pair for the Local Distributor and store it in the private store for the Local Distributor.

```
% ld/bin/crkeys -private -generate -alias ldhostname.cr.com -validity 365
```

3. Generate a key pair for the Master Server and store it in the private store for the Master Server.

```
% server/bin/crkeys -private -generate -alias mshostname.cr.com -validity 365
```

4. Export the self-signed certificate from the private store for the Local Distributor into a file.

```
% ld/bin/crkeys -private -export -file ld.cert -alias ldhostname.cr.com
```

5. Copy the self-signed certificate for the Local Distributor to the Master Server.
6. Import the self-signed certificate into the Master Server trust store.

```
% server/bin/crkeys -trust -import -file ld.cert -alias ldhostname.cr.com
```

7. Export the self-signed certificate from the private store for the Master Server into a file.

```
% server/bin/crkeys -private -export -file ms.cert -alias mshostname.cr.com
```

8. Copy the self-signed certificate for the Master Server to the Local Distributor.
9. Import the self-signed certificate into the Local Distributor trust store.

```
% ld/bin/crkeys -trust -import -file ms.cert -alias mshostname.cr.com
```

10. If already running, stop the Master Server and the Local Distributor.

11. Start the Master Server and the Local Distributor.

12. Provide the keystore password for the Master Server and Local Distributor.

13. Create a new host.

14. On the new host, add a Local Distributor with the connection type SSL.

15. Test the connection to the Local Distributor.

16. Generate a key pair for the Remote Agent and store it in the private store for the Remote Agent.

```
% agent/bin/crkeys -private -generate -alias rahostname.cr.com -validity 365
```

17. Export the self-signed certificate from private store for the Remote Agent into a file.

```
% agent/bin/crkeys -private -export -file ra.cert -alias rahostname.cr.com
```

EXAMPLE 7-4 How to Configure SSL Server and Client Authentication (Continued)

18. Copy the self-signed certificate for the Remote Agent to the Local Distributor.

19. Import the self-signed certificate into the Local Distributor trust store.

```
% ld/bin/crkeys -trust -import -file ra.cert -alias rahostname.cr.com
```

20. Copy the self-signed certificate for the Local Distributor, that you exported in Step 4, to the Remote Agent machine.

21. Import the self-signed certificate into the Remote Agent trust store.

```
% agent/bin/crkeys -trust -import -file ld.cert -alias ldhostname.cr.com
```

22. If already running, stop the Local Distributor and Remote Agent.

23. Start the Local Distributor and the Remote Agent.

24. Provide the keystore password for the Local Distributor and Remote Agent.

25. Create a new host.

26. On the new host, add a Remote Agent with the connection type SSL.

27. Test the connection to the Remote Agent.

EXAMPLE 7-5 How to Configure SSL Authentication Between a CLI Client and Master Server

1. Install the Master Server and the CLI Client and select SSL when the installation program prompts you to select a connection type. When prompted to select a cipher suite, select encryption with authentication.

2. Generate a key pair for the Master Server and store it in the private store for the Master Server.

```
% server/bin/crkeys -private -generate -alias mshostname.cr.com -validity 365
```

3. Generate a key pair for the CLI Client and store it in the private store for the CLI Client.

```
% cli/bin/crkeys -private -generate -alias clihostname.cr.com.cr.com -validity 365
```

4. Export the self-signed certificate from the private store for Master Server private store into a file.

```
% server/bin/crkeys -private -export -file ms.cert -alias mshostname.cr.com
```

5. Copy the Master Server self-signed certificate to the CLI Client.

6. Import the self-signed certificate into CLI Client trust store.

```
% cli/bin/crkeys -trust -import -file ms.cert -alias mshostname.cr.com
```

7. Export the self-signed certificate from the private store for CLI Client into a file.

```
% cli/bin/crkeys -private -export -file cli.cert -alias clihostname.cr.com
```

8. Copy the CLI Client self-signed certificate to the Master Server.

9. Import the self-signed certificate into the Master Server trust store.

```
% server/bin/crkeys -trust -import -file cli.cert -alias clihostname.cr.com
```


EXAMPLE 7-5 How to Configure SSL Authentication Between a CLI Client and Master Server (Continued)

10. If the Master Server is running, stop the Master Server.
11. Start the Master Server.
12. Provide the keystore password for the Master Server.
13. On the CLI Client, edit the `config.properties` file to include the following line:

```
net.ssl.key.store.pass=trust-store-password
```

14. Run a CLI Client command to verify the connection.

SSL Cipher Suites

Cipher Suites for Solaris OS, Red Hat Linux, and Windows

The following lists describe the supported SSL cipher suites for Solaris OS, Red Hat Linux, and Windows servers.

The following suites require server authentication:

```
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
```

The following suites do not require server authentication:

```
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_WITH_AES_128_CBC_SHA
```

The following suites require server authentication with no encryption:

SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA

Cipher Suites for IBM AIX

The following lists describe the supported SSL cipher suites for IBM AIX servers.

All of the following cipher suites are available for use with Remote Agents. Cipher suites that do not require server authentication cannot be used for Local Distributors.

The following suites require server authentication:

SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_FIPS_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

The following suites do not require server authentication:

Note – Cipher suites that do not require server authentication cannot be used for Local Distributors.

SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

The following suites require server authentication with no encryption:

SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA

Configuring the Java Virtual Machine Security Policy

This chapter describes how to configure the security policy of the N1 Grid Service Provisioning System 5.0 applications to allow them only to accept connections from a specific IP Address and Port range or to allow them only to connect to a specific IP Address and Port range.

Configuring the JVM Security Policy

Each N1 Grid Service Provisioning System 5.0 application has a Java Virtual Machine (JVM) security policy file located in `lib/security/rox.policy`. This file specifies the permissions assigned to the application. As installed, the policy file allows the application to connect to and accept connections from any host. If you are using the CLI Client with SSH, change the policy file to restrict the connection to only the localhost.

The following line in the `lib/security/rox.policy` file grants these permissions.

```
permission java.net.SocketPermission "*", "connect,accept,listen";
```

If you want to restrict the network access abilities of the application, delete this line and add more restrictive permissions.

The host parameter for `SocketPermission` is as follows:

```
host = hostname | IPaddress :portrange
```

hostname is the host name of the machine. *IPaddress* is the IP address of the machine. *portrange* is the following:

```
portrange = portnumber | -portnumber | portnumber-[portnumber]
```

For more information about the syntax for the security policy file, see <http://java.sun.com/j2se/1.4.2/docs/guide/security/PolicyFiles.html> and click on the Policy File Syntax link.

▼ How to Configure the JVM Policy for the Master Server

- Steps**
1. Edit the `lib/security/rox.policy` file.
 2. Delete the line that allows the application to connect to or accept connections from all hosts.
 3. Add the following lines to give the application permission selectively.

```
permission java.net.SocketPermission "localhost:localport", "accept";
permission java.net.SocketPermission "localhost:dbport", "connect";
permission java.net.SocketPermission "<domain>:httpport", "connect";
permission java.net.SocketPermission "ipAddress1:port1", "connect";
permission java.net.SocketPermission "ipAddress2:port2", "connect"; ...
```

- *localport* is the port that the CLI Client uses to connect to the Master Server. The first line restricts the Master Server to allow CLI Clients to connect only locally or through `ssh-proxy`.
- *dbport* is the port number for the Postgres database server.
- *domain* is the domain of the hosts that are to be allowed to connect to the browser interface. *httpport* is the port number the browser interface.
- *ipAddress1:port1* and *ipAddress2:port2* are the IP address and port numbers of the Remote Agents or Local Distributors that are connected directly to the Master Server.

▼ How to Configure the JVM Policy for the Remote Agent

- Steps**
1. Edit the `lib/security/rox.policy` file.
 2. Delete the line that allows the application to connect to or accept connections from all hosts.
 3. Add the following line to give the application permission.

```
permission java.net.SocketPermission "ipAddress", "accept";
```

ipAddress is the IP address of the Local Distributor or the Master Server to which this Remote Agent is connected.

More Information

Adding Permissions to Connect to a Host

If you plan to execute plans containing steps that require network access, such as `urltest`, you might want to add permissions for this Remote Agent to connect to a particular host.

▼ How to Configure the JVM Policy for the Local Distributor

- Steps**
1. Edit the `lib/security/rox.policy` file.
 2. Delete the line that allows the application to connect to or accept connections from all hosts.
 3. Add the following lines to give the application permission selectively.

```
permission java.net.SocketPermission "ipAddress", "accept";  
permission java.net.SocketPermission "ipAddress1:port1", "connect";  
permission java.net.SocketPermission "ipAddress2:port2", "connect"; ...
```

- `ipAddress` is the IP address of the Local Distributor or Master Server that is the parent of this Local Distributor.
- `ipAddress1:port1` and `ipAddress2:port2` are the IP address and port numbers of the Remote Agents or Local Distributors for which this Local Distributor is the parent.

Postgres Security

Ensure that the Postgres database does not accept connections from other hosts. The default configuration of the Postgres database is to accept connections from UNIX sockets and `localhost`. Change this default setting in the `server/postgres/data/pg_hba.conf` configuration file. Also, change the database password after installation using the `alter user username with password 'password'` query. If you make these changes to the Postgres configuration file, in the `N1SP5.0-MasterServer-home/config/config.properties` file, you must change the value of `db.password`.

Upgrading to the N1 Grid Service Provisioning System 5.0

This chapter contains instructions for upgrading from the 4.1 version of product to the N1 Grid Service Provisioning System 5.0.

Note – If you have a version of the software that was released prior to version 4.1, you must upgrade to version 4.1 before you upgrade to the N1 Grid Service Provisioning System 5.0. If you have a version of the software that was released prior to version 4.0, you must upgrade to version 4.0 before you upgrade to version 4.1.

- [“Upgrading Overview” on page 103](#)
- [“Upgrading the Master Server” on page 105](#)
- [“Upgrading Remote Agents and Local Distributors” on page 111](#)

Upgrading Overview

The upgrade procedure that you complete depends on whether the N1 Service Provisioning System 4.1 is running on an operating system version that is supported for the N1 Grid Service Provisioning System 5.0. Occasionally, new versions of the N1 Grid Service Provisioning System no longer contain support for operating systems that were previously supported.

Upgrading Requirements

When upgrading any of the N1 Grid Service Provisioning System applications, the new server on which you install the 5.0 application must meet the following requirements:

- Operating System – The operating system on which you run the 5.0 application must be the same type of operating system on which you were running the 4.1 application. For example, you can migrate a Master Server running on Red Hat Linux 7.2 to a Master Server running on Red Hat Linux Advanced Server 2.0. You cannot migrate a Master Server running on Red Hat Linux 7.2 to a Master Server running on any version of the Solaris OS.
- Hardware Architecture – The hardware architecture of the server on which you run the 5.0 application must be the same as the architecture on which you were running the 4.1 application. For example, you can upgrade a Remote Agent from a SPARC based server running on the Solaris OS to another SPARC based server running on the Solaris OS. You cannot upgrade a Remote Agent from a SPARC based server running on the Solaris OS to an x86 based server running on the Solaris OS.
- User Ownership of Application – The 5.0 application must be owned by the same user that owns the 4.1 application. For example, if you installed the 4.1 Master Server and assigned ownership to user f00, then the 5.0 Master Server must have user f00 assigned as its owner.

Upgrading – Process Overview

The following process overview describes the tasks necessary to properly upgrade from the N1 Grid Service Provisioning System 4.1 to the N1 Grid Service Provisioning System 5.0.

1. Determine whether the servers that you are upgrading meet the minimum requirements to run the N1 Grid Service Provisioning System 5.0.
See [Chapter 2](#).
2. Choose the Master Server upgrade instructions for your operating system.
 - If you are running the Master Server on Red Hat Linux 7.2, 7.3, or 8.0, follow the instructions in [“How to Upgrade a Master Server From an Operating System That Is No Longer Supported”](#) on page 107.
 - If you are running the Master Server on any other operating system, follow the instructions in [“How to Migrate Master Server Data From Supported Operating Systems”](#) on page 105.
3. Complete the instructions to upgrade the Master Server.
4. Identify any servers that are running Remote Agents and Local Distributors on operating systems that are not supported by the N1 Grid Service Provisioning System 5.0. See, [“Supported Operating Systems”](#) on page 25
5. Upgrade those servers to an operating system that is supported by N1 Grid Service Provisioning System 5.0.
6. Complete the instructions to upgrade the Remote Agents and Local Distributors.
See, [“Upgrading Remote Agents and Local Distributors”](#) on page 111
7. CLI Clients do not need to be upgraded. Simply install the 5.0 version of the CLI Client and uninstall the 4.1 version.

Upgrading the Master Server

The Master Server application is not upgraded like most software is upgraded. Rather, the new version of the Master Server is installed on the same server as the previous version of the Master Server. Then, the data is migrated from the previous version of the Master Server to the new version of the Master Server. The upgrade procedure you complete depends on whether you are running the 4.1 Master Server on an operating system version that is supported by the N1 Grid Service Provisioning System 5.0.

- If you are running the Master Server on Red Hat Linux 7.2, 7.3, or 8.0, which are not supported by the N1 Grid Service Provisioning System 5.0, follow the instructions in [“How to Upgrade a Master Server From an Operating System That Is No Longer Supported”](#) on page 107.
- If you are running the Master Server on any other operating system, follow the instructions in [“How to Migrate Master Server Data From Supported Operating Systems”](#) on page 105.

▼ How to Migrate Master Server Data From Supported Operating Systems

Migrating data from the 4.1 version of the Master Server to the 5.0 version of the Master Server deletes any data in the 5.0 version of the Master Server. The migration script stops both versions of the Master Server until the script completes the migration. The Master Servers will be unavailable for the duration of the migration.

Before You Begin

Verify that the operating system version on the server you want to upgrade is supported by the N1 Grid Service Provisioning System 5.0. For a list of supported operating systems, see [“Supported Operating Systems”](#) on page 25. If the operating system version is no longer supported, follow the instructions in [“How to Upgrade a Master Server From an Operating System That Is No Longer Supported”](#) on page 107.

Back up your data before you migrate. See Chapter 9, “Backing Up and Restoring,” in *N1 Grid Service Provisioning System 5.0 System Administration Guide*.

Steps

1. **Log into the machine as the user who installed the 4.1 version of the Master Server.**
2. **Install the 5.0 version of the Master Server on the same server where the 4.1 version of the Master Server is installed.**
 - If you are running the Solaris OS or Red Hat Linux follow the instructions in [“How to Install the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems”](#) on page 42 to install the N1 Grid Service

Provisioning System 5.0 Master Server.

- If you are running Windows, complete the following steps.
 - a. Stop the 4.1 Master Server by using the Service application in the Windows Administrative Tools to stop the IPC Daemon service.
 - b. Set the 4.1 Master Services to start manually, specifically the IPC Daemon and Server.
 - c. Install the 5.0 version of the Master Server by following the instructions in “How to Install the N1 Grid Service Provisioning System 5.0 Master Server on Windows” on page 51.

Install the 5.0 version of the Master Server with ownership by the same user and group that owns the 4.1 version of the Master Server.

3. For Solaris OS and Red Hat Linux Master Servers, verify that the database will not be optimized during the migration process.

Check that you do not have any `crontab` jobs scheduled that would start a database optimization while you are migrating the data.

4. Access a command prompt.

- On Solaris OS or Red Hat Linux servers, open a shell window and log in as the user that owns the Master Server.
- On Windows, open a Command Prompt window.

5. Change to the directory that contains the migration script.

- On Solaris OS or Red Hat Linux servers, type:

```
% cd /N1SPS5.0-home/server/bin/migrate
```

N1SPS5.0-home is the directory where you installed the Master Server.

- On Windows, type:

```
C:\> cd C:\N1SPS5.0-home\server\bin\migrate
```

C:\N1SPS5.0-home is the directory in which you installed the Master Server.

6. Start the migration script.

- On Solaris OS or Red Hat Linux servers, type:

```
% ./migrateMS_4.1-5.0.sh
```

- On Windows, type:

```
C:\N1SPS5.0-home\5.0\server\bin\migrate\>.\migrateMS_4.1-5.0.cmd
```

7. Follow the instructions on the screen to complete the migration.

When the migration is complete, the following message appears.

```
Master Server migration completed successfully.
```

Note – The listener port numbers for the Postgres database, browser interface, and the Master Server are not migrated. The N1 Grid Service Provisioning System 5.0 Master Server uses the port numbers that you supplied during installation.

8. Check the log file for any errors that might have occurred during migration.

The migration script displays the location of the log file.

9. Clear the cache on the browser that you use to access the Master Server browser interface.

If you started a browser session before upgrading the Master Server, graphics and style sheets that are cached in the browser might prevent you from seeing the upgraded browser interface.

10. Back up the data that you migrated to the new Master Server by using the instructions in Chapter 9, “Backing Up and Restoring,” in *N1 Grid Service Provisioning System 5.0 System Administration Guide*.

You cannot restore data from the 4.1 Master Server to the 5.0 Master Server. Back up the data on the 5.0 Master Server so that you have a complete and accurate backup of the data to use if necessary.

11. (Optional) Uninstall the 4.1 version of the Master Server.

You can uninstall the 4.1 version of the Master Server if you do not want to use it by following the instructions in [Chapter 10](#).

▼ How to Upgrade a Master Server From an Operating System That Is No Longer Supported

Occasionally, new versions of the N1 Grid Service Provisioning System no longer contain support for operating systems that were previously supported. Upgrading the Master Server from a previously supported operating system to a new operating system version requires two phases. In the first phase, the data from the previous version of the Master Server is archived into a file. In the second phase, the data stored in the archive file is migrated into the new version of the Master Server.

- Steps**
- 1. Log into the machine as the user who installed the 4.1 version of the Master Server.**
 - 2. Verify that the database will not be optimized during the migration process.**
Check that you do not have any `cron` jobs scheduled that would start a database optimization while you are migrating the data.
 - 3. Access a command prompt.**

4. Access the migration script.

- If you are migrating using a CD, insert the N1 Grid Service Provisioning System 5.0: IBM-AIX, Red Hat Linux CD.
- If you are migrating using a image that you downloaded, change to the directory where you saved the downloaded image.

5. Change to the directory on the software CD or within the downloaded image where the migration script is located.

```
% cd /migrate
```

6. Copy the migration script to the 4.1 Master Server.

```
% cp migrateMS_4.1-5.0.sh /N1SPS4.1-home/server/bin
```

N1SPS4.1-home is the directory where you installed the 4.1 Master Server.

7. Change to the directory on 4.1 Master Server that contains the migration script that you copied.

```
% cd /N1SPS4.1-home/server/bin
```

8. Create a file that contains the data from the 4.1 Master Server.

```
% ./migrateMS_4.1-5.0.sh -archive /path-to-archive-file/filename
```

path-to-archive-file is the directory in which you want to save the archive file created by the migration script. *filename* is the name that you designate for the archive file.

9. Follow the instructions on the screen to complete the creation of the file.

10. Install the 5.0 version of the Master Server.

- If you are installing the 5.0 Master Server on a new server, follow these steps:
 - a. Install the 5.0 Master Server by following the steps in [Chapter 4](#).
 - b. Copy the archive file that you created in the previous step to the new server.
- If you want to install the 5.0 Master Server on the same server as the 4.1 Master Server, follow these steps:
 - a. Copy the archive file that you created in the previous steps to another directory on the server.
 - b. Uninstall the 4.1 Master Server.
 - c. Upgrade the server to an operating system version that is supported by the N1 Grid Service Provisioning System 5.0. For a list, see [“Supported Operating Systems”](#) on page 25.
 - d. Install the 5.0 Master Server by following the steps in [Chapter 4](#).

11. Change to the directory that contains the migration script.

```
% cd /N1SPS5.0-home/server/bin/migrate
```

12. Start the migration script.

```
% ./migrateMS_4.1-5.0.sh -migrate path-to-archive-file/filename
```

path-to-archive-file is the path that you specified for the migration script to save the file that contains the archived data. *filename* is the name that you designated for the archive file.

13. Follow the instructions on the screen to complete the migration.

When the migration is complete, the following message appears.

```
Master Server migration completed successfully.
```

Note – The listener port numbers for the Postgres database, browser interface, and the Master Server are not migrated. The N1 Grid Service Provisioning System 5.0 Master Server uses the port numbers that you supplied during installation.

14. Check the log file for any errors that might have occurred during migration.

The migration script displays the location of the log file.

15. Clear the cache on the browser that you use to access the Master Server browser interface.

If you started a browser session before upgrading the Master Server, graphics and style sheets that are cached in the browser might prevent you from seeing the upgraded browser interface.

16. Back up the data that you migrated to the new Master Server by using the instructions in Chapter 9, “Backing Up and Restoring,” in *N1 Grid Service Provisioning System 5.0 System Administration Guide*.

You cannot restore data from the 4.1 Master Server to the 5.0 Master Server. Back up the data on the 5.0 Master Server so that you have a complete and accurate backup of the data to use if necessary.

Master Server Data Migration Details

This section describes details about the data that is migrated from the previous version of the Master Server to the new version of the Master Server.

Master Server Data Migration

The following table details the types of data that are migrated on the Master Server.

TABLE 9-1 Migration Overview

Data on the Master Server	Is the Data Migrated?	Mechanism for Migration
PostgreSQL data	Yes	SQL scripts
CLI Client script for changes to existing commands	No	
Migration of objects serialized through CLI Client	No	
Migration of changes to the <code>config.properties</code> file on each host	Yes	Properties listed in the file are migrated using the details found in “Migration Details for the Properties File” on page 110.
Resource migration	Yes	Copy the resources directory.
Logger Configuration file	No	
User interface customizations	No	

Migration Details for the Properties File

The 4.1 `config.properties` file is migrated to the 5.0 `config.properties` file. During the migration, the value of each property in the 4.1 file is compared to the value of the property in the 5.0 `config.properties` file. If the value is the same, the property is ignored. If the value is different, then the 4.1 value is copied to the 5.0 `config.properties` file. If a property exists in the 4.1 file and is absent in the 5.0 file, then the 4.1 value is added to the 5.0 file. Values for the following properties are not migrated to the 5.0 `config.properties` file:

- `webserver.TomcatHome`
- `rsrc.localrepo`
- `db.port`
- `hostdb.ms.ipaddress`
- `hostdb.ms.port`
- `note.mailsubject`
- `net.server.nconn`
- `net.server.type.1`
- `net.server.ip.1`
- `net.server.port.1`
- `net.server.parms.1`
- `note.url`
- `pe.defaultUserToRunAs`
- `hostdb.ms.connectiontype`
- `pe.maxSimulPlans`

If you have changed the values for any of these properties in the 4.1 properties file, you need to manually change the value in the 5.0 `config.properties` file.

Upgrading Remote Agents and Local Distributors

The N1 Grid Service Provisioning System 5.0 provides an automatic upgrade utility that allows you to upgrade Remote Agents and Local Distributors by using the browser interface to the Master Server. Before you use the automatic utility, all of the Remote Agents and Local Distributors must be running on operating system versions that are supported by the N1 Grid Service Provisioning System 5.0. If you begin an automatic upgrade and receive an error message indicating that some Remote Agents or Local Distributors were not upgraded because the operating system version is not supported, you will need to manually upgrade the Remote Agents and Local Distributors on those servers. See [“How to Manually Upgrade Remote Agents and Local Distributors From an Operating System That Is No Longer Supported”](#) on page 112.

▼ How to Upgrade Remote Agents and Local Distributors

If you are running Remote Agents and Local Distributors on an operating system version that is not supported by the N1 Grid Service Provisioning System 5.0, you first upgrade the server to an operating system that is supported by both the 4.1 and 5.0 versions of the N1 Grid Service Provisioning System. Then, you use the browser interface to upgrade all of the Remote Agents and Local Distributors in your network. After the applications have been upgraded, you can then upgrade your servers to numerically higher versions of the operating system, if they are supported by the N1 Grid Service Provisioning System 5.0.

For example, you are running a 4.1 Remote Agent on a Red Hat Linux 7.1 server and you want to upgrade that server to Red Hat Linux 3.0 Advanced Server. First, you need to upgrade the server to Red Hat Linux Advanced Server 2.1, which is supported by both the 4.1 and 5.0 versions of the N1 Grid Service Provisioning System. Second, upgrade all of the Remote Agents by using the browser interface to the Master Server. Finally, upgrade the server to Red Hat Linux 3.0.

Before You Begin Migrate the Master Server before upgrading Remote Agents and Local Distributors.

- Steps**
1. **Identify any server that is running the 4.1 Remote Agent or Local Distributor on an operating system that is not supported by the N1 Grid Service Provisioning System 5.0.**

For a list of supported operating systems, see [“Supported Operating Systems”](#) on page 25.

2. **On each server that is running the 4.1 Remote Agent or Local Distributor on an operating system that is not supported by the N1 Grid Service Provisioning System 5.0, upgrade the operating system to a version that is supported by both the 4.1 and 5.0 versions of the N1 Grid Service Provisioning System.**

3. **Log in to the browser interface of the N1 Grid Service Provisioning System 5.0 Master Server.**

4. **Click Hosts.**

5. **Click masterserver.**

6. **Click the Update Entire N1 SPS network... button.**

A window opens and displays a list of hosts that are being upgraded. The progress of the upgrade is also displayed. When the process completes, the window displays the following message.

Host Update not yet complete.

7. **Click the Close button.**

8. **To complete the second phase of the upgrade, click the Update Entire N1 SPS network... button again.**

A window displays a list of hosts that are being upgraded. The progress of the upgrade is also displayed. When the process completes, the status for each of the hosts displays as Updated.

9. **Click the Close button.**

The upgrade is complete.

10. **Prepare the Hosts that you upgraded.**

Before you can run a Plan on a Host that you upgraded, you must Prepare the Host. To Prepare Hosts, follow the instructions in "How to Prepare a Physical Host" in *N1 Grid Service Provisioning System 5.0 System Administration Guide* .

11. **(Optional) If you want to upgrade the operating system on your servers to a numerically higher version, you may do so.**

The version to which you upgrade the operating system must be supported by the N1 Grid Service Provisioning System 5.0.

▼ How to Manually Upgrade Remote Agents and Local Distributors From an Operating System That Is No Longer Supported

If you did not upgrade servers running operating systems that are no longer supported by the N1 Grid Service Provisioning System 5.0 before you automatically upgraded the Remote Agents and Local Distributors, you need to manually upgrade those systems.

Steps 1. On the server that is running the 4.1 Remote Agent or Local Distributor that you want to upgrade, log into the machine as the user who installed the 4.1 version of the Remote Agent or Local Distributor.

2. Change to the directory that contains the application scripts.

```
% cd /N1SPS4.1-home/app/bin/
```

N1SPS4.1-home is the directory where you installed the application.

app is agent for the Remote Agent and *ld* for the Local Distributor.

3. Stop the 4.1 Remote Agent or Local Distributor.

```
% ./cr_app stop
```

app is agent for the Remote Agent and *ld* for the Local Distributor.

4. Verify that the 4.1 Remote Agent or Local Distributor is not automatically started upon system reboot by system start up scripts.

5. Upgrade the operating system on the server to a version that the N1 Grid Service Provisioning System 5.0 supports.

6. Move the 4.1 Remote Agent or Local Distributor to a temporary location on the server.

```
% mv /N1SPS4.1-home/app /temporary_directory
```

N1SPS4.1-home is the directory where you installed the application.

app is agent for the Remote Agent and *ld* for the Local Distributor.

temporary_directory is the temporary directory in which to move the application.

7. Install the 5.0 Remote Agent or Local Distributor in the same directory where the 4.1 application had been installed.

For instructions, see [“How to Install the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems”](#) on page 42.

8. Change to the directory that contains the scripts for the 5.0 Remote Agent or Local Distributor.

```
% cd /N1SPS5.0-home/app/bin/
```

N1SPS5.0-home is the directory where you installed the application.

app is agent for the Remote Agent and *ld* for the Local Distributor.

9. Migrate the data to the 5.0 Remote Agent or Local Distributor.

```
% ./migrateNode_4.1-5.0.sh -n /N1SPS5.0-home/app -o /temporary_directory/N1SPS4.1-home/app
```

N1SPS5.0-home is the directory where you installed the 5.0 application.

/temporary_directory/N1SPS4.1-home is the directory to which you moved the 4.1 application.

app is agent for the Remote Agent and *ld* for the Local Distributor.

The migration script migrates the following files:

- `config.properties`
- `transport.config`
- `keystores`
- snapshots on the Remote Agent

10. Start the 5.0 Remote Agent or Local Distributor.

```
% ./cr_app start
```

app is agent for the Remote Agent and *ld* for the Local Distributor.

Uninstalling the N1 Grid Service Provisioning System 5.0

This chapter describes procedures for uninstalling the N1 Grid Service Provisioning System 5.0 in the following sections:

- [“Uninstalling Applications on Solaris OS, Red Hat, and IBM AIX Systems”](#) on page 115
- [“Uninstalling Applications on Windows Systems”](#) on page 118

Uninstalling Applications on Solaris OS, Red Hat, and IBM AIX Systems

The procedure to uninstall the N1 Grid Service Provisioning System 5.0 depends upon the application you want to install and on which operating system it is running.

- If you want to uninstall the Solaris OS Master Server or CLI Client, use the instructions in [“How to Uninstall a Solaris OS Master Server or CLI Client”](#) on page 115.
- If you want to uninstall the Solaris OS Remote Agent or Local Distributor or any of the applications on Red Hat or IBM AIX servers, use the instructions in [“How to Uninstall File-Based Applications on Solaris OS, Red Hat Linux, and IBM AIX Systems”](#) on page 116.

▼ How to Uninstall a Solaris OS Master Server or CLI Client

The Solaris OS Master Server and CLI Client are installed as packages. The uninstall script removes only 5.0 versions of the Master Server or CLI Client.

Steps 1. On the server that you want to uninstall the application, verify that you are not in the directory of the application that you want to uninstall.

2. Begin the uninstallation.

```
# /N1SPS5.0-home/app_directory/bin/cr_uninstall_app.sh
```

N1SPS5.0-home is the directory where you installed the application. The default directory is

```
/opt/SUNWn1sps/N1_Grid_Service_Provisioning_System_5.0.
```

app_directory is one of the following values:

- *server* – uninstalls a Master Server
- *cli* – uninstalls a CLI Client

app is one of the following values:

- *ms* – uninstalls the Master Server
- *cli* – uninstalls the CLI Client

The following message appears when the uninstallation is complete.

```
Successfully removed SUNWspapp  
Successfully removed SUNWspsc1  
Successfully removed SUNWspsj1
```

app is *ms* when uninstalling a Master Server and *cl* when uninstalling a CLI Client.

Note – The *SUNWspsc1* and *SUNWspsj1* packages are not removed if another application is installed on this server. For example, if you have a Master Server and a CLI Client both installed on the same server, when you uninstall only the Master Server, the *SUNWspsc* and *SUNWspsj1* packages remain on the server until you uninstall the CLI Client.

▼ How to Uninstall File-Based Applications on Solaris OS, Red Hat Linux, and IBM AIX Systems

Steps 1. On the server that you want to uninstall the application, verify that you are not in the directory of the application you want to uninstall.

2. Stop the application that you want to uninstall.

3. If you are uninstalling a Remote Agent, change the permissions on files in the */protect* directory.

```
% chmod -R 755 /N1SPS5.0-home/agent/bin/protect
```

N1SPS5.0-home is the directory where you installed the Remote Agent.

4. Delete the directory that contains the application that you want to uninstall.

```
# rm -r /N1SPS5.0-home/app-directory
```

N1SPS5.0-home is the directory where you installed the application. The default directory on Solaris OS and AIX is `/opt/SUNWn1sps/`. The default directory on Red Hat Linux is `/opt/sun.app-directory` is one of the following values:

- `server` – uninstalls a Master Server
- `agent` – uninstalls a Remote Agent
- `cli` – uninstalls a CLI Client
- `ld` – uninstalls a Local Distributor

5. **If you are uninstalling all of the applications from the machine, when the *N1SPS5.0-home* directory contains no more application directories, delete the `common/` directory.**

```
# rm -r N1SPS5.0-home/common
```

The uninstallation is complete.

▼ How to Disable Automatic Database Optimization

If you uninstall a Red Hat Linux Master Server, you must manually remove the entry from the `crontab` file that instructs the system to automatically optimize the database. The uninstall script for Solaris Master Servers automatically removes this entry from the `cronjob` file.

- Steps**
1. **As the user that owns the Master Server, list the current `crontab` and direct the output to a file.**

```
# crontab -l > newcrontabfile
```

2. **Open the `newcrontab` file in a text editor.**

3. **Remove the following line from the `newcrontab` file.**

```
MM HH * * * N1SPS5.0-home/server/bin/roxdbcmd vacuumdb -d rox > /dev/null 2> /dev/null
```

N1SPS5.0-home is the home directory of the Master Server.

4. **Save the `newcrontab` file.**

5. **Update the `crontab`.**

```
# crontab newcrontabfile
```

Uninstalling Applications on Windows Systems

To uninstall applications on Windows servers, use the Add and Remove Programs function available in the Windows Control Panel. When you perform an uninstallation, ensure that the Microsoft Management Console with Services snap-in, also known as the Services console, is not open. Otherwise, the Master Server, Remote Agent, or Local Distributor might not uninstall properly.

Installation and Configuration Reference

This appendix contains details about the installation of the N1 Grid Service Provisioning System 5.0 in the following sections:

- “Reference Data for the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems” on page 119
- “Reference Data for the N1 Grid Service Provisioning System 5.0 on Windows” on page 125

Reference Data for the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX Systems

This section contains details about the installation of the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX. The topics include the following sections:

- “Directory Structure of the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX” on page 120
- “Database Optimization on Solaris OS, Red Hat Linux, and IBM AIX Systems” on page 122
- “Sample Remote Agent Parameters File for Solaris OS, Red Hat Linux, and IBM AIX Systems” on page 123

Directory Structure of the N1 Grid Service Provisioning System 5.0 on Solaris OS, Red Hat Linux, and IBM AIX

When installing the N1 Grid Service Provisioning System 5.0, you are prompted to select a home directory for the software. The default directory on Solaris OS and AIX servers is `/opt/SUNWn1sps`. The default directory on Red Hat Linux servers is `/opt/sun`. The installation program creates the following directory tree within the home directory:

- `N1_Grid_Service_Provisioning_System_5.0` is the directory created for the Master Server and CLI Client that contains the software.
- `N1_Grid_Service_Provisioning_System` is the directory created for the Local Distributor and Remote Agent that contains the software.

The installation scripts install the N1 Grid Service Provisioning System 5.0 software into default destination directories that are subdirectories of the home directory for the software. All directories are created with the permissions set to 755, `rwxr-xr-x`, except when noted in the tables below. Most files are assigned with the permissions set to 644, `rw-r--r`, except for executable files and scripts, which are set to 755.

The following table lists the directories that are installed for every N1 Grid Service Provisioning System 5.0 application, the Master Server, Local Distributor, Remote Agent, and CLI Client.

TABLE A-1 Directories Common to All Applications

Directory	Contents
<code>/common</code>	Common files for all applications
<code>/common/jre</code>	Bundled copy of platform-specific JRE
<code>/common/lib</code>	Library files common for some or all applications

The following table lists the directories installed for the Master Server.

TABLE A-2 Directories Installed for the Master Server

Directory	Contents
<code>/server/config</code>	Master Server configuration files
<code>/server/custom</code>	User interface customization files
<code>/server/data</code>	Master Server data files
<code>/server/bin</code>	Master Server executable files

TABLE A-2 Directories Installed for the Master Server (Continued)

Directory	Contents
/server/lib	Master Server-specific library files
/server/postgres	Bundled copy of Postgres
/server/tomcat	Bundled copy of Apache Tomcat
/server/webapp	Browser Interface Web Application
/server/setup	Miscellaneous files used to initialize the Master Server
/server/config/proxy/config	Command line user interface SSH proxy properties file
/server/data/tmp	Master Server temporary directory with permissions set to 777
/server/README	Text license agreement

The following table lists the directories installed for the Local Distributor.

TABLE A-3 Directories Installed for the Local Distributor

Directory	Contents
/ld/config	Local Distributor configuration files
/ld/bin	Local Distributor executable files
/ld/lib	Local Distributor library files
/ld/data	Local Distributor specific data
/ld/data/tmp	Local Distributor temporary directory with permissions set to 777
/ld/jvm/jre/bin	Local Distributor JRE proxy
/ld/README	Text license agreement

The following table lists the directories installed for the Remote Agent.

TABLE A-4 Directories Installed for the Remote Agent

Directory	Contents
/agent/config	Remote Agent configuration files
/agent/bin	Remote Agent executable files
/agent/bin/protect	Jexec directory with permissions set to 100, --x-----

TABLE A-4 Directories Installed for the Remote Agent (Continued)

Directory	Contents
/agent/bin/protect/jexec	Jexec is used when the agent needs root permissions with permissions set to 4110
/agent/lib	Remote Agent library files
/agent/data	Remote Agent specific data
/agent/work	Default directory for execution of execNatives.
/agent/data/tmp	Remote Agent temporary directory with permissions set to 777
/agent/jvm/jre/bin	Remote Agent JRE proxy
/agent/README	Text license agreement

The following table lists the directories installed for the CLI Client.

TABLE A-5 Directories Installed for the CLI Client

Directory	Contents
/cli/config	CLI configuration files
/cli/bin	CLI executable files
/cli/lib	CLI library files
/cli/data	CLI specific data
/cli/data/tmp	CLI temporary directory with permissions set to 777
/cli/README	Text license agreement

Database Optimization on Solaris OS, Red Hat Linux, and IBM AIX Systems

The installation program prompts you to set up database optimization daily. If you select to optimize the database daily, the installation script adds the following command to the cronjob file. You can add this command to the cronjob file at any time to begin daily optimization of the database.

```
MM HH * * * N1SP5.0-home/server/bin/roxdbcmd vacuumdb -d rox > /dev/null 2> /dev/null
```

N1SP5.0-home is the home directory of the Master Server.

Sample Remote Agent Parameters File for Solaris OS, Red Hat Linux, and IBM AIX Systems

A sample parameters file is installed on the Master Server in the `/server/bin` directory, along with other scripts, when you install the Master Server. You can use this file to indicate configuration selections so that you can non-interactively install the Remote Agent. The contents of the sample parameters file are shown below.

```
# This is a sample file that sets the parameters required
# for the remote installation of Remote Agents.
#
# This file must be uncommented and edited with the correct
# values before it can be used.
# $Id: cr_ra_remote_params.sh,v 1.2 2004/09/15 18:39:01 echiquet Exp $

# CR_RA_INSTALLBASE - the base directory where the
# Remote Agent will be installed. If the directory
# does not exist, the installer will attempt to create it.
# Defaults to /opt/SUNWn1sps
#
CR_RA_INSTALLBASE=/opt/SUNWn1sps

# CR_RA_OWNER - The owner of the distribution. A pre-existing
# user must be specified. Defaults to 'n1sps'.
#
CR_RA_OWNER=n1sps

# CR_RA_GROUP - The group owner of the distribution. A
# pre-existing group name must be specified. Defaults to 'n1sps'.
#
CR_RA_GROUP=n1sps

# CR_RA_PORT - Port number that the Remote Agent will listen on.
# An integer value between 1024 and 65535 must be specified. Defaults
# to 1131.
#
CR_RA_PORT=1131

# CR_RA_CTYPE - Parent connection type. How the parent connects to
# this RA. One of 'raw' (unencrypted), 'ssh', or 'ssl'. There is no default.
# This parameter is required.
#
#CR_RA_CTYPE=raw

# CR_RA_CIPHER_TYPE - SSL cipher suite type. One of '1' (encryption,
# no authentication) or '2' (encryption, with authentication).
# Default is 1, but has no effect for parent connection type of raw or
# ssh.
#
CR_RA_CIPHER_TYPE=1

# CR_RA_INSTALL_JRE - Directive of whether or not a JRE should be
# installed with the Remote Agent for it's use. Defaults to 'y'. Valid
# values are 'y' or 'n'.
```

```

#
CR_RA_INSTALL_JRE=y

# JRE_HOME - Directive for the location of the JRE installation. If
# the CR_RA_INSTALL_JRE directive is set to 'y', the installer will
# install the JRE. In this case, the JRE_HOME value will be
# $CR_RA_INSTALLBASE/common/jre. If the installer is not going to
# install the JRE, the JRE_HOME should point to where the pre-existing JRE
# is installed.
#
JRE_HOME=$CR_RA_INSTALLBASE/N1_Grid_Service_Provisioning_System/common/jre

# CR_RA_SUID - Directive of whether or not the RA should be installed
# with the setuid root privileges. Valid values are 'y' or 'n'. This
# only works when the remote installer is run as the root user.
# There is no default. This parameter is required.
#
#CR_RA_SUID=y

# CR_RA_INSTALLER_USER - The user that should perform this install. This
# is what the remote installer will use to ssh into the remote hosts
# and run the commands as. It is highly recommended that this be set to
# root, although, it doesn't have to be. Defaults to the current user.
#
CR_RA_INSTALLER_USER=root

# CR_RA_INSTALLER_WORKDIR - The directory to use to store temporary files.
# The distribution will be copied into this directory so make sure
# that this it has enough space to store the distribution file. Defaults to
# /tmp
#
CR_RA_INSTALLER_WORKDIR=/tmp

# CR_RA_INSTALLER_LEAVEFILES - Directive of whether or not the temporary
# files should be preserved on the remote host. Defaults to 'n'.
#
CR_RA_INSTALLER_LEAVEFILES=n

# CR_RA_INSTALLER_HOSTS - List of remote hosts on which the Remote Agent is
# to be installed. This must contain at least one host name. This host list
# can also be set in the environment variable 'CR_RA_INSTALLER_HOSTS', or
# specified on the command line. Check the remote agent installer script
# usage message for exactly how this can be done.
#
# Note : The format of the list of hosts is critical. The list of hosts
# must be separated by a comma (',') and cannot have any spaces in between.
# It must be in one contiguous string.
#
CR_RA_INSTALLER_HOSTS=""

export CR_RA_INSTALLBASE CR_RA_PORT CR_RA_GROUP CR_RA_OWNER CR_RA_INSTALL_JRE CR_RA_SUID
export CR_RA_CTYPE CR_RA_CIPHER_TYPE
export CR_RA_INSTALLER_USER CR_RA_INSTALLER_WORKDIR CR_RA_INSTALLER_LEAVEFILES
export CR_RA_INSTALLER_HOSTS JRE_HOME

```

CR_RA_ALLOWFORWARDVERSION Parameter

If you want to install an N1 Grid Service Provisioning System 5.0 Remote Agent on a version of an operating system that is numerically higher than the highest version the N1 Grid Service Provisioning System 5.0 supports for that operating system, add the following parameter to the parameters file:

```
CR_RA_ALLOWFORWARDVERSION=y
```

If you use the `CR_RA_ALLOWFORWARDVERSION=y` parameter, the installation program does not verify that the operating system on which you are installing the Remote Agent is supported. There is no standard Sun Services support for use of the N1 Grid Service Provisioning System 5.0 on unsupported operating systems.



Caution – Installing the N1 Grid Service Provisioning System 5.0 on unsupported operating systems might result in undefined and unexpected behavior. Install the N1 Grid Service Provisioning System 5.0 on unsupported operating systems only for testing purposes. Do not use the N1 Grid Service Provisioning System 5.0 on unsupported operating systems in a production environment.

Reference Data for the N1 Grid Service Provisioning System 5.0 on Windows

This section contains details about the installation of the N1 Grid Service Provisioning System 5.0 on Windows in the following sections:

- [“Directory Structure of the N1 Grid Service Provisioning System 5.0 on Windows” on page 125](#)
- [“Cygwin” on page 128](#)
- [“Actions Performed by the Windows Installation Scripts” on page 128](#)

Directory Structure of the N1 Grid Service Provisioning System 5.0 on Windows

When installing the N1 Grid Service Provisioning System 5.0, you are prompted to select a home directory for the software. The default directory is one of the following.

- `C:\Program Files\N1 Grid Service Provisioning System\5.0` is the directory created for the Master Server and CLI Client that contains the software.
- `C:\Program Files\N1 Grid Service Provisioning System` is the directory created for the Local Distributor and Remote Agent that contains the software.

The installation scripts install the N1 Grid Service Provisioning System 5.0 software into default destination directories that are subdirectories of the home directory for the software. The following table lists the directories that are installed for every N1 Grid Service Provisioning System 5.0 application, the Master Server, Local Distributor, Remote Agent, and CLI Client.

TABLE A-6 Directories Common to All Applications

Directory	Contents
\common	Common files for all applications
\common\jre	Bundled copy of the JRE for Windows
\common\lib	Library files common for some or all applications

The following table lists the directories installed for the Master Server.

TABLE A-7 Directories Installed for the Master Server

Directory	Contents
\server\config	Master Server Configuration files
\server\data	Master Server data files
\server\bin	Master Server Executable files
\server\lib	Master Server-specific library files
\server\postgres	Bundled copy of Postgres
\server\cygwin	Bundled subset of Red Hat cygwin
\server\tomcat	Bundled copy of Apache Tomcat
\server\webapp	Browser Interface Web Application
\server\setup	Miscellaneous files used to initialize the Master Server
\server\data\tmp	Master Server temporary directory with permissions set to 777
\server\README	Text license agreement

The following table lists the directories installed for the Local Distributor.

TABLE A-8 Directories Installed for the Local Distributor

Directory	Contents
\ld\config	Local Distributor configuration files

TABLE A-8 Directories Installed for the Local Distributor (Continued)

Directory	Contents
\ld\bin	Local Distributor executable files
\ld\lib	Local Distributor library files
\ld\data	Local Distributor-specific data
\ld\data\tmp	Local Distributor temporary directory
\ld\jvm\jre\bin	Local Distributor JRE proxy
\ld\README	Text license agreement

The following table lists the directories installed for the Remote Agent.

TABLE A-9 Directories Installed for the Remote Agent

Directory	Contents
\agent\config	Remote Agent configuration files
\agent\bin	Remote Agent executable files
\agent\lib	Remote Agent library files
\agent\data	Remote Agent-specific data
\agent\work	Default directory for execution of execNatives
\agent\data\tmp	Remote Agent temporary directory
\agent\jvm\jre\bin	Remote Agent JRE proxy
\agent\README	Text license agreement

The following table lists the directories installed for the CLI Client.

TABLE A-10 Directories Installed for the CLI Client

Directory	Contents
\cli\config	CLI configuration files
\cli\bin	CLI executable files
\cli\lib	CLI library files
\cli\data	CLI specific data
\cli\data\tmp	CLI temporary directory with permissions set to 777
\cli\README	Text license agreement

Cygwin

To facilitate interoperability with applications running on Solaris OS, Red Hat Linux, and IBM AIX servers, the Windows version of the software includes a subset of the Red Hat `cygwin` UNIX environment. The following description of `cygwin` comes from the official Cygwin web site at <http://www.cygwin.com>.

Cygwin is a UNIX environment, developed by Red Hat, for Windows. It consists of two parts: - A DLL (`cygwin1.dll`) which acts as a UNIX emulation layer providing substantial UNIX API functionality. - A collection of tools, ported from UNIX, which provide UNIX/Linux look and feel. The Cygwin DLL works with all non-beta, non "release candidate", ix86 versions of Windows since Windows 95, with the exception of Windows CE.

Actions Performed by the Windows Installation Scripts

The Windows Master Server installation script performs the following actions:

- Copies all installation contents to the directories you specified.
- Sets up the registry entries for the proper mount points for `cygwin`.
- Registers the `cygipc` service.
- Registers the postmaster service with a dependency on the `cygipc` service.
- Registers the Master Server service with a dependency on the postmaster service.
- Creates a Start menu shortcut.
- If you selected SSL as a communications protocol, runs scripts to generate the configuration files that are needed for SSL.

The Windows Local Distributor installation script performs the following actions:

- Copies the installation contents to the directories you specified.
- If you selected SSL as a communications protocol, runs scripts to generate the configuration files that are needed for SSL.
- Registers the Local Distributor service.
- Creates a Start menu shortcut.
- If you requested that the installation script start the Local Distributor, starts the Local Distributor.

The Windows Remote Agent installation script performs the following actions:

- Copies the installation contents to the directories you specified.
- If you selected SSL as a communications protocol, it runs scripts to generate the configuration files that are needed for SSL.
- Registers the Remote Agent service.

- Creates a Start menu shortcut.

The Windows CLI Client installation script performs the following actions:

- Copies the installation contents to the directories you specified.
- If you selected SSL as a communications protocol, runs scripts to generate the configuration files that are needed for SSL.
- Creates a Start menu shortcut.

Troubleshooting

This appendix provides troubleshooting information for installation and configuration of the N1 Grid Service Provisioning System 5.0.

- “Issues During Installation on Solaris OS, Red Hat Linux, and IBM AIX” on page 131
- “Issues During Installation on Microsoft Windows” on page 132
- “SSH Connectivity” on page 132

Issues During Installation on Solaris OS, Red Hat Linux, and IBM AIX

Warning When Installing the JRE on IBM AIX

If the installation script detects any JRE instances already installed in the common directory on an AIX machine, the following warning appears:

```
WARNING: Overwriting the JRE can result in installation
problems when libraries from this JRE are cached by the
OS. If you have used, or are running another CenterRun
module that uses this JRE, you should stop that other
module, and run /usr/sbin/slibclean as root.
```

```
Do you wish to continue installation?
(default: y) [y,n]
```

When a JRE is installed on an AIX machine, AIX caches native libraries from the JRE in memory. When these libraries are cached, they are locked on disk. Trying to install a new JRE over the locked libraries creates errors.

Do not install a new version of the JRE. When prompted to install the JRE, choose no. Then, provide a path to the JRE that is already installed on the machine.

Issues During Installation on Microsoft Windows

Error When Installing on Windows

When installing on a Windows server, the following message appears:

```
!\ Internal Error 2755.
```

The error occurs when you do not have write permissions on the directory in which the MSI packages are saved. To complete the installation, change the permissions on the directory to include write permissions for the user that is running the installation program. Restart the installation.

SSH Connectivity

Master Server Unable to Connect to Local Distributor Through an Intermediate Local Distributor

If the Master Server is unable to connect to another machine and displays a TTL expiry error after you use the Host Details page to update the configuration of that machine or any machine upstream, you might need to manually generate the `transport.config` file for some or all of the intermediate Local Distributors between that machine and the Master Server. Test the connection to each of the upstream Local Distributors of the problem machine by moving from the problem machine to the Master Server. For the Local Distributor to which you can successfully connect that is closest to the problem machine, regenerate the `transport.config` file and all of its downstream Local Distributors. Use the CLI Client `net.gencfg` command to generate `transport.config` files.

Unable to Connect to an Application Using SSH

If you are experiencing problems connecting to a machine after configuring the N1 Grid Service Provisioning System 5.0 to use SSH, follow the steps below to troubleshoot the problem.

▼ How to Troubleshoot SSH Connectivity Issues

Before You Begin If you are using `ssh-agent`, complete this task from the same session as the session that you used to start the `ssh-agent`.

Steps 1. On the upstream machine, test the connection to the downstream machine.

- To test the machine immediately downstream from the upstream machine, use the following command:

```
# ssh target-IPaddress ls -l
```

target-IPaddress is the IP address of the machine that is the furthest downstream that you want to test.

- If you are using `ssh-agent`, to test a machine that is more than one other machine downstream from the machine on which you are running the `ssh-agent`, use the following command:

```
# ssh -A target-IPaddress-parentmachine  
ssh -A target-IPaddress-parentmachine ssh -A target-IPaddress ls -l
```

```
# ssh -A ssh -A target-machine-n-IPaddress ssh -A target-machine-2-IPaddress  
ssh -A target-machine-1-IPaddress ssh -A target-IPaddress ls -l
```

target-machine-n-IPaddress are the IP addresses of the upstream Local Distributor machines of the machine being tested in the specified in order. For example, 1 is the machine that is closest to the machine being tested and n is the machine that is right before the Master Server. *target-IPaddress* is the IP address of the machine that is the furthest downstream that you want to test.

target-IPaddress-parentmachine is the IP address of any machine that is between the upstream machine and the downstream machine for which you are testing connectivity.

If you are prompted for information, supply the information. Try the test again.

If you are not prompted for information, continue to the next step.

2. On the upstream machine, in the `logger_config.xml` file, before the `<root>` section, insert the following lines to enable logging with `priority="debug"`:

```
<category name="SSH.STDERR">  
<priority value="debug" />  
</category>  
<category name="com.raplax.rolloutexpress.net.transport.SshClientConnectionHandler">  
<priority value="debug" />
```

</category>

Wait for the upstream machine to read the log file updates.

3. Test the connection again using the command that you used in Step 1.

Examine the log output on the command line and in the `SSH.STDERR` log. Correct any problems found in the log files and try the test again.

Examine the application log output on the upstream machine for the SSH command line you used to invoke the downstream application and the `stderr` output of the SSH command. Correct any problems identified by the logged messages and try the test again.

If you do not find any problems in the log files, the upstream machine might be connecting properly to the downstream machine, but the application is not starting properly. Continue to the next step.

4. Examine the ROX log file for errors starting the application on the downstream machine.

- On Red Hat Linux and IBM AIX machines, examine the `/tmp/ROXappnumbers.log` file.
- On Solaris OS machines, examine the `/var/tmp/ROXappnumbers.log` file.

app is the application on the downstream machine that you are testing. Use Agent for a Remote Agent, Dist for a Local Distributor, and Proxy for a CLI Client. *numbers* are randomly generated numbers that are included in the file name.

5. Correct any errors found in the log file.

Glossary

abstract component	A component that serves only as a base component for other components to extend. An abstract component cannot be installed and only an abstract component is permitted to declare abstract child elements.
call compatibility	A compatibility type for system service components. This compatibility is also called API compatibility or interface compatibility.
category	A general class in which you can group objects that are stored in multiple folders.
child component	A component that is referenced by a container component. Also called <i>contained component</i> . See also <i>container component</i> .
comparison	A feature that searches for and identifies differences between hosts and component models. The N1 Grid Service Provisioning System supports these three types of comparisons: <ul style="list-style-type: none">■ Model to model – Examines the deployment repository and history that is stored on the master server for two hosts and reports any differences■ Model to install – Compares what the master server reports is installed on a host to what is actually on the host and reports any differences■ Install to install – Examines the contents of two hosts' file systems and reports any differences
component	A logical grouping of source information that defines an application. A component also includes a set of instructions that specifies how to manage the source information. The XML representation of a component includes the following:

	<ul style="list-style-type: none"> ■ List of resources used by the application ■ Installation steps ■ Uninstallation steps ■ Dependencies
component compatibility	A situation where a component can be safely replaced by another. The N1 Grid Service Provisioning System supports two kinds of component compatibility: call compatibility and install compatibility.
component inheritance	The means by which a component obtains attributes and behavior from another component. When you create a component, it inherits any variables, snapshots, and procedures from the associated component type.
component procedure	A program in a component that controls deployment of the component, such as installation, uninstallation, management, and capturing snapshots. Management procedures are defined in the control block.
component repository	A location on the master server where components and their resources are checked in.
component type	A special kind of component that encapsulates behavior that can be reused by other components. A component can inherit the behavior of a component type by extending from it.
component variable	A user-definable name-value pair that is used to make parts of a component accessible and configurable by objects that are external to the component.
composite component	A component that contains only references to other components, both simple and composite. A composite component cannot contain any resources.
composite plan	A plan that is composed solely of subplans, which can be simple or composite subplans. A composite plan is not directly targeted, as each subplan can run on a different set of targets.
configuration generation engine	A software engine on the master server that replaces substitution variable references with the appropriate variable setting values. The engine interacts with the host repository and component repository to resolve values any time that you run a plan to deploy a component.
contained component	A component that is referenced by other components.
container component	A component that contains references to other components.
control	A procedure defined by a component that can be used to manage the deployed applications. For example, a control might be used to start or stop an application. Also called <i>control service</i> .

deployment	Using a plan or component procedure to act on a component. The component's lifecycle includes installation, uninstallation, and application management.
direct-run procedure	A component procedure that can be run directly from the component by using the browser interface.
downstream	In the N1 Grid Service Provisioning System 5.0 network hierarchy, the server that is further from the master server. For example, the master server connects downstream to a local distributor. Any remote agents connected to the local distributor are downstream from the local distributor.
execNative call	An optional call out to custom scripts from the XML of a plan or component.
execution plan	See <i>plan</i> .
extend	To base a component on a component type so that the component inherits variables and procedures that are defined by the component type. The component can override variable values and procedure definitions defined by its associated component type.
final component	A component that cannot be extended by another component.
folder	Directory-like containers that enable you to apply permissions to and organize components, plans, and subfolders.
gold server	A reference server that contains files, directories, and other resources that make up an application and that checks in these resources to the master server.
host	A server that is managed by the N1 Grid Service Provisioning System.
host set	A user-defined, logical grouping of hosts that share one or more common attributes, such as physical location or functional group. Use a host set to quickly and easily update applications on all hosts in the set. You can also use a host set to perform model-to-install comparisons between two hosts.
host type	A base class of servers that is bound by a set of common attributes, all of which are user-defined. You can use host types to categorize hosts into logical groupings and to facilitate host searches.
host search	A query run on the host repository that yields a list of hosts whose attributes match those specified by the query. For example, you can use host searches to create a list of hosts that have the same host type, that run the same applications, and that are configured with the same subnet masks.
install compatibility	A compatibility type for component types. This compatibility is also called structural compatibility.

Java Runtime Environment (JRE)	A subset of the Java Development Kit (JDK [®]) for users and developers who want to redistribute the runtime environment. The Java runtime environment consists of the Java virtual machine (JVM), the Java core classes, and supporting files.
Java Virtual Machine (JVM)	The part of the Java runtime environment (JRE) responsible for interpreting bytecodes.
Jython	An implementation of the high-level, dynamic, object-oriented language, Python, seamlessly integrated with the Java platform. The predecessor to Jython, JPython, is certified as 100% pure Java.
label	A means of marking a component version beyond the N1 Grid Service Provisioning System version number. For example, a component version number describes the version of the component. A label can describe the version of the application that the component represents.
local distributor	<p>The application that is installed on a server. The Local Distributor application acts as a link between other servers in the N1 Grid Service Provisioning System in the following ways:</p> <ul style="list-style-type: none"> ■ master server to remote agents ■ master server to other local distributors ■ local distributor to remote agents <p>Local distributors maximize bandwidth efficiency and speed, and can also provide secure network connections for navigating restricted environments.</p>
master server	The application that is installed on a server that manages the N1 Grid Service Provisioning System. The Master Server application can connect to any of the data center environments managed by the N1 Grid Service Provisioning System. The Master Server provides centralized data storage, data processing, and user interfaces.
modeling	To create components and plans that represent an application that you want to deploy with the N1 Grid Service Provisioning System.
nested component	A contained component that, when installed, can provide its services only to its container component. A nested contained component defines a finer-grained unit of functionality required by the container component, but is not otherwise useful to other components.
network protocol	A way to transmit data between devices on a network. The N1 Grid Service Provisioning System uses TCP/IP, SSH, and SSL.
notification email	An email sent by the N1 Grid Service Provisioning System to advise that a system, administrative, or custom event has occurred. The system administrator specifies the rules used to determine when notification emails are sent and the email addresses to which the email is sent.

notification rule	The criteria used by the N1 Grid Service Provisioning System to determine whether an email notification is sent. The system administrator defines the criteria that is used to determine when an email notification is sent.
parent component	A component that contains references to other components. Also called <i>container component</i> . See also <i>contained component</i> .
physical host	A physical server that is connected to the network. Within the provisioning system, a physical host can act as a remote agent or a local distributor.
plan	A sequence of instructions that is used to manipulate one or more components. A plan can also be a sequence of other plans, which enables common instruction sequences to be shared between one or more plans.
plan executor	The software engine on the master server that runs preflights and deployments.
preflight	The simulated execution of a plan to a simulated UNIX environment that finds and reports any errors or potential errors that might affect the deployment. A preflight always precedes a deployment, but you can run a preflight as a standalone operation.
procedure	See <i>component procedure</i> .
provisioning system	The software applications that, when installed on servers, form the N1 Grid Service Provisioning System.
remote agent	The application that is installed on any server in the N1 Grid Service Provisioning System to which components are deployed. The Remote Agent application manages tasks, such as installing software, controlling services, and collecting information to deliver to the master server.
resource	A file that is deployed to a host when a plan is executed. The file might be a directory, a symbolic link, or another kind of file.
server	A computer that manages resources and supplies services to a client. In the N1 Grid Service Provisioning System, a server is a computer on which one of the N1 Grid Service Provisioning System applications has been installed.
session	A period of time that is initiated when you log in. A session persists until you log out or inactivity causes the session to expire. Logically, a session represents the authenticated credentials of a particular user. A session is used to identify the user throughout a series of related requests without reauthentication.

session variable	A variable that is associated with a user session. The user can change session variable values for each login session. Session variable values can also be securely saved for reuse in subsequent sessions.
simple component	A component that contains a single resource. A simple component cannot contain references to other components.
simple plan	A sequential list of steps that are executed on a particular set of target servers. A simple plan does not contain or call other plans.
snapshot	A capture of the resources that are stored on a host during a deployment. The snapshot is used when performing comparisons between a host and its model on the master server (model-to-install).
step	An instruction that can be part of a plan or a component.
substitution variable	A variable that appears in plans, components, or configuration files that is substituted by the configuration generation engine during deployment.
system service	A component that is automatically deployed to all applicable hosts when the hosts are prepared. System services define utility controls and resources that can be used by other components.
targetable component	A component that creates a host that serves as a deployment target for other components when it is installed. When a targetable component is uninstalled, the host it created is automatically deleted.
top-level component	A contained component that, when installed, can be used by any component just as if it had been directly installed by a plan. A top-level contained component defines services that will be used by the container component as well as by other components.
upstream	In the N1 Grid Service Provisioning System network hierarchy, the server that is closer to the master server. For example, the master server is upstream from the local distributor. The local distributor is upstream from any remote agents that are connected to that local distributor.
variable	See <i>component variable</i> .
variable settings	A collection of variable values that can be used to override the default values of one or more component variables. Based on the variable settings that you use, you can specify different values for component variables. You specify the variable settings to use when you run a plan.
virtual host	Services that act as a host for other services. For example, a virtual host can represent an application server that acts as a host for web applications.
XML schema	The language used by the N1 Grid Service Provisioning System to create plans and components.

Index

C

CLI (Command Line Interface) Client
 application directory structure, 122, 127-128
 description, 20-21
 installing, 42-43, 54-55
 running, 49
 system requirements
 IBM AIX, 31
 Red Hat Linux, 31
 Solaris OS, 30
 Windows, 32
 uninstalling, 115-116, 116-117, 118
 upgrading, 104

D

directory structure
 Solaris OS, Red Hat Linux, IBM
 AIX, 120-122
 Windows, 125-128

H

hardware requirements, 29-32

I

installing
 interactively, 42-43, 51-54, 54-55
 JRE (Java Runtime Environment), 33-34

installing (Continued)
 overview, 17-18
 pre-install decisions, 33-39

J

Java Virtual Machine, 66
jexec, 66
JRE (Java Runtime Environment), 33-34
 troubleshooting, 131-132
Jython, 36

L

Local Distributor
 application directory structure, 121, 126-127
 description, 19-20
 installing, 42-43, 54-55
 running, 49
 system requirements
 IBM AIX, 31
 Red Hat Linux, 31
 Solaris OS, 30
 Windows, 32
 uninstalling, 116-117, 118
 upgrading, 111-114

M

Master Server
application directory structure, 120-121, 126
description, 19
installing, 42-43, 51-54
running, 49
system requirements
 Red Hat Linux, 30-31
 Solaris OS, 29-30
 Windows, 32
uninstalling, 115-116, 116-117, 118
upgrading, 105-110
migrating, *See* upgrading

N

non-interactive installing
instructions, 44-46, 55-56
Remote Agent sample parameters
file, 123-125
Windows variable values, 59-60

P

product overview, 19-21

R

Remote Agent
application directory structure, 121-122, 127
description, 20
installing
 interactively, 42-43, 54-55
 non-interactively, 44-46, 55-56
 remotely, 46-49, 57-59
running, 49
sample parameters file, 123-125
system requirements
 IBM AIX, 31
 Red Hat Linux, 31
 Solaris OS, 30
 Windows, 32
uninstalling, 116-117, 118
upgrading, 111-114
Windows variable values, 59-60

remotely installing
instructions, 46-49, 57-59
Windows variable values, 59-60
running applications, 49

S

security
database, 101
JVM security policy, 99-101
overview, 21-22
SSH (Secure Shell)
additional security, 66
commands, 78-79
configuration process, 67
jexec, 66
overview, 22, 64-66
system requirement, 28
troubleshooting, 132-134
SSL (Secure Socket Layer)
cipher suites, 97-98
configuration examples, 93-97
configuration process, 85
overview, 81-85
SSL (Secure Sockets Layer), overview, 22
starting applications, *See* running applications
system requirements
hardware
 IBM AIX servers, 31
 Red Hat Linux servers, 30-31
 Solaris OS servers, 29-30
 Windows servers, 31-32
operating system versions, 25-26
operating systems
 patches, 26-28
web browsers, 26

U

uninstalling, 115-117, 118
upgrading
instructions, 105-110, 111-114
overview, 104

W

web browser requirements, 26

