Opsware System 4.7 Installation Guide

Corporate Headquarters

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.
T + 1 408.744.7300 F +1 408.744.7383 www.opsware.com

Table of Contents

Preface

Welcome to Opsware System 4.7 – an enterprise-class software solution that enables customers to get all the benefits of Opsware Inc.'s data center automation platform and support services. The Opsware System provides a core foundation for automating formerly manual tasks associated with the deployment, support, and growth of server and server application infrastructure.

About this Guide

This guide describes how to use the Opsware Installer to install the software components that make up an Opsware core. It provides information about the hardware and software required for installation, including information about how to configure an Oracle database for use with the Opsware System software.

This guide is intended for database administrators who will prepare the database for use with the Opsware System and for Unix system administrators who will perform the Opsware System installation.

Contents of this Guide

This guide contains the following chapters:

Chapter 1: Opsware System Overview – provides an overview description of the Opsware System architecture, how the Opsware System components interact, and a description of the types of installations – standalone core and multimaster core installations.

Chapter 2: Opsware Installer Operation – provides information about how the Opsware Installer runs, including the installer scripts, log files, command line syntax, and how the Opsware Installer is distributed on DVD and across CD-ROMs.

Chapter 3: Installation Prerequisites – provides information on the information you must gather and the decisions you must make before you install the Opsware System software. It also provides information about the Opsware System requirements for installing the Oracle database.

Chapter 4: Opsware Core Scalability – provides a guide to determining how many servers you will need to run the Opsware core based on the metrics in your facility and how to correctly distribute the components for the core across the servers.

Chapter 5: Opsware Standalone Installation – provides information on the tasks required to install a standalone core.

Chapter 6: Opsware System Configuration – after installing an Opsware core, provides information about setting several configuration parameter values that the Opsware System uses to send email notifications and alerts, and to display the Opsware administrator contact information.

Chapter 7: OS Provisioning Configuration – provides information about required network configuration so that you can use the Opsware OS Provisioning Subsystem to install operating systems on managed servers.

Chapter 8: Opsware Multimaster Installation – provides information on the tasks required to upgrade a standalone core to multimaster, install target facilities, and configure TIBCO for communication between the facilities.

Chapter 9: TIBCO Configuration for Multimaster – provides information about the required setup and configuration for the TIBCO Certified Messaging system so that multimaster Opsware cores transport transaction data (messages) between Model Repositories at different facilities.

Chapter 10: Software Repository Replication – describes how to set up the Software Repository Replicator to enable backup functionality for Software Repositories running in a multimaster mesh.

Chapter 11: Opsware Core Uninstallation – provides information on the tasks required to un-install a standalone core, describes how to remove a core from a multimaster mesh, and how to un-install an entire Opsware System made up of multiple cores in different facilities.

Conventions in this Guide

This guide uses the following typographical and formatting conventions.

NOTATION	DESCRIPTION
Bold	Defines terms.
Italics	Identifies guide titles and provides emphasis.
`Courier`	Identifies text of displayed messages and other output from Opsware programs or tools.
`Courier Bold`	Identifies user-entered text (commands or information).
`Courier Italics`	Identifies variable user-entered text on the command line or within example files.

Icons in this Guide

This guide uses the following icons to highlight important information.

ICON	DESCRIPTION
	This icon is a note. It identifies especially important concepts that warrant added emphasis.
	This icon is a requirement. It identifies a task that must be performed before an action under discussion can be performed.
	This icon is a tip. It identifies information that can help simplify or clarify tasks.
	This icon is a warning. It is used to identify significant information that must be read before proceeding.

Guides in the Documentation Set and Who Should Read Them

Opsware System 4.5 User's Guide is intended to be read by the system administrator who is responsible for performing the day-to-day functions of managing servers, provisioning operating systems, uploading packages, setting up the Software Tree and node hierarchies, attaching software applications and installing them on servers, managing patches, reconciling servers with software, creating and executing scripts, tracking configuration, and deploying and rolling back code and content.

Opsware System 4.7 Administration Guide is intended to be read by Opsware administrators who will be responsible for setting up accounts for users, creating user groups and additional Opsware administrators, assigning permissions for different levels of operation and access, adding customers and facilities, and monitoring and diagnosing the health of the Opsware System components.

Opsware System 4.7 Installation Guide is intended to be used by system administrators who are responsible for the installation of the Opsware System in a facility. It documents how to run the Opsware Installer, and how to configure each of the components.

How to Read the Installation Guide

This *Opsware System 4.7 Installation Guide* documents how to run the Opsware Installer to install the Opsware System in a facility. Running the Opsware Installer installs the Opsware System components to the point where they are operational and running.

This *Opsware System 4.7 Installation Guide* also documents how to complete required Opsware System configuration so that the Opsware System functions properly.

This *Opsware System 4.7 Installation Guide* does *not* document how to begin setting up the system after it is installed so that end users can start managing servers in the operational environment.

See the following guides and chapters to continue setting up the Opsware System:

- To create user accounts for the people in your organization, see the *Opsware System 4.7 Administration Guide*.
- To add new customer accounts to the Opsware System to associate managed servers with different departments, see the *Opsware System 4.7 Administration Guide*.
- To set up OS provisioning so that you can use the Opsware System to install operating systems on new servers, see the *Opsware System 4.5 User's Guide*.

Running the Opsware Installer installs the OS Provisioning Subsystem; however, you must perform additional set up tasks so that it installs specific operating systems.

- To set up automated patch management so that you can use the Opsware System to patch Opsware-managed servers, see the *Opsware System 4.5 User's Guide*.

  Running the Opsware Installer will install the Patch Management Subsystem; however, you must perform additional set up tasks so that it patches specific operating systems and applications.

- To set up application provisioning with the Opsware System, see the *Opsware System 4.5 User's Guide*.

  Running the Opsware Installer installs the Application Provisioning Subsystem; however, you must perform additional set up tasks so that it installs specific applications on Opsware-managed servers.

- To install Opsware Agents on the existing servers in your operational environment, see the *Opsware System 4.5 User's Guide*.

- To install the Opsware Command Line Interface to use with the Opsware System, see the *Opsware System 4.5 User's Guide*.

Chapter 1: Opsware System Overview

IN THIS CHAPTER

This chapter provides the following information:

- A high-level overview of the Opsware System components and a description of the interaction between the components
- Information about the types of Opsware System installations
- High-level overviews of the process for each type of installation

Description of Opsware System Components

The Opsware System utilizes an agent-server architecture. Each server under management has an Opsware Agent that can perform tasks remotely. The server portion of the Opsware System consists of multiple, integrated components, each with a unique purpose. Whenever the Opsware System needs to enact change on servers or query servers, it sends requests to the Opsware Agents.

The Opsware System is made up of the following components:

- Model Repository – the Opsware System data repository that stores information about the hardware and software deployed in the operational environment
- Access & Authentication Directory – the authentication directory that stores user account information
- Opsware Documentation - the Opsware Command Center Help
- Opsware Command Center – the primary user interface to the Opsware System
- Web Services Data Access Engine – a Web services interface to the Model Repository

  When you install the Opsware Command Center on a server, the Opsware Installer automatically installs the Web Services Data Access Engine on the same server where you are installing the Opsware Command Center.
- Data Access Engine – an XML-RPC interface to the Model Repository

- Software Repository – the central repository for all software that the Opsware technology manages
- Command Engine – a system for running distributed programs across many servers
- OS Provisioning Build Scripts – scripts (located on the Opsware Build Manager) that control the way that a Sun Solaris, a Red Hat Linux, or a Microsoft Windows operating system is installed on a server
- OS Provisioning Build Manager – part of the OS provisioning Subsystem, manages the OS installation process by communicating with the OS Build Agent and other Opsware core components

  The Opsware Build Manager is installed automatically on the same server by the Opsware Installer when you install the OS Provisioning Build Scripts.
- OS Provisioning Boot Server – the server that controls the initial bootstrap process for bare metal servers that boot over the Opsware core network, which installs OS Build Agents on the servers and causes them to appear in the Server Pool in the Opsware Command Center
- OS Provisioning Media Server – the server that contains the OS media (installation software from vendors for Sun Solaris, Red Hat Linux, and Microsoft Windows operating systems) so that the OS Provisioning Subsystem can access the media over the network
- Multimaster Infrastructure Components – an application (installed on the server running the Model Repository) that propagates and synchronizes changes from each Model Repository in each Opsware core to all other Model Repositories in a multimaster mesh

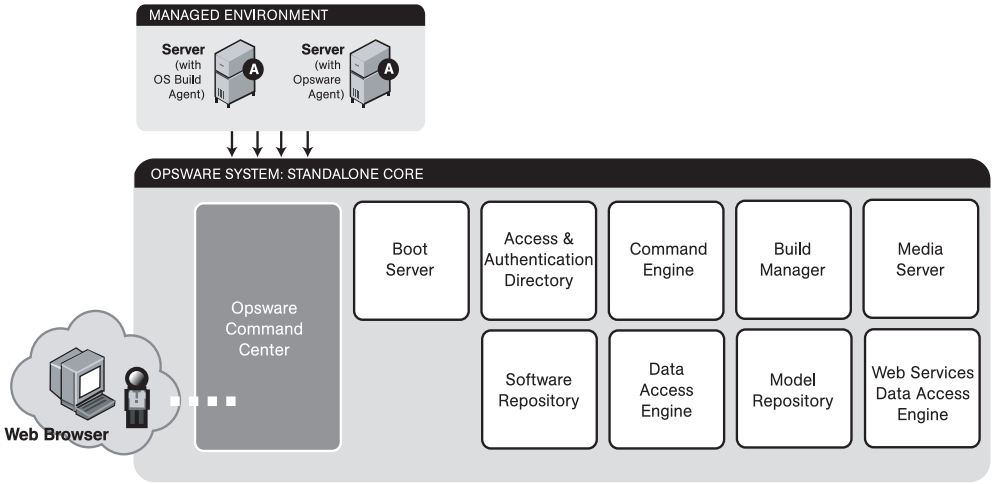
Opsware System Architecture

The Opsware System has the following general interaction between components:

- The Opsware Command Center, Command Engine, Access & Authentication Directory, Software Repository, and Opsware Agent interact with the Model Repository through the Data Access Engine.
- The Data Access Engine issues queries against the Model Repository. It does not cache query results.
- The Software Repository contacts the Model Repository to map the client's IP address to the customer name. The Software Repository performs this mapping to enforce access rules on customer-specific files.

Figure 1-1 shows these components. See the *Opsware System 4.7 Administration Guide* for information about how the Opsware System components interact.

Figure 1-1: Opsware System Component Architecture



Types of Opsware System Installations

The following installation types are supported:

- Standalone Opsware Core
- Converting a Standalone Opsware Core to a Multimaster Core
- Multimaster Opsware Core – Subsequent Core

A **standalone** installation is performed for a facility that a single Opsware core manages.

A **multimaster** installation is performed for multiple facilities that two or more multimaster Opsware cores manage. A multimaster installation allows you to centralize management of several facilities while at the same time providing the performance benefits of having a local copy of key Opsware System data at each of the facilities.

This guide uses the term *facility* to refer to the collection of servers and devices that a single Opsware core manages. A facility can be all or part of a data center, server room, or computer lab.

Standalone Installation Overview

A standalone installation involves installing a single Opsware core in a facility. The standalone installation process consists of the following tasks:

1. Installing and configuring an Oracle database. A properly configured Oracle database instance must be running and a listener must be active when you run the Opsware Installer scripts
2. Setting up your network and domain name system to resolve Opsware host names
3. Running the Opsware Installer script to install the Opsware System components

   The script prompts you for information about your environment, such as database passwords and how to identify the facility.
4. Setting initial Opsware System configuration parameters though the Opsware Command Center

Multimaster Installation Overview

A multimaster installation involves installing the Opsware System in multiple facilities and configuring the Opsware Systems to communicate with each other. The multimaster installation process consists of the following tasks:

1. Installing a standalone Opsware core by following the process for a standalone installation.

   See “Overview of the Standalone Installation Process” on page 75 in Chapter 5 for more information.
2. Running the Opsware Installer script a second time to update these Opsware System components in the standalone core to support multimaster operation:

   - Model Repository
   - Opsware Command Center
   - Software Repository
   - Data Access Engine

   See “About a Source Core Upgrade for Multimaster” on page 108 in Chapter 8 for more information.
3. Exporting the data from the Model Repository in the source core
4. Installing the Opsware core in multimaster mode in the subsequent facilities

See “Steps for Creating a Multimaster Mesh and Installing a Second Core” on page 113 in Chapter 8 for more information.

See “Steps for Adding a Third Core or More to a Multimaster Mesh” on page 122 in Chapter 8 for more information.

5 Performing database synchronization tasks by importing the Model Repository data exported from the first facility

In a multimaster installation, the first Model Repository that you set up is referred to as the *source* (the script interface uses the term *master*). Subsequent Model Repository databases are referred to as *targets* (the script interface uses the term *slave*).

The target databases are only target databases in the sense that data is copied from the source Model Repository to the Model Repositories in the target facilities. After the Model Repository databases are up and running, each Model Repository instance functions as a master (that is, it can be accessed for both read and write operations).

6 Configuring the TIBCO Rendezvous routing daemon (rvrd), which provides secure communications between cores in multiple facilities

See “TIBCO rvrd Configuration” on page 138 in Chapter 9 for more information.

Opsware System Architecture for Multimaster Cores

The following diagrams show how Opsware components interact when Opsware technology is running in multiple facilities.

See the *Opsware System 4.7 Administration Guide* for information about how the Opsware System runs in multimaster mode and for information about how to administer this Opsware System configuration.

Customers who need to manage more than one facility should run the Opsware system in multimaster mode. In multimaster mode, any Model Repository database in any facility can be used as the updateable source at any time. In the multimaster architecture, there is no designated master for any individual data element.

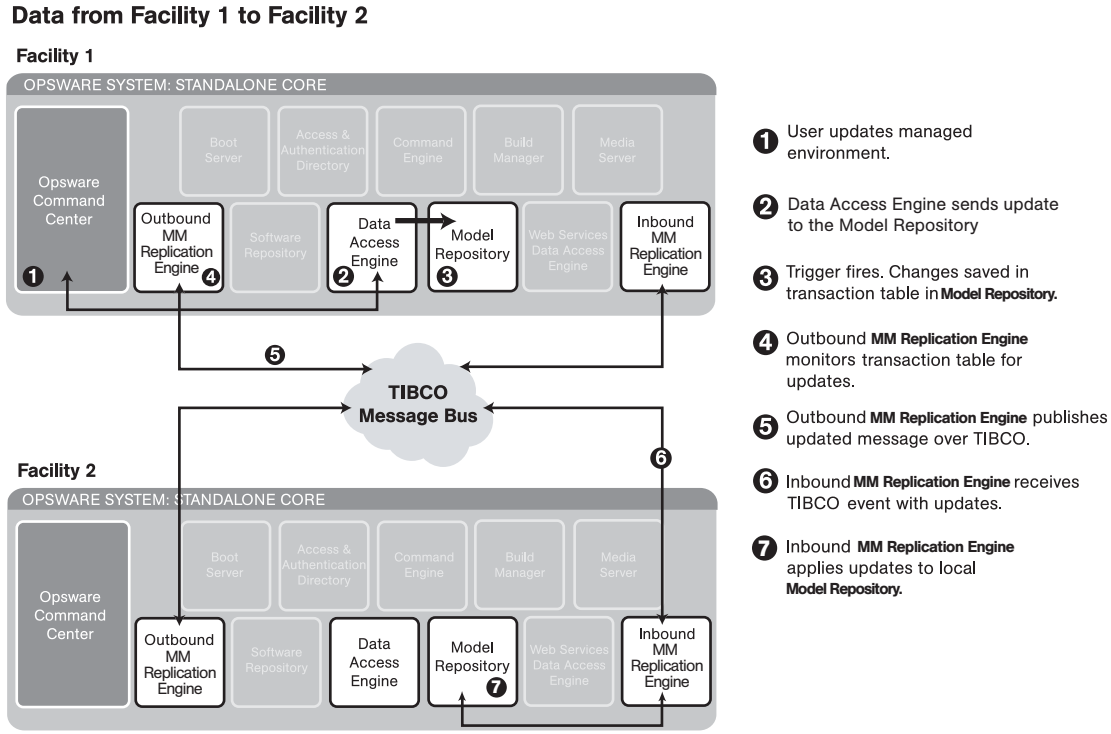
When running in multimaster mode, the Opsware System uses the TIBCO Certified Messaging system to transport transaction data (messages) between Model Repositories at different facilities. The Opsware System uses the TIBCO messages to keep the Model

Repositories synchronized. Additionally, the multimaster Software Repository uses the TIBCO message bus to request distributed files (though the Opsware System actually sends the files over HTTPS). See Figure 1-2.

Running Opsware technology in multimaster mode has the following characteristics:

- Model Repository databases are geographically dispersed.
- Each facility is independent of other facilities.
- Each Model Repository database is read/write.
- Data is updated locally and then propagated to every facility in the multimaster architecture.
- The multimaster mesh is invisible to operations personnel.

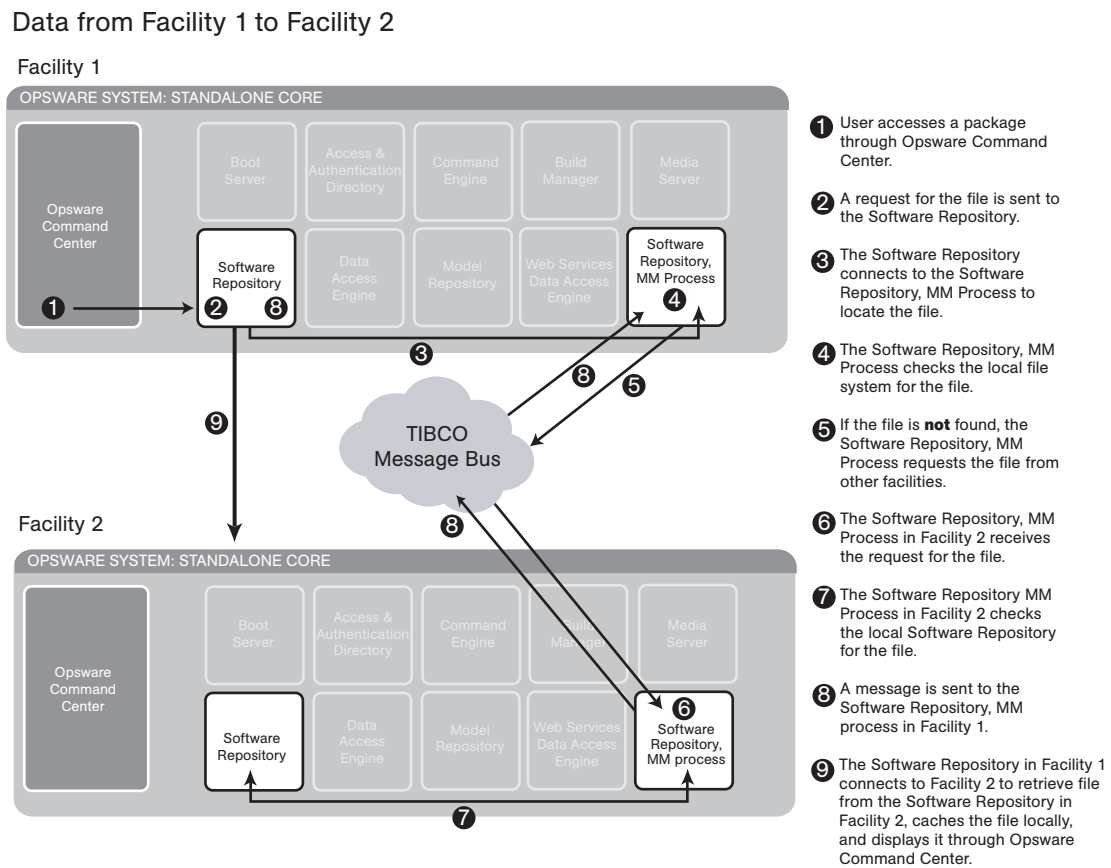
Figure 1-2: Architecture for Multimaster Model Repository



Running the Software Repository in multimaster mode allows users to distribute the contents of the repository (packages and scripts) across facilities, rather than keeping local copies of all packages at each facility. See Figure 1-3.

Packages uploaded to any facility can be used in any other facility, transparently to users.

Figure 1-3: Architecture for Multimaster Software Repository



Chapter 2: Opsware Installer Operation

IN THIS CHAPTER

This chapter provides the following information:

- An overview of how the Opsware Installer operates when you install an Opsware core
- A description of the Opsware Install scripts and how each script is used
- An overview of the Opsware Installer command line syntax
- Where to find the Opsware Installer logs
- How the Opsware Installer interview runs

Overview of Opsware Installer Operation

The process of installing, upgrading, or un-installing the Opsware System in a facility involves several phases, as follows:

1. Specify whether you want to install, upgrade, or un-install a core by running the appropriate Opsware Installer script.

   See "Opsware Installer Command Line Syntax" on page 10 in this chapter for more information.

2. Select the type of installation you want to perform. The following installation types are supported:

   - Standalone Opsware Core
   - Converting a Standalone Opsware Core to a Multimaster Core
   - Multimaster Opsware Core – Subsequent Core

3. Complete the interview.

   See "About the Interview" on page 12 in this chapter for more information.

4. Select a component. You install each component one at a time by running the Opsware Installer script on a server. You cannot install multiple components concurrently by selecting multiple components from the Opsware Installer menu.

5 Perform additional steps.

Depending on the action being performed, the extent of each of the phases is somewhat different. For example, the interview is short or nonexistent when un-installing an Opsware core. Whereas, an initial multimaster installation involves significant steps in all four phases.

For each Opsware component, you must run the Opsware Installer script on the server where you want to install it and select the component name from the Opsware Installer menu. You cannot install multiple components at the same time (by selecting multiple components from the Opsware Installer menu), even though the Opsware Installer does not prevent you from doing this.

For example, if you are installing the Opsware core on six servers, you must log into each of these servers, run the Opsware Installer script, and select the component that you want to install on that server until all the components are installed.

Before running the Opsware Installer, the Opsware System software must be accessible from all core servers, either by mounting the Opsware CD directly or using NFS to mount a directory that contains the software.

When installing, upgrading, or un-installing components, it is important to follow the component order given in the directions, because many components depend on having earlier components up and running. Each step listed in the directions must be followed in sequence, and must run to completion before proceeding.

Opsware Installer Command Line Syntax

The Opsware Installer is run by using one of the following three scripts:

- `install_opsware.sh` invokes the Opsware Installer to install a component.
- `upgrade_opsware.sh` invokes the Opsware Upgrader to upgrade a component.
- `uninstall_opsware.sh` invokes the Opsware Uninstaller to uninstall a component.

You run these scripts each time you want to install, upgrade, or un-install one component on a server.

All three of these scripts run with the same command line options as Table 2-1 shows.

Table 2-1: Opsware Installer Command Line Options

OPTION	DESCRIPTION
`-h`	Displays the Opsware Installer help for the command line options
`--resp_file=<file>` (`-r <path_to_file>`)	Use this response file to find values for component parameters.
`--interview`	Conduct the installation interview to obtain values for component parameters. Primarily, you specify this option when the Opsware Installer is run on the host where the Model Repository has been or will be installed. Additionally, specify the `--interview` option when you have a complete response file but need to run the Opsware Installer in a different mode. For example, you need to upgrade a standalone core to multimaster. **NOTE** You cannot specify the `--interview` option to un-install an Opsware core.

About the Opsware Installer Logs

Each time you run the Opsware Installer, it generates a log in the following directories:

- `/var/lc/install_opsware/install_opsware.<timestamp>.log`
- `/var/lc/install_opsware/uninstall_opsware.<timestamp>.log`
- `/var/lc/install_opsware/upgrade_opsware.<timestamp>.log`

In addition, some components have supplementary logs that contain additional details about the installation of those components.

Additional messages regarding the installation of the Model Repository can be found in the following directory:

`/var/lc/install_opsware/truth/truth_install_<number>.log`

The log file name includes a generated number that is different for each installation.

Additional messages regarding the installation of the Access & Authentication Directory can be found in the following directory:

```
/cust/usr/depot/ds411/netscape/server4/setup/setup.log
```

About the Interview

The command line arguments control the mode of the interview. The Opsware Installer can be run in several different modes:

- **Full Interview** – When command line arguments are not provided (so that a response file is not specified), the Opsware Installer runs the full interview by default. The interview guides a user through building a response file that is appropriate to the type of core being built. First, the user is asked to select the type of installation so that the appropriate prompts are included in the interview.

  The Opsware Installer validates responses to the interview prompts as the user enters them; the user is asked to re-enter a value until the Opsware Installer is able to validate the answer. Some parameters are also revalidated during the actual installation of components. For example, the Opsware Installer verifies during installation that file names provided refer to files that exist on the installation host. If a response to a prompt cannot be validated at installation, the Opsware Installer runs a mini-interview.

  At any time during the interview, the user can press `ctrl-P` to display help for the current prompt.

  When the interview is complete (valid responses have been provided for every prompt), the Opsware Installer returns to the beginning of the list of interview prompts so that the user can review and correct their responses. After the user is satisfied with the responses, the user enters `ctrl-F` to finish the interview. The Opsware Installer prompts the user for a location in which to save the response file, which contains the user's responses to the interview. Then, the Opsware Installer restarts using the newly generated response file.

  When you install a core across multiple servers, the generated response file should be copied to all servers in the core so that the user can perform subsequent component installations by using the response file.

- **Interview with defaults** – When a response file and the `--interview` option are entered on the command line, the Opsware Installer interview runs with the values from the response file as defaults. The user is able to review and change the responses if necessary.

- **Mini-Interview** – When an incomplete response file is specified on the command line and the user has *not* included the `--interview` option, the Opsware Installer prompts the user to select which component to install, and then runs an interview that only prompts for data not included in the response file.
- **No Interview** – When a complete response file is provided, the Opsware Installer displays the list of components to select for installation. The Opsware Installer runs in this mode automatically after the interview is complete.

The Opsware Installer keeps an inventory of the components that are installed on a given server.

Installation Media for the Opsware Installer

The Opsware System is available on and installable from a DVD or a five CD-ROM set.

In the CD-ROM set, all Opsware Installer scripts are contained on CD 1:

- `install_opsware.sh`
- `uninstall_opsware.sh`
- `upgrade_opsware.sh`

The remaining Opsware System CDs (CDs 2 – 5) contain the packages used in the installation of the Opsware components.

If you are installing the Opsware System directly from a CD-ROM, the Opsware Installer prompts you numerous times to change the CD-ROM that is loaded in the server you are installing a component on.

Opsware Inc. recommends that you copy the contents of the Opsware System CDs to local disk or to a network share and run the Opsware Install from that location. When you copy the contents of the CDs to local disk or the network, you must create a directory structure that duplicates the structure of the CDs, as follows:

- `/opsware_system/disk001` – Will contain the contents of CD 1, including the Opsware Installer scripts
- `/opsware_system/disk002` – Will contain the contents of CD 2
- `/opsware_system/disk003` – Will contain the contents of CD 3
- `/opsware_system/disk004` – Will contain the contents of CD 4
- `/opsware_system/disk005` – Will contain the contents of CD 5

The path of the directory where you copy the contents of the CDs cannot have spaces.

When you run the Opsware Installer from the common parent directory, `/opsware_system`, the Opsware Installer switches automatically to the directory it needs to complete the part of the installation process that it is currently performing.

Chapter 3: Installation Prerequisites

IN THIS CHAPTER

This chapter provides the following information:

- The decisions that you must make before you install the Opsware System software
- The installation requirements for the facility and network that the Opsware System uses
- The Opsware System requirements for the Oracle database
- Information that you must obtain before you start the installation process

Before you run the Opsware Installer, you must install and configure the Oracle database as this guide specifies.

Before You Install the Opsware System

Before you install the Opsware System software, you must gather the following information and make the following decisions:

- Decide how you will distribute the Opsware System components on servers

  See “Distribution of Opsware System Components” on page 67 in Chapter 4 for more information.

- Gather information about your IT environment and Oracle installation, TNS names, and database passwords

  See “Information about Your Environment” on page 16 in Chapter 3 for more information. See “Description of Required Information for Installation” on page 42 in Chapter 3 for more information.

- Decide how you will name facilities in the Opsware System

  See “Identifying the Facilities” on page 16 in this chapter for more information.

- Decide how you will identify your authorization domain in the Opsware System

  See "Identifying the Authorization Domain" on page 16 in this chapter for more information.

Information about Your Environment

Before you install the Opsware System software, you must gather certain information about your system. This information includes the following data:

- The password for the `opsware_admin` user in your Oracle databases. Your database administrator should set this up.
- The net service names of your Oracle databases.

See "Installation and Configuration Requirements for Oracle" on page 35 in this chapter for more information. This topic explains how you must install and configure the Oracle database for the Opsware System.

You enter this information when you run the Opsware Installer during the interview. See "Description of Required Information for Installation" on page 42 in this chapter for more information.

Identifying the Facilities

A facility refers to the collection of servers that a single Opsware core manages.

If you are performing a single core installation, your deployment is made up of a single facility. Multimaster installations, however, make up two or more facilities: one facility for each instance of the core that you install.

Before you run the Opsware Installer, you must decide how you are going to identify the facilities that make up your deployment.

A facility is identified by a facility name and a facility ID. You can choose any name, but each facility must have a unique name and a unique ID. The Opsware System uses the facility name and ID internally. You also specify a unique facility display name that the Opsware Command Center user interface displays.

Identifying the Authorization Domain

The Opsware Installer prompts you for the name of your authorization domain. The Access & Authentication Directory component in the Opsware System, which utilizes an LDAP Directory server, requires this information. Specifying an authorization domain while running the Opsware Installer sets up the LDAP authentication domain.

For the sake of convenience, the authorization domain usually has the same name as the domain name. However, it is possible to assign any name.

The authorization domain you specify controls the subset of managed servers Opsware users access at a facility when they log into Opsware Command Center.

Installation Requirements

Before you install the Opsware System, you must meet the following requirements:

- Facility and network requirements for standalone and multimaster installations
- Installation and configuration requirements for the Oracle database

Supported Operating System for the Opsware System

The Opsware System components are installed on one or more Solaris 8 servers or Red Hat Linux AS 2.1 servers. While it is possible to install all the components on a single Solaris server, in most deployments, the components are installed on at least two servers for performance reasons.

The Opsware Agent runs on many additional platforms, including AIX, HP-UX, Linux, Solaris, and Windows. See the *Opsware System 4.5 User's Guide* for information about how to install an Opsware Agent on servers running in the operational environment.

Installation Prerequisites for Linux Servers

On each Linux server where you will install an Opsware System component, you must meet the following additional prerequisites for server configuration:

- When building the server on which you will install the Opsware Model Repository, Opsware Command Center, and Build Manager, you must install the RPM compat-libstdc++ from the distribution directory.

  If you are using Kickstart to build the servers, you can use this ks.cfg%packages section for building the server:

  ```
  @ Server

  compat-libstdc++
  ```

  The Opsware core server functions correctly with this setting.

- If using Integrated Drive Electronics (IDE) hard disks, enable direct memory access (DMA) and some other advanced hard disk features to improve performance. Run the following script as root on the server, and then reboot the server:

```
cat > /etc/sysconfig/harddisks << EOF

USE_DMA=1

MULTIPLE_IO=16

EIDE_32BIT=3

LOOKAHEAD=1

EOF
```

- In the 2.1 AS Linux distribution, correct the text in these files so that Oracle installs successfully.

Table 3-1: Corrections for the Linux Distribution

IN THIS RPM:	MODIFY THIS FILE:
IBMJava2-JRE	/etc/profile.d/java_jre.csh
IBMJava2-SDK	/etc/profile.d/java_sdk.csh

In these two files, you must make the following changes.

Change:

```
root = /opt/IBMJava2-131

if ( $root/jre/bin !~ "${path}" ) then

    set path = ( $root/jre/bin $path )

endif
```

To:

```
set root=/opt/IBMJava2-131

if ( $root/jre/bin !~ "${path}" ) then

    set path=( $root/jre/bin $path )

endif
```


The spaces around the equal sign (=) are gone and "set" was added to the beginning of the first line.

- Network File System (NFS) and expat (a C library for XML parsing) must be installed on the server before installing any Opsware components.
- Verify that the packages zip, unzip, and ncompress are on the server. By default, these packages are not installed when installing the Linux operating system.
- Verify that the latest glibc package is installed on all Linux servers running an Opsware component. (For example, as of January 28, 2004, glibc-2.2.4-32.11 is the latest glibc package.) You can obtain the latest version of the glibc package from the Red Hat errata website.
- Change the initial run level of the server to level 3. Change the run level in the file /etc/inittab.
- If the server already has Apache or Samba installed on it, you must uninstall these applications before you install an Opsware component on the server.

  If Apache or Samba is installed on the server first, the Opsware Installer will stop the installation and prompt you to uninstall the application, after which you can resume the installation.

Hardware Requirements for Opsware Core Servers

Each server that you install an Opsware System component on must have the following hardware configuration:

- 2 CPUs

  When an Opsware core is managing 1500 servers or more, 4 CPUs are recommended for the Model Repository.
- 1 GB of RAM per CPU
- 4 GB swap space (minimum) per server
- A 36 GB hard drive

  The root directory must have 36 GB disk space because, by default, Opsware components are installed in the directories `/cust` and `/lc`.

  When the server is running the Model Repository, Software Repository, or OS Media Server, additional storage is required, as Table 3-2 shows.

This requirement for hard disk space does *not* include the amount of disk space required by Oracle on the server where you install the Opsware Model Repository. See the Oracle documentation for the disk space requirements for an Oracle installation.

- You should install Opsware components on a local disk. Do not install Opsware components on a file server from NetApp.
- Load balancing for the Data Access Engine and Opsware Command Center

Table 3-2: Storage Requirements for the Software Repository and Media Server

OPERATING SYSTEM	SPACE ON MEDIA SERVER	SPACE ON SOFTWARE REPOSITORY
Red Hat Linux 6.2	0.62 GB	0.62 GB
Red Hat Linux 7.1	0.88 GB	0.88 GB
Red Hat Linux 7.2	1.10 GB	1.10 GB
Red Hat Linux 7.3	1.40 GB	1.40 GB
Red Hat Linux 8.0	1.60 GB	1.60 GB
Red Hat Linux AS 2.1	1.10 GB	1.10 GB
Windows NT	0.16 GB	0
Windows 2000	0.31 GB	0
Windows 2003	0.31 GB	0
Solaris 5.6	0.31 GB	0.31 GB
Solaris 5.7	0.35 GB	0.35 GB
Solaris 5.9	0.76 GB	0.76 GB
Solaris 5.9	0.90 GB	0.90 GB
Total for all Operating Systems	9.80 GB	9.02 GB (plus additional storage for packages, see the following paragraphs.)

On the Software Repository, you should allow an additional 0.5 GB storage space for each package. The Software Repository sizing assumes a standalone Opsware core. In a multimaster formation, the amount of storage goes up due to replication across facilities.

Storage requirements for the Software Repository are completely dependent on the number and size of software packages and other installable files that are required for a facility.

For example, for 40 packages, you might need 20 GB additional storage space for the Software Repository. Therefore, if you wanted to have space for all supported versions of Red Hat Linux, Windows, and Solaris, and had 40 packages, you would need 29.02 GB storage.

Organizations can use a variety of different methods to implement the Software Repository, including internal storage, network attached storage (NAS), and storage area networks (SANs). Typical installations would start with approximately 100 to 200 GB. However, much more could be used depending on the number of packages and the size, frequency and duration of configuration backups.

Storage requirements for the Model Repository grow as the number of managed servers grows. As a benchmark figure, you should allow an additional 3.1 GB Model Repository storage for every 1000 servers in the facility that the Opsware System manages.

Additional size factors include whether the Opsware System is deployed across multiple facilities, and how long the Opsware System is maintaining audit information for transactions.

See “Distribution of Opsware System Components” on page 67 in Chapter 4 for more information. This topic explains how the Opsware components should be distributed when the Opsware core consists of multiple servers.

Requirements for the Opsware System

Before you run the Opsware Installer to install an Opsware core in a facility (either a standalone core or a core that is part of an Opsware multimaster mesh), the facility must meet the following requirements:

- The time on the servers running the Opsware core must be synchronized.

  See “Core Time Requirements” on page 23 in this chapter for more information.

- The facility in which the Opsware core is installed must meet certain networking requirements.

  See “Network Requirements within a Facility” on page 25 in this chapter for more information.

- The Opsware System must be able to resolve Opsware server host names and service names.

  See “Component Name Resolution Requirements” on page 23 in this chapter for more information.

- The Opsware core servers communicating with the Model Repository must be able to resolve Opsware-specific database names.

  See “Database Name Resolution for Opsware Components” on page 25 in this chapter for more information. See “Installation and Configuration Requirements for Oracle” on page 35 in this chapter for more information.

- For Opsware cores to function properly in a multimaster mesh, certain requirements must be met.

  See “Requirements Between Multimaster Facilities” on page 28 in this chapter for more information.

Patch Requirement for the Web Services Data Access Engine

For the Web Services Data Access Engine to function properly, you must install the following patches on the servers where the Web Services Data Access Engine is to be installed. The Web Services Data Access Engine is installed on the servers where the Opsware Command Center component is installed.

J2SE v 1.3.1 that installs the Cluster Patches for Solaris

You can download the recommended patches from the following location:

http://java.sun.com/j2se/1.3/download.html

Requirement when Using Opsware Configuration Tracking

When you run the Opsware Configuration Tracking feature in a facility, you must create a separate partition on the server running the Software Repository for the following Configuration Tracking directory:

```
/cust/word/mmword_local/acsbar
```

The Configuration Tracking feature uses this directory to store the back up versions of tracked configuration files and databases.

See the *Opsware System 4.5 User’s Guide* for information about how to set up and use this Opsware System feature.

Core Time Requirements

The servers running the Opsware System components *must* meet the following requirements:

- All servers running Opsware System components, whether a standalone core or part of a multimaster mesh, must maintain synchronized clocks throughout the lifetime of the core. For example, you can accomplish this requirement by synchronizing the system clocks on all the servers with an external time-server that uses NTP (Network Time Protocol) services.
- All servers running Opsware System components must have their time zone set to Coordinated Universal Time (UTC).

This requirement applies to all servers running the core components (such as the Data Access Engine, Model Repository, the Opsware Command Center, and so forth). This requirement does *not* apply to your servers in the operation environment that the Opsware System manages (servers on which the Opsware Agent is running).

Component Name Resolution Requirements

The Opsware System must be able to resolve Opsware server host names and service names (for example, Data Access Engine, Command Engine, and Opsware Command Center) to IP addresses through configuration of DNS CNAMES or `/etc/hosts`.

When you install Opsware components on servers where a previous release of the Opsware System was installed (for example, Opsware System 4.0), you *must* verify that the host names and service names resolve correctly for Opsware System 4.7 Installation Guide. The host names and service names might incorrectly resolve for the previous release.

The following entries should be mapped to the host name of the server on which they are installed:

- `truth.<`*`subdomain`*`>` – Model Repository service
- `way.<`*`subdomain`*`>` - Command Engine service

  Every Command Engine in a multimaster mesh of Opsware cores must be able to resolve the host names of the servers running the other Command Engines in the mesh or Opsware operations will fail and display the following error message:

`The Command Engine cannot proxy a command from one facility to another`

- `spin.<subdomain>` - Data Access Engine service
- `theword.<subdomain>` – Software Repository service
- `twist.<subdomain>` – Web Services Data Access Engine service
- `occ.<subdomain>` – Opsware Command Center service

  The servers running the Opsware components must be able to resolve the Opsware Command Center service. Additionally, users' desktops must be able to resolve this service so that they can log into the Opsware Command Center.

- `buildmgr.<subdomain>` – OS Provisioning Build Manager

  See "Network Requirements for the OS Provisioning Subsystem" on page 30 in this chapter for more information. This topic provides the complete list of network requirements for the OS Provisioning Subsystem.

- `cast.<subdomain>` – Access & Authentication Directory service
- `mastercast.<subdomain>` – Access & Authentication Directory service

  This installation guide documents how to manage all the facilities in a multimaster installation by a single Access & Authentication Directory, which is installed at the first facility (the source facility). In this configuration an Opsware Access & Authentication Directory is installed at the source facility. All other facilities set up their deployment so that the Access & Authentication Directory resolves to the IP address of the directory server at the source facility.

  The Opsware System does support installing an Access & Authentication Directory in each facility. In this configuration, you must set up supplier and consumer Access & Authentication Directories by following the procedures documented in the Netscape Directory Server documentation.

  See your Opsware Support Representative for assistance installing and setting up the Access & Authentication Directories to support this configuration.

  The entries for `cast.<subdomain>` and `mastercast.<subdomain>` are the same when the Opsware multimaster installation uses a single Access & Authentication Directory installed at the source facility.

- Any managed server also has to be able to resolve unqualified Opsware service names (for example, using DNS, `/etc/hosts`, and `/etc/resolv.conf`) to communicate with services installed on Opsware core servers:
  - `spin`
  - `way`
  - `theword`

Database Name Resolution for Opsware Components

All Opsware core servers that communicate with the Model Repository database require a TNS file (`tnsnames.ora`), which enables resolution of Opsware-specific database names.

These servers include the servers where the Data Access Engine, Web Services Data Access Engine, the Model Repository, and the Opsware Command Center are installed.

When you install the Opsware core on multiple servers, the `tnsnames.ora` file with the *same* directory path must exist on the servers where the Model Repository, Data Access Engine, and Opsware Command Center are to be installed.

Network Requirements within a Facility

You must meet the following network requirements and you must configure the network properly before you can run the Opsware Installer:

- The Opsware servers running the components for the same core must be on the same local area network (LAN or VLAN).
- The Opsware core servers must have network connectivity to the servers the Opsware core manages, and vice versa.
- The servers on which the Opsware components are installed cannot be using Network Information Service (NIS) for system file sharing because all Opsware components check for the existence of certain target accounts before creating them during installation.
- When using network storage for Opsware components, such as the Software Repository or Media Server, the network storage configuration must allow root write access over NFS to the directories where the components are to be installed.
- The following DNS CNAMES must resolve on all core servers:

  `truth`

```
way

spin

theword

twist

occ

cast

mastercast

buildmgr
```

- The link speed and duplex of Opsware cores and managed servers should match with the switch to which they are connected. Failing to do so will result in network slowness between the Opsware core and the managed servers.
- Table 3-3 shows the TCP ports that must be open on the core servers so that the components can communicate with each other. .

Table 3-3: Open Firewall Ports on Core Servers within a Facility

PORT	COMPONENT
1004	Data Access Engine
1018	Command Engine
1003	Software Repository
389	Access & Authentication Directory
1521	Model Repository
7500	TIBCO (installed on the server running the Model Repository)

Port 7500 is used for TIBCO communication between the Model Repository and the Software Repository within a core.

- Table 3-4 shows the TCP ports that must be open on managed servers so that core servers can connect to managed servers.

Table 3-4: Open Firewall Ports between the Core Servers and Managed Servers

PORT	COMPONENT
1002	Opsware Agent

- Table 3-5 shows the TCP ports that must be open between managed servers so that managed servers can connect to one another for CDR synchronizations.

Table 3-5: Open Firewall Ports between Managed Servers

PORT	COMPONENT
1002	Opsware Agent

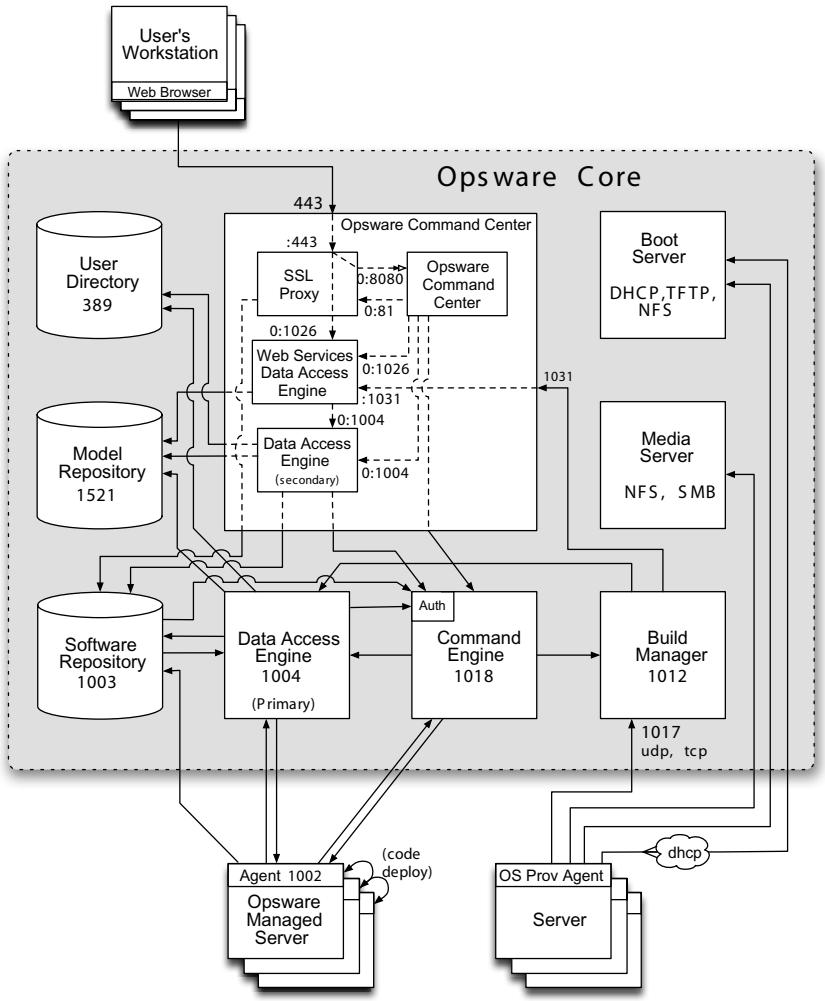
- Table 3-6 shows the TCP ports that must be open from the desktop systems of users managing the Opsware System to the core servers.

Table 3-6: Open Firewall Ports from Desktops to Core Servers

PORT	COMPONENT
22	SSH
80, 443	Opsware Command Center
1002	Opsware Agent
1003	Software Repository
1004	Data Access Engine
1012, 1017	OS Provisioning Build Manager
1018	Command Engine
7580, 7581	TIBCO Management
1031, 1026	Web Services Data Access Engine

Figure 3-1 shows the requirements for open firewall ports in an Opsware System.

Figure 3-1: Open Firewall Ports in an Opsware System Core



Requirements Between Multimaster Facilities

When running the Opsware System in multimaster mode, you must meet the following requirements for the facilities:

- After the time on all servers within a facility is synchronized, you must synchronize the time between the facilities in the multimaster mesh. Synchronize the local time

between servers in different facilities with an external time-server that uses NTP so that all servers are using the same Coordinated Universal Time (UTC).

- A multimaster installation has the same network requirements as a standalone installation, except that each core must be on a different local area network (LAN or VLAN). They must be in different broadcast domains.
- Each core in a mesh should have a different subdomain so that managed servers can resolve the unqualified host name `spin`, `way`, and `theword`.

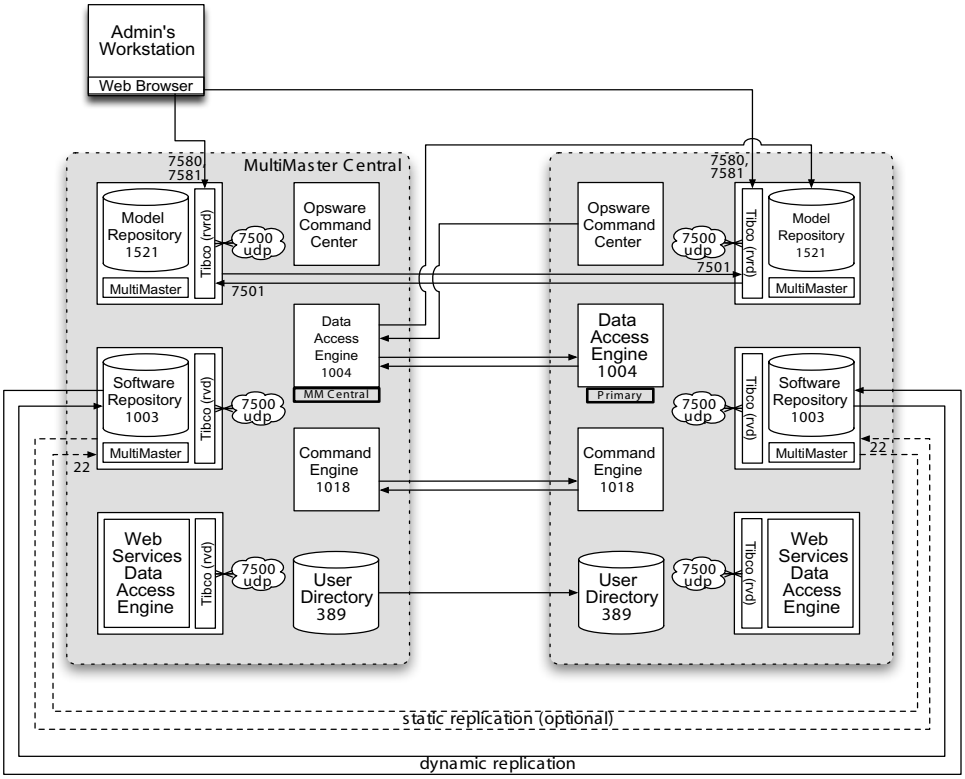
Firewall conduits between cores must allow bidirectional access on the following TCP ports, as Table 3-7 shows.:

Table 3-7: Open Firewall Ports for the Components Between Facilities

PORT	COMPONENT
389, 636	Access & Authentication Directory
1004	Data Access Engine
1018	Command Engine
1003	Software Repository
7501	TIBCO
1521	Oracle sqlnet
22	Software Repository Replicator to use SSH

Figure 3-2 diagrams the requirements for open firewall ports between Opsware System cores.

Figure 3-2: Open Firewall Ports between Opsware System Cores



(This illustration does not include port 636, which is required to allow for LDAP over SSL.)

Network Requirements for the OS Provisioning Subsystem

If you are using OS provisioning for Solaris (JumpStart) on an isolated network, you must have a default gateway (router) available, even if it does not route packets. For Solaris JumpStart to function properly, the IP address of the default gateway must be sent to the installation client that is being provisioned with DHCP. When you use the Opsware DHCP Configuration Tool, a default gateway is properly configured for Solaris because the DHCP Configuration Tool adds the default router appropriately.

The OS Provisioning Subsystem requires that the following networking requirements are met for the subsystem to function:

- **DHCP Requirement** – When you install the OS provisioning components, the Opsware Installer also installs a DHCP server.

  If network provisioning occurs on a separate network from the Opsware core components, you must set up DHCP proxying (for example, with Cisco IP Helper) to the DHCP server. If you set up DHCP proxying, the server/router performing the DHCP proxying must be the router for the network so that PXE will function correctly in the Opsware OS Provisioning Subsystem. You can configure the installed DHCP server after installation by using the Opsware DHCP Network Configuration Tool.

  See "Overview of Network Configuration for OS Provisioning" on page 97 in Chapter 7 for more information.

  Host Name Resolution – For Windows OS provisioning, the host name `buildmgr` should resolve on Windows installation clients.

  The Opsware core host names must resolve using the DNS search order and DNS server information that the DHCP server provides. The DHCP server provides the DNS server IP address and the DNS search order. You must configure the DHCP server to provide the correct information by using the Opsware DHCP Tool.

  For each subnet you configure with the Opsware DHCP Tool, the DNS domain used by that subnet must have a DNS entry for `buildmgr`.

  For example, you configure two subnets: the first subnet domain name uses `subnet1.example.com` and the second subnet domain name uses `subnet2.example.com`. Therefore, there must be two DNS entries: `buildmgr.subnet1.example.com` and `buildmgr.subnet2.example.com`.

- **VLAN Requirement** – You can provision installation clients on the same network as the DHCP server or on a remote network. You must use a DHCP proxy when you provision installation clients on a remote network. You must configure Each VLAN (subnet) by using the Opsware DHCP Tool before you can use the remote network for provisioning.

- **Firewall Requirement** – The installation client has the same requirements for connectivity to the Opsware core network as a managed server.

  See "Network Requirements within a Facility" on page 25 in this chapter for more information.

In addition, the installation clients must be able to reach the OS provisioning components (the OS Provisioning Boot Server, Media Server, and Build Manager) on the ports that Table 3-8 shows.

Table 3-8: Open Firewall Ports for the OS Provisioning Components

PORT	SERVICE	COMPONENTS
67 (UDP)	DHCP	Boot Server
69 (UDP)	TFTP	Boot Server
111 (UDP/TCP)*	RPC (portmapper), required for NFS	Boot Server, Media Server
Dynamic	rpc.mountd, required for NFS	Boot Server, Media Server
137 (UDP/TCP)	NETBIOS Name Service (required for Windows provisioning unless lmhosts is used)	Media Server
139 (TCP)*	NETBIOS Session Service (required for Windows provisioning)	Media Server
1017 (UDP/TCP)	OS Provisioning Build Manager	Build Manager
2049 (UDP/TCP)*	NFS	Boot Server, Media Server

***** `rpc.mountd` runs on a dynamic port and is not fixed. Therefore, if a firewall is in place, it must be an application layer firewall that can understand the RPC request that the client uses to locate the port for `mountd`. The firewall must dynamically open that port.

The Boot Server and Media Server run various services (such as portmapper and rpc.mountd) that have been susceptible to network attacks. Opsware Inc. recommends that you segregrate the OS Provisioning Boot Server and Media Server components onto their own DMZ network. When you segregate these components, the ports listed previously (except for port 1017) should be opened to the DMZ network from the installation client network. Additionally, the Boot Server and Media Server should have all vendor-recommended security patches applied.

Patch Management Setup Prerequisites

You must obtain `qchain.exe`, `mbsacli.exe`, and `mssecure.cab` from Microsoft and copy them to a location on your network that is accessible by the Opsware Installer. The Opsware Installer prompts you for the paths to these Windows utilities during the installation interview.

Setting up the Opsware Patch Management Subsystem involves performing the following tasks:

1. Obtaining the three utilities from Microsoft
   - The `qchain.exe` utility from Microsoft

     See "How to Install Multiple Windows Updates or Hotfixes with Only One Reboot," Microsoft Knowledge Base Article 296861, at the Microsoft support Web site support.microsoft.com/?kbid=296861.
   - The Microsoft patch database Mssecure (`mssecure.cab`)

     You can download `mssecure.cab` from the Microsoft download Web site

     http://go.microsoft.com/fwlink/?LinkId=18922
   - The `mbsacli.exe` patch utility, which is shipped with the Microsoft Base Security Analyzer (MBSA version 1.2.1 or the latest version)

     You can download the `mbsacli.exe` patch utility from the Microsoft support Web site

     http://www.microsoft.com/downloads/details.aspx?FamilyID=b13ebd6b-e258-4625-b0a3-64a4879f7798&DisplayLang=en
2. Copying these three utilities to a directory that is accessible by the server on which you are running the Opsware Installer interview

   You will provide the paths to the utilities while responding to the prompts in the interview.

The Opsware System does not require that you perform any special configuration for these three utilities for the Opsware System. As long as these utilities are properly uploaded during installation, they should get installed on the servers automatically.

The Opsware System downloads them from the Opsware core servers onto the appropriate servers during Opsware Agent installation. If newer versions of the utilities are uploaded to the Opsware Software Repository, the Opsware System downloads the

newer version of the file to managed servers. The Opsware System downloads the newer version the next time the managed server contacts the Opsware core to automatically register its installed software.

Prerequisite for Patch Management on Windows NT 4.0 and Windows 2000

To use the `mbsacli.exe` patch utility for patch management on Windows NT 4.0, you must first install Internet Explorer 6.0 or later because the `mbsacli.exe` patch utility depends on it. This prerequisite is not required for Windows 2003 because IE 6.0 is pre-installed for this operating system.

Creating a Silent Installable Version of IE 6.0 or Later

To create a silent-installable version of IE 6.0 or later, use the Internet Explorer Administrator's Kit (IEAK) for the version of IE that you want to install.

For more information on IEAK, see

`www.microsoft.com/windows/ieak/default.asp`

IEAK creates a re-distributable silent-installable copy of the software component.

Perform the following steps to create a silent installable version of IE 6.0 or later:

1. Install IEAK on your desktop system.
2. After you install IEAK, start the Internet Explorer Customization Wizard.
3. When creating the package, IEAK prompts for a Media Selection option. Select the option Flat (all files in one directory).
4. Select the defaults for all other options when you use the wizard.
5. After the wizard is complete, zip the contents of the directory it created, which contains the silent-installable version of IE. This operation produces a ZIP package.

   (Complete Steps 6 through 9 after you install an Opsware core for the facility.)
6. To upload the ZIP package into the Opsware System, click Software ➤ Packages in the Opsware Command Center left navigation panel, then click the Upload tab in the Browse Packages page, and then follow the prompts to upload the package.
7. Set the following attributes for the package when you upload it into the Opsware System:

   - In the **Customer** field, select Customer Independent.

- In the **Operating System** field, select Windows NT 4.0 or Windows 2000, depending on the version of Windows for which you are setting up silent installation.
- In the **Package Type** field, select Windows Zip file.
- In the Edit Properties page in the **Installation Directory** field, enter the installation location:

  `%SystemDrive%\IE-redist`

- In the Edit Properties page in the **Post-Install Script Filename** field, enter this text:

  `%SystemDrive%\IE-redist\ie5setup.exe /q:a /r:n`

  Where `ie6setup.exe` is the IE 6.x stub installer

  The /q:a install option specifies quiet install mode, with no user prompts. The /r:n install option suppresses restarting the server after IE installation.

- In the Edit Properties page in the **Reboot on Successful Install field**, select the Yes option.

8. Create a node in a Software category or in Templates and attach the uploaded packages to the node.
9. Use the Opsware System Install Software Wizard to install the necessary software on a Windows NT 4.0 managed server.

Installation and Configuration Requirements for Oracle

Before running the Opsware Installer, a database administrator must install an Oracle database on the server where you will also install the Model Repository. The Oracle database must be properly configured and an instance must be running before you can proceed with the installation of the Opsware core.

This section discusses Opsware System requirements for the Oracle database. It does not provide all the information needed to set up and administer an Oracle database.

After you complete these steps, you can use the Opsware Installer to install the Model Repository without any additional database administrator involvement.

1. On the server where you will also install the Model Repository, Install one of the following versions of Oracle on Solaris 8 or Red Hat Linux AS 2.1:

- Oracle version 8.1.7 Enterprise Edition
- Oracle version 9.2.0 Standard Edition
- Oracle version 9.2.0 Enterprise Edition

Install Oracle9i Database Release 2 or later for new globalization installations. Do not install Oracle 9.2.0.5. This version of Oracle is not supported with the Opsware System.

2 Create an Oracle instance that has the minimum settings for the Oracle database, as Table 3-9 shows.

Table 3-9: Recommended Oracle Database Minimum Settings

SETTINGS	MINIMUM VALUES
Temporary tablespace	At least 3000 MB
Rollback segments	At least 7 segments created with `initial_extent` of 8 MB, `next_extent` size 8 MB, optimal size of 64 MB and `pctincrease` set to 0
Database block size	At least 8 KB

3 Create the Oracle database with the UTF8 database character set.

4 Specify initialization parameters in the Oracle `init.ora` file. The Opsware System requires the following parameter settings. All other Oracle settings can follow your corporate guidelines or you can use the Oracle default settings.

```
optimizer_mode = CHOOSE
query_rewrite_enabled = TRUE
query_rewrite_integrity = TRUSTED
open_cursors >= 2000
shared_pool >= 200000000
sort_area_size >= 1048576
nls_sort = punctuation
job_queue_processes = 1
nls_length_semantics = char
```


Set the `nls_length_semantics` parameter to '`char`' for a standalone core installation. When you are installing a second, third, or more core into an existing multimaster mesh, use the same setting for the `nls_length_semantics` parameter that the other Opsware cores are using. If you use different settings in the Opsware cores, the Opsware System will not function correctly. Contact Opsware Professional Services for assistance upgrading the setting for an `nls_length_semantics` parameter in a core.

5 Set up the `tnsnames.ora` entry and listener and start the listener.

The Opsware core servers running the Data Access Engine, Web Services Data Access Engine, and Model Repository require a `tnsnames.ora` file, which enables resolution of Opsware-specific database names. The Data Access Engines and the Model Repository rely on the file to communicate with each other.

In a standalone core, the `tnsnames.ora` file must contain an entry for the Model Repository.

In a multimaster mesh, the `tnsnames.ora` file must contain entries for every Model Repository in the mesh.

When you install the Opsware core on multiple servers, the `tnsnames.ora` file with the *same* directory path must exist on the servers where the Model Repository, Data Access Engine, and Opsware Command Center are to be installed.

6 Initialize the Oracle JVM. The Oracle Installer provides an option for this, but you can also use the following script in the Oracle product directory:

```
$ORACLE_HOME/javavm/install/initjvm.sql
```

7 Create the following four tablespaces for the Model Repository before running the Opsware Installer:

- `LCREP_DATA`
- `LCREP_INDX`
- `TRUTH_DATA`
- `TRUTH_INDX`

When you create the `LCREP_DATA` and `TRUTH_DATA` tablespaces, you must use the following default storage clause so that the sizing formula is accurate:

```
DEFAULT STORAGE( INITIAL 128K
NEXT 128K
PCTINCREASE 0
MAXEXTENTS UNLIMITED)
```

When you create the LCREP_INDX and TRUTH_INDX tablespaces, you must use the following default storage clause so that the sizing formula is accurate:

```
DEFAULT STORAGE( INITIAL 64K
NEXT 64K
PCTINCREASE 0
MAXEXTENTS UNLIMITED)
```

When sizing the tablespaces, follow the general guidelines that Table 3-10 shows. You can request a detailed tablespace sizing spreadsheet if you need to determine a more exact tablespace sizing. Contact your Opsware Support Representative if you need this spreadsheet.

Table 3-10: Guidelines for Sizing the Opsware Tablespaces

TABLESPACE	MB/1000 SERVERS	MINIMUM SIZE
LCREP_DATA	3,000 MB	1,500 MB
LCREP_INDX	1,600 MB	800 MB
TRUTH_DATA	1,300 MB	700 MB
TRUTH_INDX	300 MB	400 MB

8 Create the opsware_admin database user. This user is used to install and manage the Model Repository schema and data. The Opsware System uses the opsware_admin user to manage the installation, upgrade, and maintain the Model Repository without requiring intervention by a database administrator.

Use the TRUTH_DATA tablespace with unlimited quota as the default tablespace for the opsware_admin database user. Set the password for the opsware_admin database user by following the Oracle restrictions for passwords. Set the temporary tablespace according to your organization's policies and requirements.

Grant the following privileges to the opsware_admin user with the admin option:


```
ALTER SESSION
CREATE PROCEDURE
CREATE PUBLIC SYNONYM
CREATE SEQUENCE
CREATE SESSION
CREATE TABLE
CREATE TRIGGER
CREATE TYPE
CREATE VIEW
DELETE ANY TABLE
DROP PUBLIC SYNONYM
SELECT ANY TABLE
SELECT_CATALOG_ROLE
QUERY REWRITE
RESTRICTED SESSION
```

Grant these privileges to the `opsware_admin` user without the admin option:

```
CREATE ROLE
CREATE USER
ALTER USER
DROP USER
ALTER SYSTEM
CREATE PROFILE
ALTER PROFILE
DROP PROFILE
```

Grant these privileges to the `opsware_admin` user with the grant option:

```
EXECUTE ON DBMS_UTILITY
```

9 Set up database monitoring. See “Database Monitoring for the Model Repository” on page 39 in Chapter 3 for more information.

Database Monitoring for the Model Repository

For the Oracle instance that the Opsware Model Repository uses, you should set up monitoring for the following key diagnostics:

- The availability of the Oracle instance and database
- The availability of space for the Model Repository (truth) schema growth

Additionally, Opsware Inc. recommends you monitor key Oracle log files, including the `alert.log` and background and user trace files.

Instance and Database Availability

In this topic, the examples for basic monitoring assume that the Oracle instance name is `truth`.

The Opsware System becomes unavailable when Oracle becomes unavailable. Therefore, to ensure that the Opsware System has access to the Oracle database, you must ensure that the Oracle instance is running, the Oracle database is open, and the listener is monitoring for connections.

- **Checking the Instance**

  1. To check for the status of the instance, perform a Unix system process listing, and look for the presence of a series of `ora_` processes. For example:

```
oracle$ ps -ef | grep ora_
oracle 14239     1  0   Mar 19 ?        0:08 ora_lgwr_truth
oracle 14245     1  0   Mar 19 ?        0:00 ora_reco_truth
oracle 14241     1  0   Mar 19 ?        0:16 ora_ckpt_truth
oracle 14237     1  0   Mar 19 ?        0:04 ora_dbw0_truth
oracle 14243     1  0   Mar 19 ?        0:16 ora_smon_truth
oracle 14235     1  0   Mar 19 ?        0:00 ora_pmon_truth
oracle 14247     1  0   Mar 19 ?        0:00 ora_cjq0_truth
```

  2. Confirm that the instance is running by connecting to the database as `sysdba`. (Be sure to set your `ORACLE_HOME` and `ORACLE_SID` environment variables appropriately.)

```
oracle$ sqlplus "/ as sysdba"
SQL*Plus: Release 9.2.0.4.0 - Production on Mon Mar 22
20:13:21 2004
Copyright (c) 1982, 2002, Oracle Corporation.  All rights
reserved.
Connected to:
Oracle9i Enterprise Edition Release 9.2.0.4.0 - 64bit
Production
JServer Release 9.2.0.4.0 - Production
```

     The "`Connected to:`" message confirms that the instance is available.

- **Checking the database**

The Opsware System needs the database to be mounted and open for general use in order to function.

1. To check the status of the database, connect to the instance as `sysdba` and issue the following query:

   ```
   sql> select database_status from v$instance;
   ```

   The result should be `ACTIVE`.

2. Check the mode in which the database was opened:

   ```
   sql> select open_mode from v$database;
   ```

   The result should be `READ WRITE`.

- **Checking the Listener**

  1. Check the status of the listener by looking for its presence in a Unix process listing. You should see something like the following output:

     ```
     oracle$ ps -ef | grep -v grep | grep tns
     oracle 14253 1 0 Mar 19 ? 0:01 /u01/app/oracle/product/9.2.0/
     bin/tnslsnr LISTENER -inherit
     ```

  2. Test connectivity to the instance from the Data Access Engine (spin) and Web Services Data Access Engine (twist) hosts by running the `tnsping` utility (or by connecting with SQL*Plus with a net-service name identifier):

     ```
     oracle$ tnsping truth
     TNS Ping Utility for Solaris: Version 9.2.0.4.0 - Production
     on 22-MAR-2004 20:16:43
     Copyright (c) 1997 Oracle Corporation.  All rights reserved.
     Used parameter files:
     Used TNSNAMES adapter to resolve the alias
     Attempting to contact
     (DESCRIPTION=(ADDRESS=(HOST=localhost)(PORT=1521)(PROTOCOL=t
     cp))(CONNECT_DATA=(SERVICE_NAME=truth)))
     OK (0 msec)
     ```

     The OK confirms that the listener is up and was able to connect to the instance.

- **Checking for datafile space availability**

  Opsware stores its data in a series of four tablespaces, each of which consists of one or more datafiles. For the size of the data set to grow, you must ensure that each tablespace has enough space for the allocation of new rows.

You can verify this for auto-extensible tablespaces by executing the following query:

```
sql> select sum(bytes), sum(maxbytes) from dba_data_files
where tablespace_name = '<name>';
```

Where <*name*> is the name of an Opsware tablespace. As bytes approaches maxbytes, ensure you increase the size of the datafile or add additional space.

Monitoring Oracle Log Files

You should monitor the following files:

- The Oracle `alert.log` file for ORA- errors because some of the errors will not manifest themselves directly in the application.
- `$ORACLE_BASE/admin/truth/bdump/alert_truth.log`
- `$ORACLE_BASE/admin/truth/[bcu]dump/*.trc`

Configure a cronjob to perform the following actions:

- Periodically poll for changes to or creation of these files or for the presence of ORA- errors
- Report these errors by email or another way to a DBA

Description of Required Information for Installation

Before you install components on a server, the Opsware Installer interviews you for information about how you will install the Opsware core in that facility.

Depending on the type of installation you are performing (such as, installing a standalone core on one or multiple servers, upgrading a standalone core to multimaster mode, installing a subsequent core in a multimaster mesh, or un-installing a core), the Opsware Installer presents you with a slightly different set of interview prompts. For example, the interview is short when un-installing an Opsware core; whereas, an initial multimaster installation requires data for all the interview prompts.

See “Overview of Opsware Installer Operation” on page 9 in Chapter 2 for more information. This topic provides information about the types of interviews the Opsware Installer presents you with for different types of installations.

In particular, you are prompted to provide the following types of information.

- Information related to the Model Repository, including:

  - How Oracle was installed for the Opsware Model Repository
  - How to export and import data between Model Repositories when you install an Opsware multimaster mesh
  - How you want to handle the data in the Model Repository when you un-install an Opsware core
- How to define the facility that you will manage with the Opsware core that you are installing, including:
  - How to uniquely identify the facility with an ID number, internal system name, and display name that will appear in the Opsware Command Center
  - The default customer that will be associated with the facility
  - The authorization domain and subdomain for the facility
- User account names and passwords that the components will use internally when communicating with each other
- Information required to install and configure the OS Provisioning and Patch Management Subsystems

Model Repository Prompts

The Model Repository is the Opsware System data repository that stores information about the hardware and software deployed in the operational environment.

The majority of the prompts requesting information for the Model Repository installation apply to installing a standalone Opsware core. However, if you are installing a subsequent Opsware core in a multimaster mesh, you need to provide some additional information so that the Opsware Installer can export and import data from the source core to the subsequent core being installed. See Table 3-11.

Table 3-11: Model Repository Prompts

PROMPT	DESCRIPTION
Enter the service name (aka TNS name) of the Model Repository instance. (Parameter: `truth.servicename`)	Specifies the service name, also known as the alias, for the Model Repository The service name can be determined by looking in the `tnsnames.ora` file on the Model Repository instance. The location of this file can vary, so check with your DBA if you are not sure where to look. Source: The DBA who installed Oracle Example: `SERVICE_NAME = truth.opsware.com`
Enter the SID of the Oracle instance that contains the Data Model Repository. (Parameter: `truth.sid`)	Specifies the database system ID (SID) that was set when Oracle was installed on the server where the Model Repository will be installed You can find out the SID by looking at the `tnsnames.ora` file. The location of this file can vary, so check with your DBA if you are not sure where to look. Source: The DBA who installed Oracle Example: `DTC05`

Table 3-11: Model Repository Prompts

PROMPT	DESCRIPTION
Enter the path of the Oracle home. (Parameter: `truth.orahome`)	Specifies the base directory of the Oracle installation that was set when Oracle was installed You can determine the Oracle home directory by logging in as the `oracle user` on the Model Repository server, and checking the value of the `$ORACLE_HOME` environment variable. Source: The DBA who installed Oracle Example: `/cust/oracle/product/8.1.7.3.0`
Enter the path to the TNS admin directory (where the tnsnames.ora file resides). (Parameter: `truth.tnsdir`)	Specifies the directory that contains the `tnsnames.ora` file. The location of the `tnsnames.ora` file can vary, so check with your DBA if you are not sure where to look. When you install the Opsware core on multiple servers, the `tnsnames.ora` file with the *same* directory path must exist on the servers where the Model Repository, Data Access Engine, and Opsware Command Center are installed. Source: The DBA who installed Oracle Example: `/var/opt/oracle`

Table 3-11: Model Repository Prompts

PROMPT	DESCRIPTION
Enter the full path to the directory where the export file will be saved. (Parameter: `truth.dest`)	**A multimaster prompt** – Specifies the directory where the database export file will be saved. This directory must exist on the Model Repository server in the source facility. When adding a facility to a multimaster mesh, you must export the Model Repository from the source facility, then copy it to the destination facility. Source: Arbitrary (however, you must create the directory on the server before you run the Opsware Installer) Example: `/export/home/core1`
Enter the full path to the directory that contains the export file. (Parameter: `truth.sourcePath`)	**A multimaster prompt** – Specifies the directory on the Model Repository server in the destination facility where the export data file was copied from the source facility. When adding a facility to a multimaster mesh, you must export the Model Repository data from the source facility, then copy it to the destination facility. Source: Arbitrary (however, the directory must exist on the server and contain the database export file before you run the Opsware Installer on that server) Example: `/export/home/core2`
Do you need to preserve any of the data in this database? (Parameter: `truth.uninstall.needdata`)	Appears when un-installing the Model Repository Because un-installing the Model Repository permanently deletes all data in the database, the un-installation process stops if you answer yes to this parameter, so you have the opportunity to back up the data you would like to preserve. The Opsware Installer does not preserve any data.

Table 3-11: Model Repository Prompts

PROMPT	DESCRIPTION
Are you sure you want to remove all data and schema from this database? (Parameter: `truth.uninstall.aresure`)	Appears when un-installing the Model Repository Because un-installing the Model Repository permanently deletes all data in the database, the un-installation process stops if you answer no to this parameter.

User Account and Password Prompts

To ensure a secure installation of the Opsware System, the Opsware Installer prompts you to set passwords for numerous Oracle user accounts that the Opsware components use to interact with one another. See Table 3-12. The passwords must meet standard Oracle criteria, as the following list shows:

- The password cannot contain an Oracle reserved word (see Oracle's documentation for a full list).
- The password must be between 1 and 30 characters long.
- The password must start with a letter and use only alphanumeric and underscore (_) characters.

All passwords for the Opsware System (set by providing values during the Opsware Installer interview) must have the same values across facilities so that components can communicate when the Opsware System is running in multimaster mode. For example, you install your first core and enter `spin_x145_pwd` as the password for the spin user. When you install the second core in the Opsware System, the spin user running in the second core must also have the password `spin_x145_pwd`.

Table 3-12: User and Password Prompts

PROMPT	DESCRIPTION
Enter database password for the opsware_admin user. (Parameter: `truth.oaPwd`)	Specifies the `opsware_admin` password created by your database administrator `opsware_admin` is an Oracle user that the Opsware Installer uses during installation to perform certain functions. Source: This *must* be the password that your DBA set for the `opsware_admin` user when setting up the Oracle instance on the server where you will install the Model Repository.
Enter database password for the lcrep user. (Parameter: `truth.lcrepPwd`)	Sets the password for the `lcrep` database user The Opsware Installer automatically creates an Oracle user `lcrep`, which the Opsware System uses internally for running multimaster replication between Opsware cores. Source: Arbitrary (however, must meet the requirements for Oracle passwords) Example: `x145_pwd03`
Enter database password for the gcadmin user. (Parameter: `truth.gcPwd`)	Sets the password for the `gcadmin` database user The Opsware Installer automatically creates an Oracle user `gcadmin`, which the Opsware System uses internally for removing old data from certain tables (referred to as the garbage collection process). Source: Arbitrary (however, must meet the requirements for Oracle passwords) Example: `x145_pwd03`

Table 3-12: User and Password Prompts

PROMPT	DESCRIPTION
Enter the database password for the truth user. (Parameter: `truth.truthPwd`)	Sets the password for the he `truth` user The Opsware Installer automatically creates this Oracle user, which is the main schema owner for the Model Repository. Source: Arbitrary (however, must meet the requirements for Oracle passwords) Example: `x145_pwd03`
Enter the database password for the spin user. (Parameter: `truth.spinPwd`)	Sets the password for the `spin` user The Opsware Installer automatically creates this database user. Source: Arbitrary (however, must meet the requirements for Oracle passwords) Example: `x145_pwd03` Note: Passwords for the `spin` user should be the same across all the cores in the mesh.
Enter the database password for the twist user. (Parameter: `truth.twistPwd`)	Sets the password for the `twist` user The Opsware Installer automatically creates this user. Source: Arbitrary (however, must meet the requirements for Oracle passwords) Example: `x145_pwd03`

Table 3-12: User and Password Prompts

PROMPT	DESCRIPTION
Enter the database password for the vault user. (Parameter: `truth.vaultPwd`)	Sets the Model Repository, Multimaster Component password. This prompt only appears when installing the Opsware System in multimaster mode. The Opsware Installer automatically creates the `vault` user. The Model Repository, Multimaster Component propagates and synchronizes changes from each Model Repository database to all other Model Repository databases. Source: Arbitrary (however, must meet the requirements for Oracle passwords) Example: `x145_pwd03`
Enter the database password for the public views user. (Parameter: `truth.pubViewsPwd`)	Sets the password for the `public_views` user, which the Opsware System uses for the Data Center Intelligence (DCI) module (server reporting). The DCI module uses this password when connecting with the Model Repository. The Opsware Installer automatically creates the public views user. If you are using Brio, Crystal Reports, or other data reporting tools with the DCI module, you are asked for the database user password when you log into those applications so that you have read-only access to the Model Repository data. Source: Arbitrary (however, must meet the requirements for Oracle passwords) Example: `x145_pwd03`

Table 3-12: User and Password Prompts

PROMPT	DESCRIPTION
Enter the password for Build Manager user. (Parameter: `twist.buildmgr.passwd`)	Sets the password for the `buildmgr` user that the `buildmgr` process will use when connecting to and authenticating with the Web Services Data Access Engine. The Opsware Installer automatically creates this user. The password cannot contain spaces or a forward slash (/). Source: Arbitrary Example: `x145_pwd03`
Enter the password for Integration user. (Parameter: `twist.integration.passwd`)	Sets the password for the `integration` user that a customer can use to access the SOAP APIs on the Web Services Data Access Engine. The Opsware Installer automatically creates the `integration` user. The password cannot contain a forward slash (/). Source: Arbitrary Example: `x145_pwd03`
Enter the password to decrypt cryptographic material. (Parameter: `decrypt_passwd`)	Sets the password to use for decrypting cryptographic material. It cannot contain any spaces. The password must be between 4 and 20 characters long. This password *must* be the same across all Opsware cores in a multimaster mesh. Source: Arbitrary Example: `x145_pwd03`

Table 3-12: User and Password Prompts

PROMPT	DESCRIPTION
Enter the password to use for the Directory Manager entry. (Parameter: `cast_mgr.pwd`)	Sets the password to use for the Directory Manager entry in the Access & Authentication Directory. It cannot contain any spaces. Source: Arbitrary Example: `x145_pwd03`
Enter the password to use for admin entry. (Parameter: `cast.admin_pwd`)	Sets the password for the `admin` user in the Access & Authentication Directory. It cannot contain any spaces The Opsware Installer automatically creates this user. When you log into the Opsware Command Center in the facility, you log in as the `admin` user (user name “admin”) and supply the password you provide at this prompt. In general, you will *not* need to log into the directory manager (Netscape Directory Server) by using this user and password unless you need to troubleshoot directory issues. Source: Arbitrary Example: `x145_pwd03`
Enter the username for Web Services Data Access Engine Admin Interface. (Parameter: `twist.adminuser`)	Sets the user name to enter at the browser interface when accessing the WebLogic Management Console Source: Arbitrary Example: twistuser

Table 3-12: User and Password Prompts

PROMPT	DESCRIPTION
Enter the password for Web Services Data Access Engine Admin Interface. (Parameter: `twist.adminpasswd`)	Sets the password for the user you created to access the WebLogic Management Console The password cannot contain a forward slash (/). Source: Arbitrary Example: `x145_pwd03`
Please enter password for wsapiReadUser user (Parameter: `twist.wsapiReadUser.passwd`	Sets the password for the wsapiReadUser user. The wsapiReadUser user must authenticate itself to the Web Services API. The password cannot contain spaces. Source: Arbitrary Example: `x145_pwd03`
Please enter password for `wsapiWriteUser` user (Parameter: `twist.wsapiWriteUser.passwd`	Sets the password for the wsapiWriteUser user. The wsapiWriteUser user must authenticate itself to the Web Services API. The password cannot contain spaces. Source: Arbitrary Example: `x145_pwd03`

During the Opsware Installer interview, you must define the facility that you will manage with the Opsware core you are installing, by providing the following information:

- How to uniquely identify the facility with an ID number, internal system name, and display name that will appear in the Opsware Command Center
- The default customer that will be associated with the facility
- The authorization domain and subdomain for the facility

  See “Identifying the Authorization Domain” on page 16 in Chapter 3 for more information.

You need to identify each facility in the following ways:

- The first facility you create for the standalone core must be defined by answering prompts during the Opsware Installer interview. You specify a facility ID, long name

(used internally by the Opsware System), and short name (displayed in the Opsware Command Center to identify a facility).

Opsware facility IDs must be less than 1000. Therefore, you must specify a number for the first facility that is well below 1000 so you can continue to add facilities to your multimaster mesh. If the Opsware Command Center automatically generates a number that is 1000 or higher, the installation will fail.

- The subsequent facilities that you create are part of an Opsware multimaster mesh. You create these target facilities in the Opsware Command Center installed at the source core (the first core installed). You specify a name (the long name that the Opsware System uses internally) and a short name. The Opsware Command Center automatically creates the facility ID.

When you later install the core by using the Opsware Installer, you must enter the information that you specified in the Opsware Command Center at the Opsware Installer interview prompts for the target facility. See Figure 3-3 and Table 3-13.

Figure 3-3: New Facility Page in Opsware Command Center

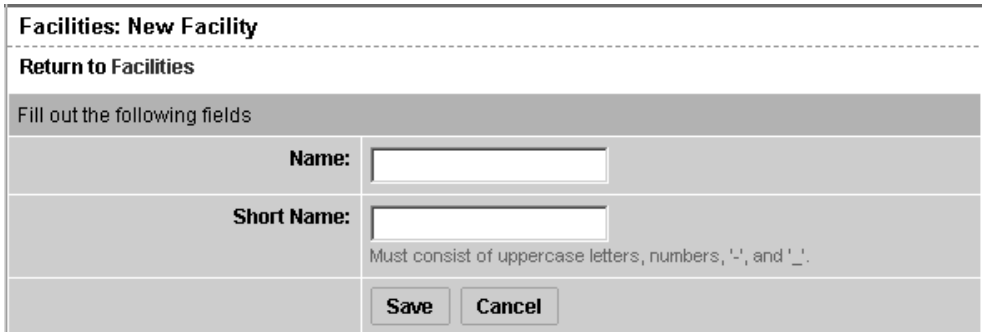


Table 3-13: Facility Prompts

PROMPT	DESCRIPTION
Enter the authorization domain (uppercase). (Parameter: `truth.authDom`)	Sets the authorization domain for the initial (default) customer. This value is usually the same as the domain name. It must be uppercase, less than 50 characters, and in domain name format. You must provide a valid, uppercase domain name. You must use the same value for every Opsware core in your multimaster mesh. The Opsware Installer only prompts you for this value when you are installing your first, standalone Opsware core. Source: Arbitrary Example: `XYZ.COM`

Table 3-13: Facility Prompts

PROMPT	DESCRIPTION
Enter the subdomain for this facility (lowercase, no spaces). (Parameter: `truth.dcSubDom`)	Specifies the fully-qualified DNS subdomain where the Opsware core is deployed This value must be unique for each core in the multimaster mesh. The value is based on the VLAN for the facility in which you are installing the Opsware core. It must be lowercase, less than 50 characters, and in subdomain format. Source: Your network administrator Example: `dc1.opsware.com`
Enter the facility short name (uppercase, no spaces). (Parameter: `truth.dcNm`)	Sets the default facility in the Opsware System Some Opsware System processes use this name internally. It must be uppercase, less than 25 characters, and *cannot* contain spaces or special characters (although dashes and underscores are allowed). Source: Arbitrary Example: HEADQUARTERS
Enter the default locale for users of the Opsware Command Center (en) (Parameter: default_locale)	Specifies the default locale (language, character sets, and date and time formats) for the Opsware System core. Source: Opsware System 4.7 only supports the English-US locales) Example: `en` Note: Enter `en`. Do not enter `en/us` or any other locales.

Table 3-13: Facility Prompts

PROMPT	DESCRIPTION
Enter the facility long name. (Parameter: `truth.dcDispNm`)	Sets the name that displays in the Opsware Command Center It must be unique, less than 50 characters, and cannot include any special characters (< > & * \ ' ?). Source: Arbitrary Example: West Coast Office
Enter the facility ID (number only, less than 1000, with no leading zeros). (Parameter: `truth.dcId`)	When creating the first facility, assigns the ID number for the facility. If you have more than one facility, this ID is used to identify an individual facility. When you create the target facility at the source facility, the Opsware Command Center creates the facility ID automatically. Specify the number that appears in the Opsware Command Center. Find the target facility ID by logging into the Opsware Command Center at the source facility. Select Opsware Facilities under Environment in the navigation panel and click the facilities' name. **REQUIREMENT** Opsware facility IDs must be less than 1000. Therefore, you must specify a number for the first facility that is well below 1000 so you can continue to add facilities to your multimaster mesh. If the Opsware Command Center automatically generates a number that is 1000 or higher, the installation will fail. Source: Arbitrary for the first facility; set by the Opsware System for subsequent facilities Example: 100

Table 3-13: Facility Prompts

PROMPT	DESCRIPTION
Enter the customer name (uppercase, no spaces). (Parameter: `truth.acctNm`)	Sets the default customer for the facility in which you are installing the core. Some Opsware System processes use this name internally. It must be a unique name, uppercase, less than 35 characters, and cannot contain spaces. Source: Arbitrary Example: MARKETING
Enter the customer display name (Parameter: `truth.acctDispNm`)	Sets the display name in the Opsware Command Center for the initial (default) customer The name must be unique, less than 50 characters, and cannot include any special characters (< > & * \ ' ?). Source: Arbitrary Example: IT Department

OS Provisioning and Patch Management Prompts

You must provide the following configuration information during the interview for the OS Provisioning and Patch Management Subsystems to function properly in the operational environment.

In addition to providing this information, these subsystems also require that you perform prerequisite setup tasks before you install the components. For example, you must have obtained the Microsoft patch management utilities and copied them to the server where you will install the Software Repository.

See “Patch Management Setup Prerequisites” on page 33 in this chapter for more information.

See “Overview of Network Configuration for OS Provisioning” on page 97 in Chapter 7 for more information. This topic provides information about the configuration you must perform for the OS Provisioning Subsystem. See Table 3-14 also.

Table 3-14: OS Provisioning and Patch Management Prompts

PROMPT	DESCRIPTION
Enter the full path location of Microsoft's qchain.exe utility. (Parameter: `word_windows_qchain_util`)	Specifies the full path to the Microsoft qchain utility that was copied to the server where you will install the Software Repository This Microsoft utility facilitates installation of multiple Hotfixes, by managing the Pending File Rename queue and other system attributes that are modified during Hotfix installation. When two or more Hotfixes are being chain installed, the qchain utility allows you to defer rebooting until all Hotfixes are completely installed. Source: Arbitrary (however, this directory must exist on the server where the Software Repository is installed) Example: `/home/win_util/qchain/qchain.exe`
Enter the full path location of the Microsoft Baseline Security Analyzer command line utility, mbsacli.exe. (Parameter: `word_windows_hfnetchk_util`)	Specifies the full path to the Microsoft mbsacli utility that was copied to the server where you will install the Software Repository This utility is used on Windows managed servers to determine exactly which Hotfixes are installed (explicitly or implicitly) and which Hotfixes are recommended for installation. Source: Arbitrary (however, this directory must exist on the server where the Software Repository is installed) Example: `/home/win_util/mbsacli/mbsacli.exe`

Table 3-14: OS Provisioning and Patch Management Prompts

PROMPT	DESCRIPTION
Enter the full path location of Microsoft's mssecure.cab file. (Parameter: `word_windows_mssecure_file`)	Specifies the full path to the Microsoft Patch Database `mssecure.cab` file that was copied to the server where you will install the Software Repository The `mssecure.cab` file contains the `mssecure.xml` file, which is Microsoft's Windows OS Patch Database. It is imported during Opsware Installation and provides details of all Microsoft Hotfixes and Servicepacks known to the Opsware System. Source: Arbitrary (however, this directory must exist on the server where the Software Repository is installed) Example: `/home/win_util/mssecure/mssecure.cab`
Enter the OS Provisioning Boot Server ip or hostname. (Parameter: `bootagent.host`)	Specifies the server on which you will install the OS Provisioning Boot Server component You must provide a valid IP address or host name that can be resolved from the server on which you installed the OS Provisioning Boot Server and the Build Manager. Additionally, the host name must be resolvable by Opsware managed servers for OS provisioning.
Enter the hostname or ip of the Build Manager. (Parameter: `boot_server.buildmgr_host`)	Specifies the server on which you will install the OS Provisioning Build Scripts You must provide a valid IP address or host name that can be resolved from the server on which you install the OS Provisioning Boot Server.

Table 3-14: OS Provisioning and Patch Management Prompts

PROMPT	DESCRIPTION
Enter the default network speed/ duplex setting for Solaris servers. (Parameter: `boot_ server.speed_duplex`)	Sets the default network speed and duplex that will be used by Solaris servers booted from this boot server during Opsware OS provisioning. Valid responses are: 100fdx, 100hdx, 10fdx, 10hdx, 100T4, and autoneg. Enter a value without spaces. Source: Arbitrary Example: `100fdx`
Enter the pathname of the RedHat Linux media. (Parameter: `media_ server.linux_media`)	Specifies the path to the Red Hat Linux OS media on the server on which the Software Repository will be installed Providing the path to the Linux OS media does not actually copy the media to this host. See the *Opsware System 4.5 User's Guide* for the steps required to set up the media on the Media Server. Source: Arbitrary (however, this directory must exist on the server where the Software Repository is installed) Example: `/home/os_media/linux/`

Table 3-14: OS Provisioning and Patch Management Prompts

PROMPT	DESCRIPTION
Enter the pathname of the Solaris media. (Parameter: `media_server.sunos_media`)	Specifies the path to the Sun Solaris OS media on the server on which the Software Repository will be installed Providing the path to the Solaris OS media does not actually copy the media to this host. See the *Opsware System 4.5 User's Guide* for the steps required to set up the media on the Media Server. Source: Arbitrary (however, this directory must exist on the server where the Software Repository is installed) Example: `/home/os_media/solaris/`
Enter the pathname of the Windows media. (Parameter: `media_server.windows_media`)	Specifies the local file system path on the Windows OS media part of the Software Repository host The OS Provisioning Subsystem exports Windows OS media to SMB clients through a Samba share. Providing the path to the Windows OS media does not actually copy the media to this host. See the *Opsware System 4.5 User's Guide* for the steps required to set up the media on the Media Server. Source: Arbitrary (however, this directory must exist on the server where the Software Repository is installed) Example: `/home/os_media/windows/`

Table 3-14: OS Provisioning and Patch Management Prompts

PROMPT	DESCRIPTION
Enter the share name to use for the Windows media sharing server. (Parameter: `media_server.windows_share_name`)	Sets the share name that you want Samba to use to export the Windows OS media The share name is *not* case sensitive. Source: Arbitrary Example: `WINMEDIA`
Enter a password to write-protect the Windows media share. Import_media prompts for this password each time it is run. (Parameter: `media_server.windows_share_password`)	Sets the root user password, which enables write access to the Windows share. The Opsware Import Media Tool prompts for this password each time it is run. The password cannot contain spaces. Source: Arbitrary Example: `x145_pwd03`
Enter the hostname of the Package Repository. (Parameter: `media_server.wordbot_host`)	Specifies the host name where you will install the Software Repository You must provide a valid IP address or host name that can be resolved from the server on which you install the OS Provisioning Media Server.

Miscellaneous Prompts

In addition to the prompts described previously, you must provide data for the following prompts, as Table 3-15 shows.

Table 3-15: Miscellaneous Prompts

PROMPT	DESCRIPTION
Is this going to be a multidevice core installation? (Parameter: `spin.clear`)	Indicates whether the Data Access Engine and the Opsware Command Center will be installed on different servers Example: `y`

Table 3-15: Miscellaneous Prompts

PROMPT	DESCRIPTION
Does this device have cryptographic material from previous Opsware releases (for example Opsware 3.6.1)? (Parameter: `upgrade_crypto`)	Indicates if cryptographic material was installed as part of the Opsware System 3.6.1 release Example: `n`
Would you like to preserve the database of cryptographic material? (Parameter: `save_crypto`)	Appears when un-installing an Opsware core If you answer yes, the database of cryptographic material is saved. Otherwise, it is deleted when the un-installation finishes. Example: `y`

Chapter 4: Opsware Core Scalability

IN THIS CHAPTER

This chapter provides the following information:

- Recommendations for scaling an Opsware System core for performance
- How to distribute Opsware components across servers in the multi-server core

Opsware Core Scalability for Performance

Opsware Inc. works with each customer to design an infrastructure that meets their exact requirements. However, as an organization's requirements grow, you can add resources to the Opsware Systems because all Opsware components are designed to scale.

The system requirements for the Opsware System vary based on the following factors:

- The number of servers that the Opsware System is managing
- The number and complexity of requests the Command Engine is processing
- The number of users accessing the Opsware Command Center to perform updates
- The number of facilities in which the Opsware System operates

A typical configuration includes the servers necessary to run the Opsware System components, plus attached or network storage to maintain the Opsware model and Software Repositories. For small environments, the Opsware System can run on a single Solaris server. In larger environments, the Opsware System scales to run on more servers.

All components of the Opsware System are designed to scale, so organizations can add resources easily as their requirements grow. The way in which the Opsware System scales is similar to other typical three-tier applications. You can generally scale horizontally, adding servers and load balancing, on Web and application tiers that support the Opsware Command Center and other Opsware components. You can scale vertically, adding system resources such as processors and memory to the Opsware core configuration (supporting the database tier, providing the Model Repository).

Opsware System Sizing Guidelines

Table 4-1 provides an approximate guide to determining how many servers you need to run the Opsware core based on the metrics in your facility. This determination varies, potentially significantly, depending on the number of active users, amount of change in the environment and types of servers in the environment. For multiple facility installations, repeat the sizing exercise separately for each facility.

The server assumed is a Sun Enterprise class machine with the following specifications:

- 2 CPUs (4 CPUs are recommended for the Model Repository server in installations of six core servers)
- 1 GB RAM or higher per CPU (2 GB recommended)
- Solaris 8 with latest patches from Sun installed
- 36 GB hard drive in each server (with additional storage for the Software Repository and Model Repository)

  The root directory must have 36 GB disk space because, by default, Opsware components are installed in the directories `/cust` and `/lc`.
- Load balancing for the Data Access Engine and Opsware Command Center components

Table 4-1: Opsware System Sizing Guidelines

IF YOU HAVE...		YOU WILL NEED...
# MANAGED SERVERS	**# OPSWARE USERS**	**# CORE SERVERS**
480	19	**1**
1125	45	**2**
2250	90	**3**
3600	144	**4**
3750	150	**5**
5700	228	**6**

These recommendations for Opsware core sizing are based on the following assumptions:

- The entries for number of users assumes that 20% of the users would be using the system concurrently, which is a conservative assumption.
- A single installation of an Opsware Command Center in a core can support 30 concurrent Opsware System end users and manage 3750 servers.
- A single installation of a Data Access Engine in a core can support managing 3000 servers.

Distribution of Opsware System Components

You can install the various components that make up the Opsware System on a single server or on a combination of servers. Before you install, you need to determine how many servers will make up the Opsware core and where (for example, on which servers) you are going to install each of the components of the Opsware System.

To make this decision, you should consider the performance requirements of your deployment. You can install multiple components on a single server, but for performance reasons, you might want to distribute the Opsware System components across a larger number of servers. See Table 4-2.

Do not install the Opsware Command Center component and the Data Access Engine on the same server when you are installing an Opsware core on multiple servers.

Table 4-2: Server/Opsware Component Distribution

# OF CORE SERVERS	DISTRIBUTION OF OPSWARE COMPONENTS
1	**Server 1:** All Opsware components
2	**Server 1:** Data Access Engine, Software Repository, Command Engine, OS Provisioning components (Build Manager, Build Scripts, Boot Server, and the Media Server) **Server 2:** Model Repository, Access & Authentication Directory, Opsware Command Center, Opsware Documentation

Table 4-2: Server/Opsware Component Distribution

# OF CORE SERVERS	DISTRIBUTION OF OPSWARE COMPONENTS
3	**Server 1:** Data Access Engine, Command Engine, OS Provisioning components (Build Manager, Build Scripts, Boot Server, and the Media Server) **Server 2:** Model Repository, Access & Authentication Directory, Data Access Engine #2 **Server 3:** Software Repository, Opsware Command Center, Opsware Documentation
4	**Server 1:** Data Access Engine, OS Provisioning components (Build Manager, Build Scripts, Boot Server, and the Media Server) **Server 2:** Model Repository, Access & Authentication Directory, Data Access Engine #2 **Server 3:** Software Repository, Command Engine **Server 4:** Opsware Command Center, Opsware Documentation
5	**Server 1:** Data Access Engine, OS Provisioning components (Build Manager, Build Scripts, Boot Server, and the Media Server) **Server 2:** Model Repository, Access & Authentication Directory **Server 3:** Software Repository, Command Engine **Server 4:** Data Access Engine #2 **Server 5:** Opsware Command Center, Opsware Documentation
6	**Server 1:** Data Access Engine, OS Provisioning components (Build Manager, Build Scripts, Boot Server, and the Media Server) **Server 2:** Model Repository, Access & Authentication Directory **Server 3:** Software Repository, Command Engine **Server 4:** Data Access Engine #2 **Server 5:** Opsware Command Center, Opsware Documentation **Server 6:** Opsware Command Center #2

Overview of Multiple Data Access Engines in a Core

When you install multiple Data Access Engines in a core, you must make the following designations:

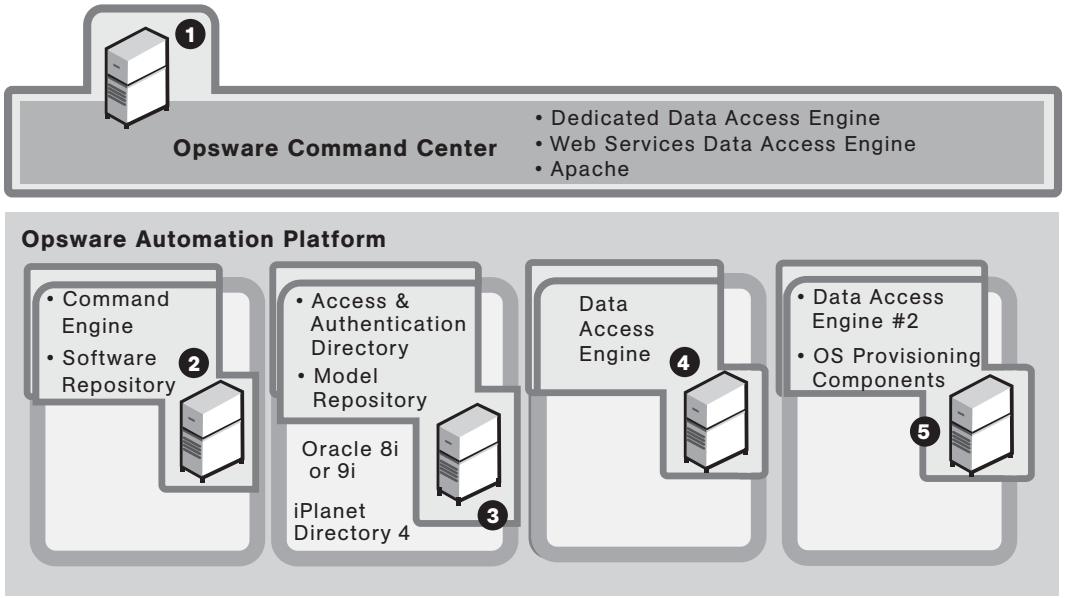
- **Primary Data Access Engine** – Each facility has only one primary Data Access Engine. This Data Access Engine periodically checks the managed servers to determine if the Opsware System can communicate with them. If a facility has more than one primary Data Access Engine, the competing reachability checks can interfere with each other.
- **Multimaster Central Data Access Engine** – This Data Access Engine performs the same functions as the primary Data Access Engine in a facility. Additionally, it generates multimaster state data periodically and resolves multimaster conflicts between facilities. Each multimaster mesh has only one Multimaster Central Data Access Engine. The Opsware core that contains the designated Multimaster Central Data Access Engine should not also have a primary Data Access Engine designated.
- **Secondary Data Access Engine** – When a facility has multiple Data Access Engines installed (for scalability), the additional ones are designated *secondary*. The first Data Access Engine installed is designated the Primary or Multimaster Central Data Access Engine. A secondary Data Access Engine does not check managed servers to determine if they are reachable. It only communicates with the Model Repository write or read data.

Example of an Opsware System Configuration

Figure 4-1 shows a five-server configuration that might typically be used to manage a facility with 4000 managed servers.

Opsware Inc. works closely with customers to design an infrastructure that meets their exact requirements. The following information is provided as a reference only.

Figure 4-1: Example Distribution of Opsware System Components



1. Sun Fire V480 (2CPU @1GB RAM per CPU, 36 GB drive)
2. Sun Fire 280R (2CPU @1GB RAM per CPU, 36 GB drive) + 29 GB Storage
3. Sun Fire V480 (2CPU @1GB RAM per CPU, 36 GB drive) + 3 GB Storage
4. Sun Fire 280R (2CPU @1GB RAM per CPU, 36 GB drive)
5. Sun Fire 280R (2CPU @1GB RAM per CPU, 36 GB drive)

In this example, the Opsware Command Center is hosted on a single Sun 220R server. The Command Engine and Software Repository are running together on the second server. The Access and Authentication Directory and Model Repository are run on a third 220R server, with the Data Access Engine running on a fourth 220R server. A second Data Access Engine is running on the fifth server with the OS Provisioning Components – the Build Manager, Build Scripts, Boot Server, and Media Server. Also, the two Data Access Engines are load balanced.

Scaling the Opsware System in Multiple Facilities

A typical Opsware System installation would locate an Opsware core in each managed facility in order to support global scalability. The size of the Opsware core in each facility can be scaled based on the number of servers managed in each facility.

Organizations can manage applications running in each facility or manage applications running in all facilities from a single location with the Opsware Command Center. Therefore, the number and location of Opsware Command Center instances is more flexible. The most common implementation is with two geographically distributed Opsware Command Centers.

In addition to full Model Repository replication, multimaster Opsware supports replication and caching of packages stored on the Software Repository. Typically the Opsware core in each facility will *own* the software that was uploaded to it. To support full disaster recovery, one or more full replicas can be maintained in remote Software Repository servers.

See "Overview of the Software Repository Replicator" on page 147 in Chapter 10 for more information.

Overview of Additional Instances of Opsware Components

If the Opsware System needs to support a larger operational environment, you need to install additional instances of the Data Access Engine, OS Provisioning Media Server, and Opsware Command Center.

The additional instances of the Data Access Engine and Opsware Command Center must be distributed correctly on servers in relation to the other components running in the core.

See "Distribution of Opsware System Components" on page 67 in this chapter for more information. This topic explains how to determine on which servers to install the additional Data Access Engine and Opsware Command Center.

The Opsware System does *not* support installing additional instances of the other components, such as the Command Engine or OS Provisioning Boot Server.

Installing Additional Instances of Opsware Components

You can install an additional instance of the Data Access Engine, Opsware Command Center, or OS Provisioning Media Server. Perform the following steps to install additional instances of Opsware components:

1. Using the response file created for the core, run the Opsware Installer on the server designated for the additional instance of the component. Do not include the `--interview` option.


```
/opsware_system/disk001/opsware_installer/install_opsware.sh
-r <full_path_to_response_file>
```

You must specify the full path to the script. You can run the Opsware Installer from any directory on the server except for any of the directories in the path to the Opsware Installer script (in the `/opsware_system/disk001` directory or subdirectories).

2. When the component selection menu displays, select and install the Data Access Engine, Opsware Command Center, or OS Provisioning Media Server.

   Depending on the type of core for which you are installing this additional instance (standalone or multimaster core), you install the standalone or multimaster version of the Opsware Command Center or Data Access Engine.

Reassigning the Data Access Engine to a Secondary Role

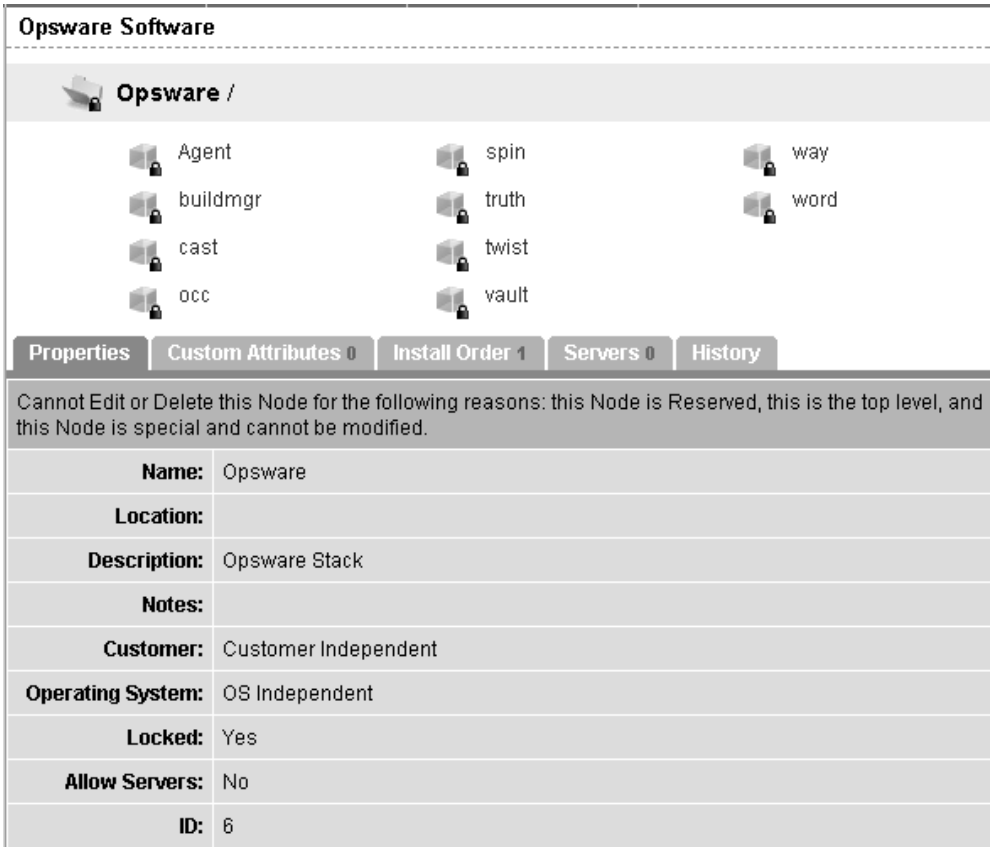
If an additional Data Access Engine was installed in a core, perform the following steps to reassign the new Data Access Engine to a secondary role:

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2 Click Administration ➤ Opsware Software from the navigation panel. The Opsware Software page appears, as Figure 4-2 shows.

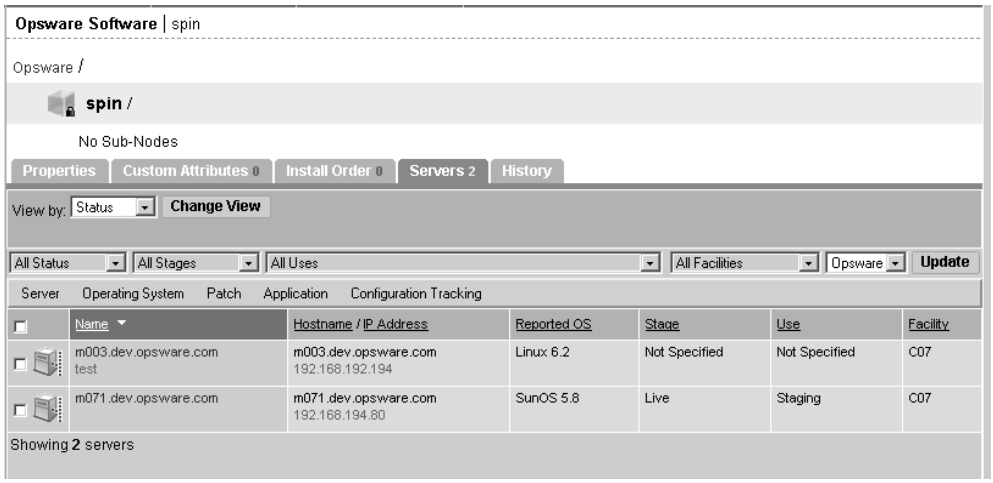
Figure 4-2: Opsware Software Page



3 Click the spin link. The Opsware Software | spin page appears.

4 Click the Servers tab. The list of servers that are running the Data Access Engine in the core appears, as Figure 4-3 shows.

Figure 4-3: List of Servers Running the Data Access Engine



5 Select the check box for the additional Data Access Engine server.

6 From the Server menu, choose Re-Assign Node.

7 Select the radio button for the Service Levels | Opsware | spin node.

8 Click the Select button.

9 Navigate the node hierarchy by clicking the following nodes:

- Opsware
- spin
- Secondary

10 Click the Re-Assign button.

11 Log in as root to the server running the additional Data Access Engine and enter the following command to restart the Data Access Engine:

```
/etc/init.d/spin restart
```


Chapter 5: Opsware Standalone Installation

IN THIS CHAPTER

This chapter describes the following tasks that you must perform in a standalone deployment:

- Running the Opsware Installer script to install a standalone Opsware core
- Verifying successful installation of an Opsware core in a facility

Overview of the Standalone Installation Process

Before you install a standalone Opsware core, you must satisfy the installation prerequisites, such as installing and configuring an Oracle database, setting up your network and domain name system to resolve Opsware host names, and copying the Microsoft patch management utilities to the host where you will install the Software Repository.

See “Installation Prerequisites” on page 15 in Chapter 3 for information about the exact prerequisites that you must meet before you install a standalone Opsware core.

A standalone installation involves installing a single Opsware core in a facility by running the Opsware Installer script `install_opsware.sh` to install the Opsware System components.

When you start the Opsware Installer, you are presented with the following installation choices:

1. Standalone Opsware Core
2. Multimaster Opsware Core – Subsequent Core
3. Convert a standalone Opsware Core to a multimaster core

For a standalone core installation, you select option 1 or 2 depending on how you need to scale the Opsware System to manage servers.

See “Opsware Core Scalability for Performance” on page 65 in Chapter 4 for more information.

An Opsware core can consist of a single server or the components can be distributed across multiple servers.

The process for installing a standalone core on a single server versus multiple servers is the same with the exception that you must copy some files from the first server to the other servers in the core before you run the Opsware Installer on them.

After you specify the type of standalone installation you want to perform (on one server or multiple servers), you must provide the required data for the installation by answering the prompts presented during the Opsware Installer interview. The interview prompts you for information about your environment, such as the addresses of DNS servers, database passwords, and so forth.

After the interview is complete and you provide *valid* answers for *every* prompt, you specify the components that you want to install on the server where you are running the Opsware Installer. When you run the Opsware Installer script, it presents you with a numbered list of components. The components are the components that make up the Opsware System, such as the Model Repository and the Software Repository.

1. The Model Repository (truth)
2. Access & Authentication Directory (cast)
3. Opsware Documentation
4. Opsware Command Center (occ)
5. Software Repository (word)
6. Data Access Engine (spin)
7. Command Engine (way)
8. OS Provisioning Build Scripts
9. OS Provisioning Boot Server
10. OS Provisioning Media Server

This Opsware Installer menu does *not* present the list of components in the order in which you must install them. Do *not* install the components in the order in which they are listed in this menu. You install the Model Repository first, then install the components one at a time in the order listed in step 11 on page 79 in “Installing a Standalone Core”.

On each server where you install an Opsware component, you must run the Opsware Installer script and select the component you want to install on that server. For example, if you are installing the Opsware components on six different servers, you must log into each of these servers, run the Opsware Installer script, and select the component that you want to install on that server.

After you successfully install an Opsware standalone core, you need to configure the OS Provisioning Subsystem for the facility in which the core is installed and set Opsware System parameters required to send Opsware System emails and specify certain contact information.

See "Distribution of Opsware System Components" on page 67 in Chapter 4 for more information. This topic provides information about how to determine which servers to install the components on. See "Opsware System Configuration Parameters" on page 85 in this chapter for more information. See "Required Configuration for the OS Provisioning Network" on page 98 in this chapter for more information.

Installing a Standalone Core

Before you install a standalone Opsware core, you must satisfy the installation prerequisites, such as installing and configuring an Oracle database and setting up your network and domain name system to resolve Opsware host names. You should have also determined which component distribution is required for the size of the managed environment. See "Installation Prerequisites" on page 15 in Chapter 3 for information about the exact prerequisites that you must meet before you install a standalone Opsware core.

1. Mount the Opsware System software on all core servers by mounting the CD or NFS-mounting a directory containing the CD contents.

   The Opsware Installer must have root read/write access to the directories where it installs Opsware components, even NFS-mounted network appliances.

2. On the server where Oracle was installed, invoke the Opsware Installer with no command line options:

   ```
   /opsware_system/disk001/opsware_installer/install_opsware.sh
   ```

You must specify the full path to the script. The directory path shown in this step assumes that you copied the Opsware System CDs to local disk or network share using the required directory structure.

See “Installation Media for the Opsware Installer” on page 13 in Chapter 2 for more information.

If you are running the Opsware Installer from a CD, you cannot run the installation while under the CD mount point.

You must install the Model Repository on the server where Oracle was installed. See “Installation and Configuration Requirements for Oracle” on page 35 in Chapter 3 for more information. This topic provides information about how Oracle is required to be installed.

You can run the Opsware Installer from any directory on the server except for any of the directories in the path to the Opsware Installer script (in the `/opsware_system/disk001` directory or subdirectories).

The Welcome Menu appears for the Opsware Installer, which prompts you to select the type of installation.

3 Select option 1, Standalone Opsware Core – Single Server or option 2, Standalone Opsware Core – Multiple Servers.

The Opsware Installer interview phase begins. In this phase, you specify information about the environment in which the Opsware core will run.

4 Complete the interview.

See “Description of Required Information for Installation” on page 42 in Chapter 3 for more information.

When you run the interview, the path for the Windows OS provisioning media must already exist on the server where you will install the OS Provisioning Media Server component.

When you enter all required information for installation, the Opsware Installer displays this message:

```
NOTE: All parameters have values. Hit control-F to finish the
interview.
```


If you do not enter `control-F` and press `Enter` to continue to the next prompt, the Opsware Installer has you validate the data you entered previously by displaying the prompt again and showing, in brackets [ ], the value that you previously entered.

5. After you provide all information in the interview, enter `control-F` to finish the interview and create a response file for the installation of the core.

   See "About the Interview" on page 12 in Chapter 2 for more information. This topic provides information about how the Opsware Installer works with the response file.

   The Opsware Installer prompts you to indicate whether you want to continue the installation by using the response file. Enter "y" to continue.

6. When the component selection menu displays, select and install the Model Repository (truth) option.

7. If you are installing the Opsware core on multiple servers, copy the response file that the Opsware Installer generated to all other servers in this core. (When you installed the first component, you were prompted for a location in which to save the response file.)

8. On the server where you want to install the Data Access Engine (spin), invoke the Opsware Installer with the newly generated response file by entering the following command line:

   ```
   /opsware_system/disk001/opsware_installer/install_opsware.sh
   -r <full_path_to_response_file>
   ```

9. Select and install the Data Access Engine (spin) option. When prompted to generate cryptographic material during Data Access Engine installation, answer "y".

10. If you are installing the Opsware core on multiple servers, copy the database of cryptographic material from the following directory to every core server:

    ```
    /var/lc/crypto/cadb/realm/opsware-crypto.db.e
    ```

    If necessary, first create the directory `/var/lc/crypto/cadb/realm` on each core server. The directory and database need to be readable by the root user.

11. Install the remaining Opsware components on the server designated for each component by running the Opsware Installer with the response file. You must install each component by a separate invocation of the Opsware Installer script even if you are installing some or all of the components on the same server.

```
/opsware_system/disk001/opsware_installer/install_opsware.sh
-r <full_path_to_response_file>
```

You must install the OS Provisioning Build Scripts on the server that was specified during the interview at the prompt asking for the IP address or host name of the Build Manager.

This Opsware Installer menu does *not* present the list of components in the order in which they must be installed. You *must* install the remaining components one at a time in the following order:

1. Access & Authentication Directory (cast)
2. Command Engine (way)
3. Software Repository (word)
4. OS Provisioning Build Scripts
5. OS Provisioning Boot Server
6. OS Provisioning Media Server
7. Opsware Documentation
8. Opsware Command Center (occ)

You must install the Opsware Documentation component on the server where you install the Opsware Command Center component. Install the Opsware Documentation component before you install the Opsware Command Center component. If you install the Documentation after installing the Opsware Command Center, you must restart the Opsware Command Center component.

If the following message appears while you install an Opsware component, you forgot to copy the database of cryptographic material to the server where you are installing the component:

```
Database with cryptographic material not found.
Would you like Opsware Installer to generate new database of
cryptographic material?
```

12 Reboot the server running the OS Provisioning Boot Server component and the server running the OS Provisioning Media Server component.

If the Boot Server and Media Server are installed on a host where other Opsware components are installed (for example, all components are installed on a single server), you must restart the processes for these components as well. When you restart multiple Opsware components, you must restart them in the correct order.

See the *Opsware System 4.7 Administration Guide* for information about the correct restart sequence for Opsware System components.

13 If the Model Repository, Boot Server, or Access & Authentication Directory exists on a server with no other Opsware components installed on it, you must manually install an Opsware Agent on that server.

Opsware System 4.5 User's Guide for information about the procedure to install an Opsware Agent on a server.

14 (Optional) Install additional instances of the OS Provisioning Media Server, Data Access Engine, and Opsware Command Center depending on how you need to scale the Opsware System for performance.

See "Opsware Core Scalability for Performance" on page 65 in Chapter 4 for more information.

15 Set configuration parameter values that the Opsware System requires to send email notifications and alerts, and to display the Opsware administrator contact information.

See "Opsware System Configuration Parameters" on page 85 in Chapter 6 for more information.

16 Configure the OS Provisioning Subsystem for the facility.

See "Overview of Network Configuration for OS Provisioning" on page 97 in Chapter 7 for more information.

Verifying Successful Installation of an Opsware Core

After you install an Opsware System core, you should perform the following tasks to determine that the installation was successful and to troubleshoot any problems that might have occurred. Performing these tasks verifies the basic functionality of the Opsware System in the facility.

1 Log in to Opsware Command Center and run the Opsware System Diagnosis by clicking System Diagnosis under Administration in the navigation panel.

Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

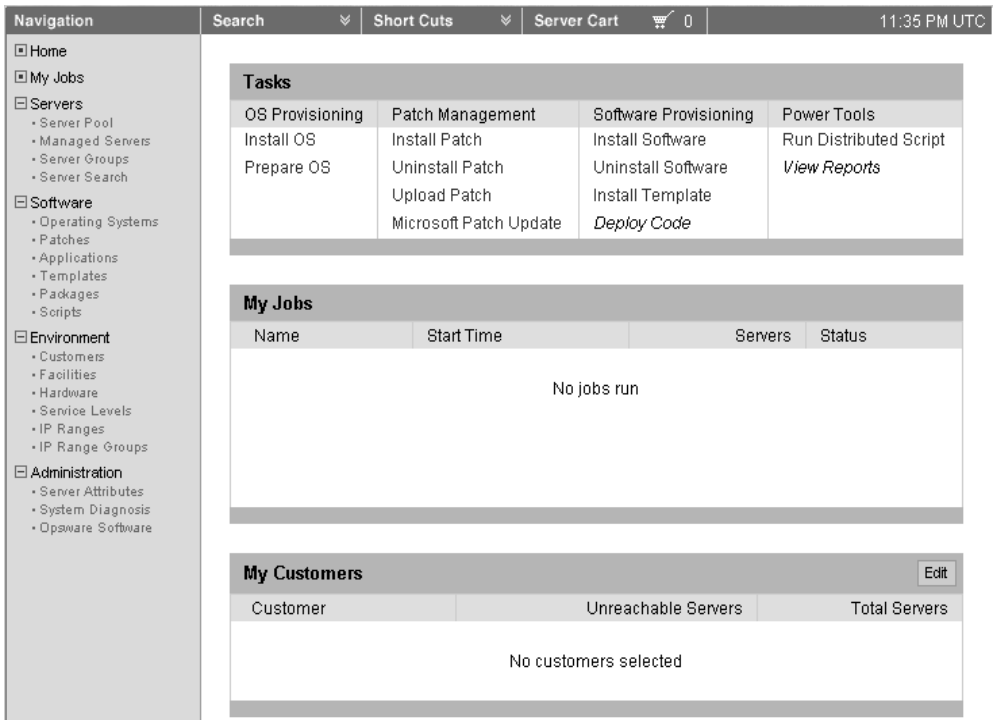
See the *Opsware System 4.7 Administration Guide* for information about the procedures for running the system diagnosis tool.

2. Create a new user by using the Users & Groups page under Administration and assign the user basic privileges (include the user in the "Basic" user group). After creating the user, log in as that user to check that the user is given the appropriate access.

   See the *Opsware System 4.7 Administration Guide* for information about the procedures for creating Opsware users.

3. While you are logged into the Opsware Command Center as the user you just created, exercise different Opsware System functions by clicking the links in the left navigation panel and by opening the wizards on the home page. See Figure 5-1.

Figure 5-1: Opsware Command Center Home Page and Navigation



4. Install an Opsware Agent on a server running in the operational environment.

See the *Opsware System 4.5 User's Guide* for information about the procedure to install an Opsware Agent on a server.

5. Upload a software application to the Opsware Software Repository by using the Packages feature in Opsware Command Center.

   See the *Opsware System 4.5 User's Guide* for information about the steps to upload a package.

6. Install the uploaded package on the managed server.

   See the *Opsware System 4.5 User's Guide* for information about Application Provisioning Setup and Application Provisioning.

7. Set up synchronization between two managed servers by using the Code Deployment & Rollback Subsystem in Opsware Command Center. Test the synchronization after you set it up.

   See the *Opsware System 4.5 User's Guide* for information about the steps to set up the CDR subsystem.

8. If you configured the OS Provisioning Subsystem by using the Opsware DHCP Tool, set up the OS Provisioning Subsystem. Then use this subsystem to install an operating system on a managed server.

See the *Opsware System 4.5 User's Guide* for information about OS Provisioning Setup and Operating System Provisioning.

If you have any problems during this process, you can search the Opsware Knowledge Base at

engsupport.opsware.com/

for troubleshooting directions and solutions, or contact our support organization for further help (support@opsware.com).

Chapter 6: Opsware System Configuration

IN THIS CHAPTER

This chapter describes the following tasks that you must perform after you install an Opsware core so that the Opsware System configuration is complete:

- Configure required email address for the Configuration Tracking Subsystem
- Configure required email address for the Opsware System when operating in multimaster mode
- Configure required email addresses for the Opsware Agent to use when notifying users about scheduled operations
- Set the mail server for a facility in which an Opsware core is installed
- Set the Opsware administrator contact information that appears in the Opsware System Help page
- Configure required email addresses for the Code Deployment & Rollback Subsystem
- Configure password policy parameters

These tasks *must* be performed after you have successfully installed an Opsware standalone core or a subsequent Opsware core in a multimaster mesh.

Opsware System Configuration Parameters

This chapter documents how to set specific parameters after you install an Opsware core so that the Opsware System properly sends email alerts and displays the correct support contact information for your organization.

Where a value for a configuration parameter *must* be set for an installation of an Opsware core, this guide provides instructions for setting the value. Set configuration values for those parameters as *explicitly* directed by the steps in the installation procedures.

Do not change other configuration values, unless *explicitly* directed to do so by this guide or by your Opsware Support Representative.

After you install an Opsware core, you should set several configuration parameter values that the Opsware System uses to send email notifications and alerts, and to display the Opsware administrator contact information.

These values are set by selecting Administration ➤ System Configuration in the Opsware Command Center.

Configuring Contact Information in the Opsware Help

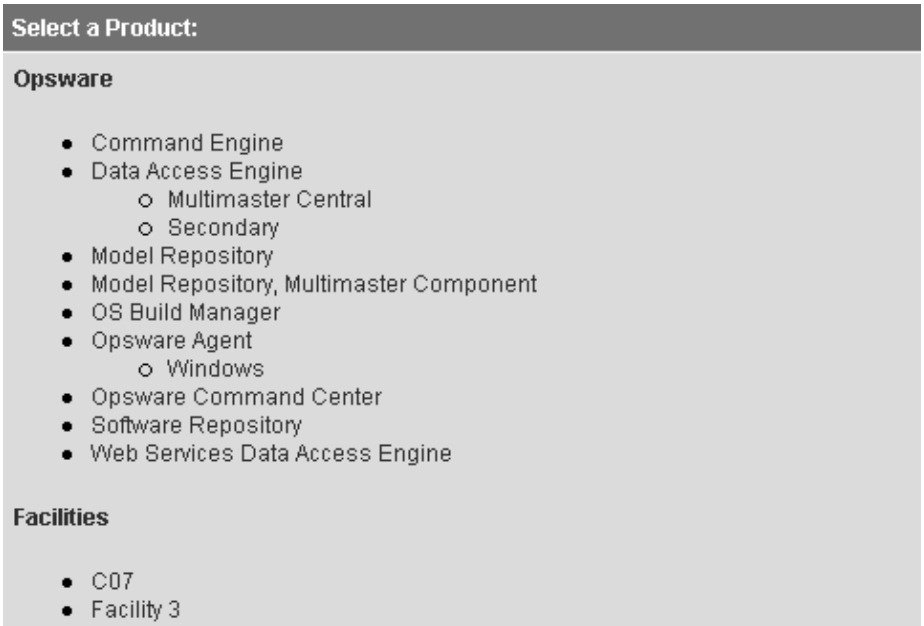
Perform the following steps to configure the Opsware administrator contact information that appears in the Opsware System Help page:

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2 From the navigation panel, click System Configuration under Administration. The Select a Product page appears, as Figure 6-1 shows.

Figure 6-1: Select a Product page in the Opsware System Configuration



3 Under Select a Product, click the link for the Opsware Command Center. The configuration page for the Opsware Command Center appears.

4 Configure the following contact information by setting these parameters:

- In the field **owm.name.opswareadministratorphonenumber**, enter the telephone number for your organization's Opsware System support.
- In the field **owm.name.opswareadministratoremail**, enter the email address for your organization's Opsware System support.

5 Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

Configuring the Mail Server for a Facility

Perform the following steps in an Opsware multimaster mesh to configure the mail server for the core running in *each* facility.

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3. Under Select a Product, click the link for the facility name. The configuration page for the facility appears.

   Opsware components use the parameter `opsware.mailserver` to determine the address of the mail server to use. If a value is not entered in the field, by default, the value of `opsware.mailserver` is smtp. If managed servers are able to contact a mail server by using this name as the address, then you do not need to modify this parameter.

4. In the field **opsware.mailserver**, enter the host name of the mail server.

5. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

6. Restart the Command Engine and Opsware Command Center.

7. If the Opsware System is running in multimaster mode, restart the Multimaster Replication Engine (running on the server where the Model Repository is installed).

   When restarting multiple Opsware components, you must restart them in the correct order.

   See *Opsware System 4.5 User's Guide* for information about the correct restart sequence for Opsware System components.

Setting Email Alert Addresses for an Opsware Core

You should configure these email alert addresses before you install an Opsware Agent on the servers in your operational environment because the Opsware Agent on a managed server will *only* read this email configuration information the first time it contacts the Opsware System.

Perform the following steps to configure these email alert addresses. The Opsware Installer installs an Opsware core with placeholder values (EMAIL_ADDR) for these parameters.

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3. Under Select a Product, click the Opsware Agent link. The configuration page for the Opsware Agent appears.

4. Configure the following required email alert addresses:

   - In the field **acsbar.ErrorEmailAddr**, enter the address that the Opsware System will send warning emails to when any configuration tracking limit is exceeded (for example, when the configuration tracking feature stopped backing up configuration files and databases).
   - In the field **acsbar.emailFromAddr**, enter the address that the Opsware Agent will use as the email From address in the emails when the Opsware System detects a tracked configuration change.
     Recommendation – use agent@yourdomain.com.
   - In the field **CronbotAlertAddress**, enter the email address that the Opsware Agent will use to alert the recipient about failed scheduled jobs.
   - In the field **CronbotAlertFrom**, enter the email address that the Opsware Agent will use as the email From address in the emails about failed scheduled jobs.
     Recommendation – use agent@yourdomain.com.

5. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

Configuring Email Alert Addresses for Multimaster

Perform the following steps to configure email alert addresses for multimaster. The Opsware Installer installs an Opsware core with placeholder values (EMAIL_ADDR) for these parameters.

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3. Under Select a Product, click the Model Repository, Multimaster Component link. The configuration page for the Model Repository, Multimaster Component appears.

4. Configure the following email parameters:

   - In the field **sendMMErrorsTo**, enter the email address to which multimaster conflicts will be sent.
   - In the field **sendMMErrorsFrom**, enter the address that the Opsware System will use as the email From address in the emails when multimaster conflicts are detected.

5. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

6. Restart the Multimaster Replication Engine (running on the server where the Model Repository is installed) in all Opsware cores in the multimaster mesh.

   See *Opsware System 4.7 Administration Guide* for information about the correct restart sequence for Opsware System components.

Configuring Email Notification Addresses for CDR

You can set up email notification addresses for the Opsware Code Deployment & Rollback Subsystem. When users request that a service operation or synchronization be performed on their behalf, an email notification is sent to the individuals assigned to perform the requested service operation or synchronization.

Perform the following steps to configure email notification addresses for CDR. The Opsware Installer installs an Opsware core with placeholder values (EMAIL_ADDR) for these parameters.

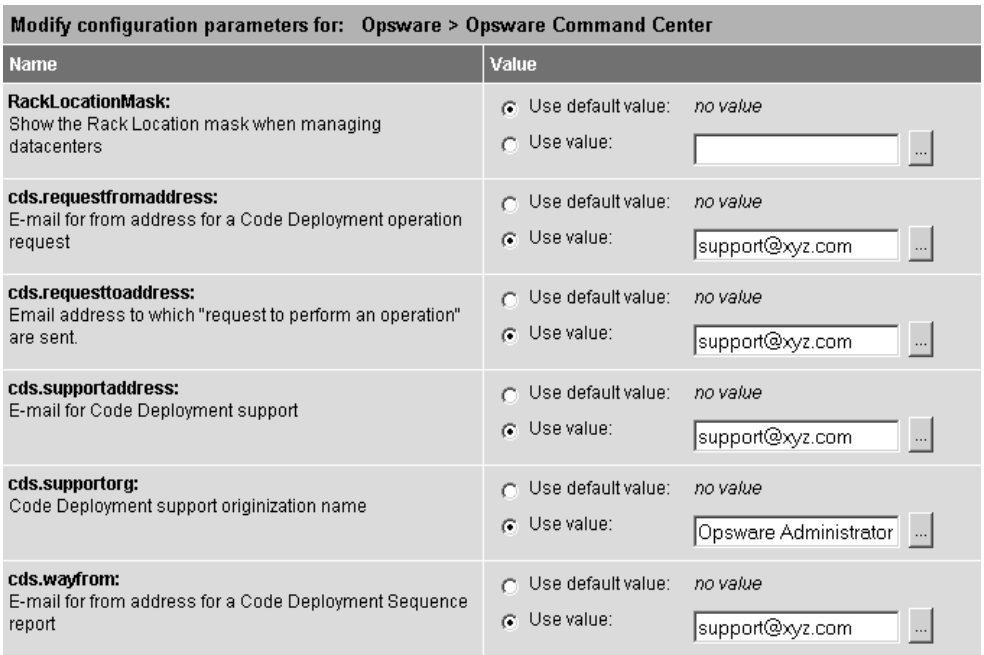
1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3. Click the link for the Opsware Command Center. The configuration page for the Opsware Command Center appears, as Figure 6-2 shows.

Figure 6-2: CDR Email Notification Configuration Parameters



4. Customize the following parameters to include the following email notification information:

   - In the field **cds.requesttoaddress**, enter the email address to include in the “To:” field of the email message for a request notification.
   - In the field **cds.requestfromaddress**, enter the email address to include in the “From:” field of the email message for a request notification.
   - In the field **cds.wayfrom**, enter the email address to include in the “From:” field of the email message sent following completion of a sequence.
   - In the field **cds.supportaddress**, enter the email address to include for a facilities' support organization or contact person.

- In the field **cds.supportorg**, enter the display name of a facilities' support organization.

5. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.
6. Restart the Command Engine, Opsware Command Center, and the Multimaster Replication Engine (running on the server where the Model Repository is installed).

   When you restart multiple Opsware components, you must restart them in the correct order.

   See the *Opsware System 4.7 Administration Guide* for information about the correct restart sequence for Opsware System components.

Overview of Password Policy Parameters

The Opsware administrator can enable and configure the password policy parameters for accessing the Opsware Command Center. The passwords will be checked against the configured parameters when user accounts are created by the Opsware administrator or when the passwords are changed by the users or the administrator. The users, including the administrators will be alerted with an error message if their password does not match the criteria specified in the configured password policy parameters.

Enabling and Disabling Password Policy Parameters

Perform the following steps to disable the password policy parameters for accessing the Opsware Command Center.

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. The Opsware Command Center home page appears.
2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.
3. Under Select a Product, click the Opsware Command Center link. The Modify Configuration Parameters for the Opsware Command Center page appears.

4 To enable the password policy parameters, in the field **owm.features.MiniPasswordPolicy.allow**, enter `true` as Figure 6-3 shows. The default value is false.

Figure 6-3: Enabling Password Policy Parameters

OR

In the field **owm.features.MiniPasswordPolicy.allow**, select the default value (`false`) as Figure 6-4 shows. If you select the default value, the password will be checked to ensure that it has atleast 6 characters.

Figure 6-4: Disabling Password Policy Parameters

5 If you have enabled the password policy parameters, See “Configuring Password Policy Parameters” on page 93 in this chapter for information about how to configure the password policy parameters.

6 If you have disabled the password policy parameters, click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

Configuring Password Policy Parameters

Perform the following steps to enable and configure the password policy parameters for accessing the Opsware Command Center.

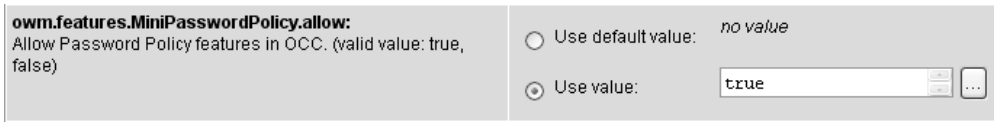
1 Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. The Opsware Command Center home page appears.

2 From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3 Under Select a Product, click the Opsware Command Center link. The Modify Configuration Parameters for the Opsware Command Center page appears.

4 In the field **owm.features.MiniPasswordPolicy.allow**, enter `true` as Figure 6-5 shows.The default value is false.

Figure 6-5: Enabling Password Policy Parameters

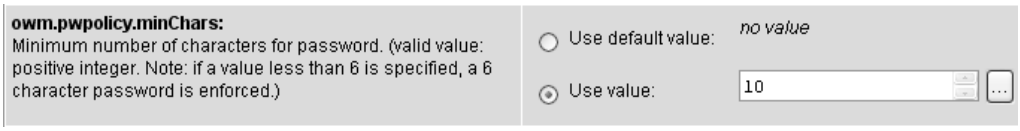


5 In the field **owm.pwpolicy.maxRepeats**, enter a value specifying the maximum number of consecutive repeating charaters allowed for a password. The value entered must be greater than 0; the default value is 2. See Figure 6-6.

Figure 6-6: Configuring Maximum Number of Repeating Characters for a Password

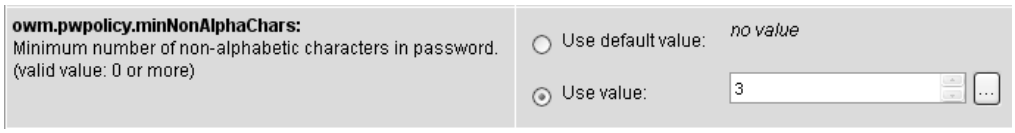
6 In the field **owm.pwpolicy.minChars**, enter a value specifying the minimum number of characters required for a password. The value must be a positive integer; the default value is 6. See Figure 6-7.

Figure 6-7: Configuring Minimum Number of Characters for a Password



7 In the field **owm.pwpolicy.minNonAlphaChars**, enter a value specifying the minimum number of non-alphabetic characters required for a password. The value cannot be greater than the value specified for the minimum character limit; the default value is 0. See Figure 6-8.

Figure 6-8: Configuring Non-alphabetic Characters for a Password



8 Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

Chapter 7: OS Provisioning Configuration

IN THIS CHAPTER

This chapter provides the following information for setting up the OS Provisioning Subsystem after you install an Opsware core in a facility:

- A description of the network requirements for the OS Provisioning Subsystem in a facility
- How to use the Opsware DHCP Network Configuration Tool to configure a local or remote network for OS provisioning

Overview of Network Configuration for OS Provisioning

Opsware OS provisioning uses DHCP to allow network booting and configuration of unprovisioned servers in the Server Pool. DHCP is also used to configure networking on newly provisioned servers that have not been assigned a static network configuration.

When you install the Opsware Boot Server component, the Opsware Installer also installs an Internet Software Consortium DHCP server (`ISC dhcpd`), and includes a default configuration file (`dhcpd.conf`) and the Opsware DHCP Network Configuration Tool.

`dhcpd` is the ISC DHCP server process that provides the configuration information contained in the `dhcpd.conf` configuration file. The included `dhcpd.conf` file provides the neccessary parameters to support network booting of Sun hardware (a DHCP-capable PROM is required) and x86 hardware (a PXE-compatible system is required).

For x86 hardware that does not support PXE, the server can be booted from a CD. When a boot CD is used, the DHCP server still provides network configuration information to the host.

The DHCP Network Configuration Tool is a menu-driven utility that allows you to customize the dhcpd configuration file (`dhcpd.conf`) for your environment. Running the tool prompts you for network information needed to configure DHCP for each OS

provisioning network. Using the DHCP Network Configuration Tool simplifies configuration of the DHCP server and ensures that the DHCP configuration contains the options that are needed for the OS Provisioning Subsystem to function properly.

If you need to configure other DHCP values not handled by the DHCP Network Configuration Tool, see the ISC documentation on the configuration file format.

Using the Opsware DHCP Network Configuration Tool, you can customize the dhcpd.conf file to support common local and remote network configurations.

If you need to configure network for the Opsware OS Provisioning Subsystem to support non-standard configurations (for example, dual-interfaces with split-horizon DNS requirements, private build networks, or static NAT), you must modify the dhcpd.conf file manually. Contact Opsware Support for more assistance.

Required Configuration for the OS Provisioning Network

A network must only have one DHCP server responsible for it. Otherwise, conflicts occur when more than one DHCP server attempts to answer a DHCP request. Check with your network administrator before you configure any networks with the DHCP Network Configuration Tool.

The DHCP server can provide service to two types of networks:

- **Local networks** – Networks that are attached directly to the network interfaces of the host on which the DHCP server runs. No special network configuration is needed to support local networks.
- **Remote networks** – Networks that are not directly attached to the DHCP server host. A router sits between the DHCP server host and the remote networks. For remote networks, a DHCP proxy (sometimes called IP helper) must be configured on each remote network to relay DHCP packets to the DHCP server host.

  A DHCP proxy is *not* provided with the Opsware System and instructions for setting one up are beyond the scope of this document. DHCP proxy functionality is often included in modern routers. Check with your network administrator or router vendor.

Additionally, in some environments, multiple IP networks (layer 3) are layered on top of a single VLAN (layer 2). While this configuration is supported by the ISC DHCP server, generally such a topology requires careful consideration to work properly with DHCP. Therefore, the DHCP Network Configuration Tool can only configure a single IP network per VLAN.

Required Information for the DHCP Network Configuration Tool

Before you use the DHCP Network Configuration Tool to configure any OS provisioning networks, you need the following information for each network to be configured:

- The network address and size (netmask or bits). For example, 192.168.0.0/255.255.255.0 or 192.168.0.0/24. Both specify a network range of 192.168.0.0 - 192.168.0.255.
- The network gateway or default router. For example, this value might be 192.168.0.1 in the example network.
- The range of IP addresses that are assigned dynamically by the DHCP server. For example, 192.168.0.11, 192.168.0.20 might be used to configure a pool of 10 addresses. **Important:** Each of these IP addresses must resolve to a host name on the DNS server.
- The IP addresses of one or more DNS servers. The servers given must be able to resolve the standard required Opsware DNS entries. The DNS servers do not need to be on the same network that is being configured.
- A default DNS domain. This domain must include the standard, required Opsware DNS entries. For example, if the default DNS domain is `example.org`, then there must be an entry `spin.example.org` that can be resolved by the DNS servers.

Configuring Networks for OS Provisioning

The DHCP Network Configuration Tool is installed with the Opsware Boot Server component. Perform the following steps to configure networks for OS provisioning:

1. Log in as root to the server running the Opsware Boot Server component and enter the following command:

   ```
   /opt/OPSWdhcpd/sbin/dhcpdtool
   ```

   The DHCP Network Configuration Tool main menu appears, as Figure 7-1 shows.

2. To add a new network, enter `a`.

Figure 7-1: DHCP Network Configuration Tool Main Menu

3 To configure the DHCP service on the local network, enter `l`, as Figure 7-2 shows. Local networks are detected automatically and displayed. When configuring local networks, the network address, network size, and network gateway are supplied for you.

OR

To add a remote network, enter `r`. For remote networks, you need to supply information for the network address, network size, and network gateway.

Figure 7-2: Menu to Add Local or Remote Networks

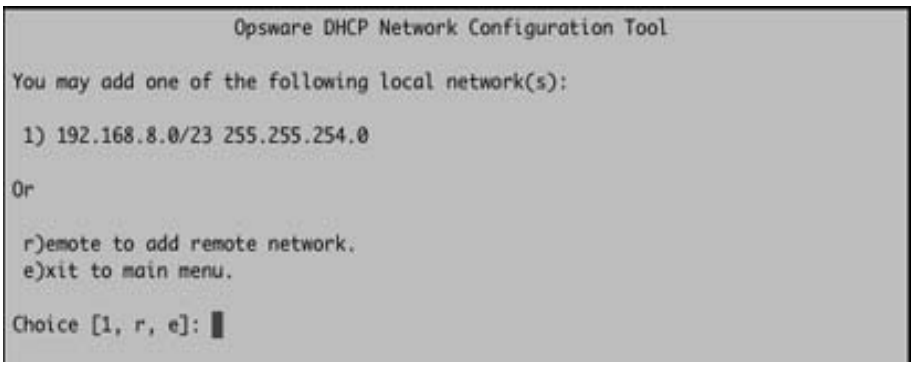


Figure 7-3 and Figure 7-4 show how to configure a local network and a remote network.

Figure 7-3: Example for Configuring a Local Network

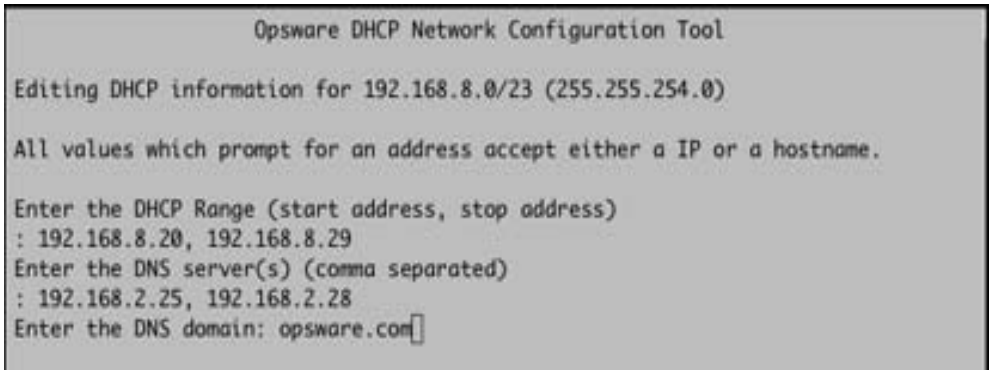
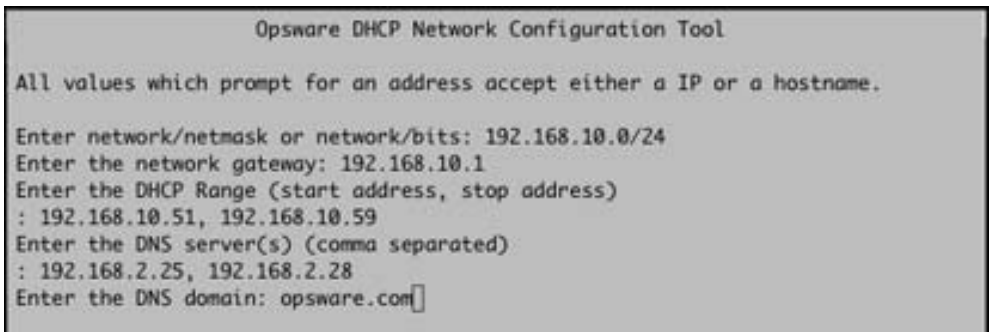
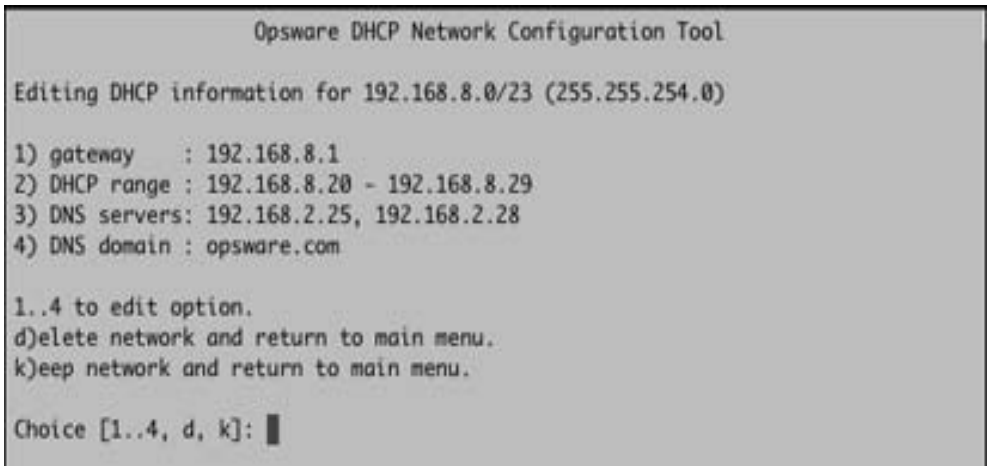


Figure 7-4: Example for Configuring a Remote Network



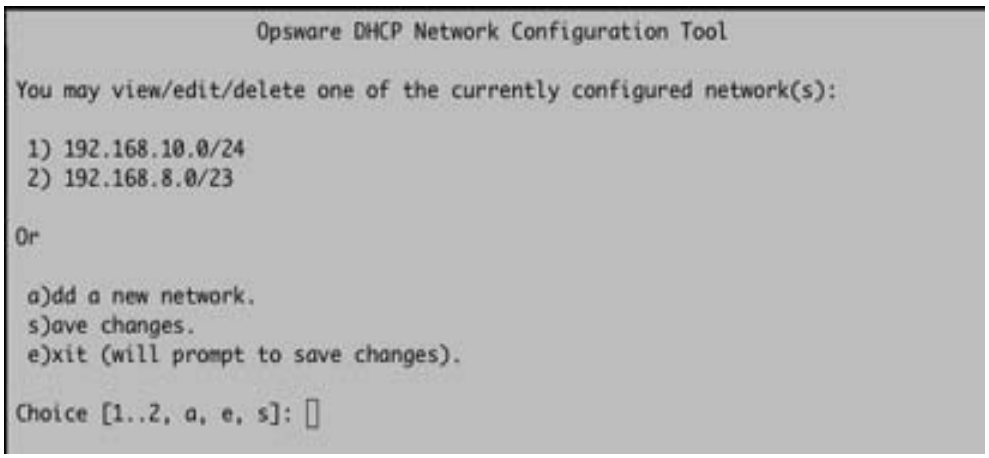
After you configure a local or remote network and return to the main menu, the DHCP Network Configuration Tool displays the new network and a summary of each configured network, as Figure 7-5 shows.

Figure 7-5: Summary of Network Information



4 If the displayed information is correct, enter `k` to keep the network and return to the main menu.

Figure 7-6: Networks Displayed in the Main Menu



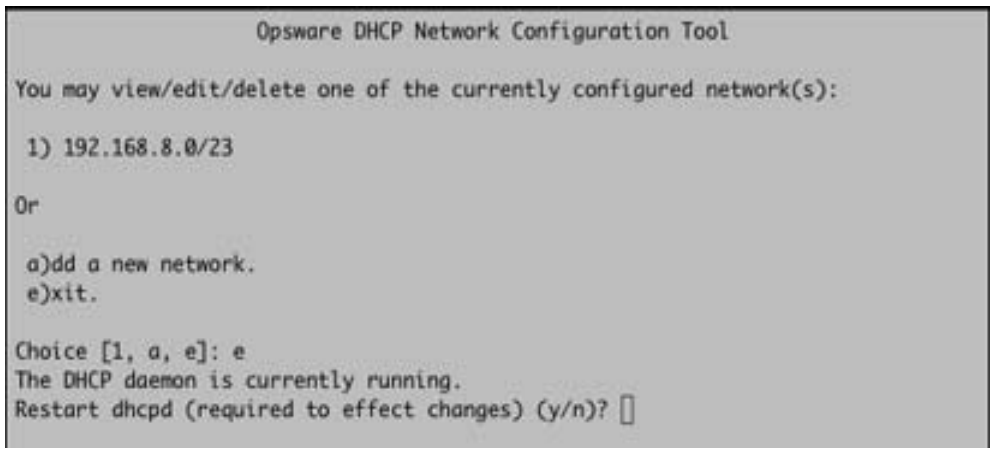
5 (Optional) Select the number of a network to edit its values.

6 (Optional) To continue to add new networks, enter `a` and repeat Steps 3 and 4.

7 When you are done adding networks and editing their values, enter `s` to save the changes.

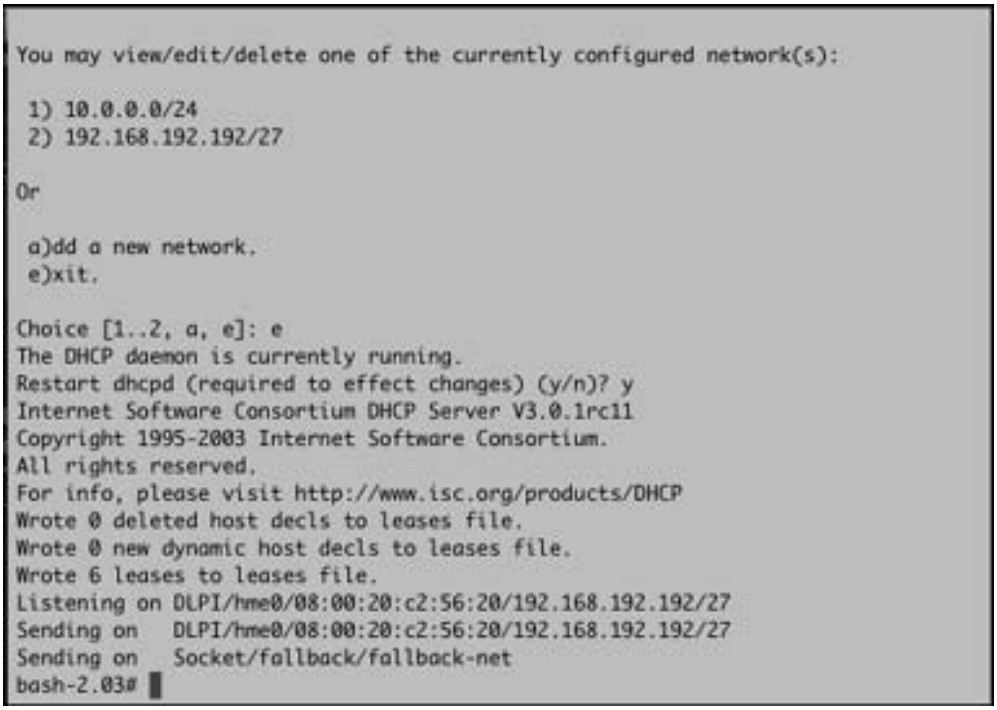
8 To exit the DHCP Network Configuration Tool, enter `e`. You are prompted to start (or restart) the DHCP server process, as Figure 7-7 shows.

Figure 7-7: DHCP Network Configuration Tool Prompt to Restart DHCP Process



9 To restart the DHCP server process, enter `y`. The DHCP Network Configuration Tool displays diagnostic output as part of its startup, as Figure 7-8 shows.

Figure 7-8: Diagnostic Output when Restarting the DHCP Network Configuration Tool



References for Managing the DHCP Server

To start the DHCP server process, enter the following command on the server running the Opsware Boot Server:

```
/etc/init.d/dhcpd start
```

To stop the DHCP server process, enter the following command on the server running the Opsware Boot Server:

```
/etc/init.d/dhcpd stop
```

The DHCP configuration file is `/opt/OPSWdhcpd/etc/dhcpd.conf`. This file can be edited for advanced configurations. Documentation is available at the ISC Web site `www.isc.org`.

Additionally, man pages for the DHCP Network Configuration Tool are installed in

/opt/OPSWdhcpd/man on the Boot Server. They are also available at the Opsware Support Web site.

The DHCP leases file is /var/opt/OPSWdhcpd/dhcpd.leases. Normally, this file should not need editing.

Log messages that the DHCP server produces are sent to the standard Unix syslog process with the daemon facility. Consult your vendor documentation on how to configure and view syslog messages.

Creating a Linux Boot Image

The Opsware System includes a command line utility, OPSWlinuxdbootiso, that you can use to create a Linux Boot Image on CD.

1. In the Opsware Command Center, search for the package name OPSWlinuxdbootiso* and operating system Red Hat Enterprise Linux AS 3.0. See "Searching for Packages" on page 290.
2. Download the package to a server or desktop running Linux. "Downloading a Package" on page 306 for information.
3. On the server or desktop where you downloaded the OPSWlinuxdbootiso utility, verify that version 1.10-4 of the mkisofs utility is installed.
4. From the following directory, run the mkcdrom.sh script:

   ```
   /opt/OPSWlinuxbootiso>./mkcdrom.sh
   ```

   ```
   Usage: ./mkcdrom.sh <outputiso> sin:/opt/OPSWlinuxbootiso>./
   mkcdrom.sh /tmp/boot.iso
   ```

5. At the prompts, enter the following information:
   - The IP address or hostname of Build Manager (default hostname: buildmgr).
   - The port for the OS Build Agent to use to contact the Build Manager [default: 1017].
   - The IP address or hostname of the Boot Server (default hostname: buildmgr).
   - The path to the media for the OS Build Agent (default path: /opt/OPSWboot/kickstart).
   - The server from which to run Linux Kickstart.

Running the OPSWlinuxdbootiso utility creates an iso file that you can write to CD-ROM.

Chapter 8: Opsware Multimaster Installation

IN THIS CHAPTER

This chapter describes the following tasks that you must perform in a multimaster installation:

- Run the Opsware Installer script to install a multimaster system by upgrading a standalone core to multimaster and by installing subsequent Opsware cores
- Use the Opsware Command Center to set certain configuration parameters for a multimaster Opsware System
- How to verify that multimaster traffic is flowing between the Opsware cores after the multimaster system is configured

Overview of Multimaster Installation

A multimaster installation involves installing the Opsware System in multiple facilities and configuring the Opsware cores to communicate with each other.

The first facility is sometimes referred to as the *source* or *master* facility, because the subsequent Opsware System cores start with a copy of the data from the Model Repository database at the source facility. After all the facilities are up and running, however, there is no real distinction between the source and target facilities. All Model Repository databases are masters.

After you set up and configure the multimaster mesh with two facilities, you can add additional facilities to the mesh.

The procedure for installing a second core and the procedure for installing a third core or more are similar. However, there are some differences between the procedures to minimize downtime for the existing facilities when you install a third core.

About a Source Core Upgrade for Multimaster

Before you install the second core in a multimaster mesh, you must upgrade some of the Opsware components to multimaster mode by running the Opsware Installer once per component that needs to be upgraded on the server where the standalone version of the component is installed. You must upgrade the following components:

- The Model Repository (truth)
- The Data Access Engines (spin)

  If an Opsware core has multiple Data Access Engines installed, you must upgrade all of them.
- Opsware Command Center (occ)
- Software Repository (word)
- Command Engine (way)

For example, if you are upgrading the Model Repository and Software Repository running on a server, you must run the Opsware Installer to update the Model Repository on the server, and then you must run the Opsware Installer a second time on the server to update the Software Repository.

Additionally, you must install the Multimaster Infrastructure Components on the server where the Model Repository is installed.

About Target Core Installations

You install secondary Opsware System cores (called *target* cores) by following many of the procedures you used to install a standalone core.

See “Requirements for the Opsware System” on page 21 in Chapter 3 for more information. This section provides information about database, system, and network requirements for a standalone core.

You must meet the same requirements before you can begin the installation of additional Opsware System cores. You must also meet the requirements for installing a multimaster mesh.

See “Requirements Between Multimaster Facilities” on page 28 in Chapter 3 for more information.

Site Planning for Target Cores

The components that make up a target core can be installed on one or multiple servers.

See "Before You Install the Opsware System" on page 15 in Chapter 3 for more information. This section describes the decisions you must make and tasks you must perform before you install subsequent cores.

As described in this section, you should decide where you want to install each of the components that make up the Opsware core before you run the Opsware Installer script.

Facility Name and ID

Each target facility must have a distinct facility ID and facility name.

When you create the target facility at the source facility, the Opsware Command Center creates the facility ID automatically. You can find the facility ID for any facility by logging into the Opsware Command Center at the source facility. From the navigation panel, select Facilities under Environment and click the facilities' name.

See "Identifying the Facilities" on page 16 in Chapter 3 for more information.

Authorization Domain

All subsequent deployments in a multimaster mesh must use the same authorization domain that is used in the first or source deployment, where the master Model Repository is installed. You set the authorization domain when you entered this information in the interview while installing the source core (the first standalone core).

See "Identifying the Authorization Domain" on page 16 in Chapter 3 for more information.

Components for Target Cores

You must install the following Opsware System components in all subsequent facilities that will be added to the multimaster mesh:

- Software Repository, Multimaster Component (slave)
- Model Repository, Multimaster Component (slave)
- Opsware Documentation
- Opsware Command Center, Multimaster
- Software Repository, Multimaster
- Multimaster Infrastructure Components (vault)

- Command Engine, Multimaster
- Data Access Engine, Multimaster

Target facilities in the multimaster mesh are *not* required to have an Opsware Command Center installed. Instead, you can manage the facility from any site in the multimaster mesh that does have an Opsware Command Center installed.

You need to install the Opsware Command Center only if you want to manage your multimaster mesh locally from that facility or if you want to have a backup Opsware Command Center.

This installation guide documents how to manage all the facilities in a multimaster installation by a single Access & Authentication Directory, which is installed at the first facility (the source facility). In this configuration an Opsware Access & Authentication Directory is installed at the source facility. All other facilities set up their deployment so that the Access & Authentication Directory resolves to the IP address of the directory server at the source facility.

The Opsware System does support installing an Access & Authentication Directory in each facility. In this configuration, you must set up supplier and consumer Access & Authentication Directories by following the procedures documented in the Netscape Directory Server documentation. See your Opsware Support Representative for assistance on how to install and set up the Access & Authentication Directories to support this configuration.

Overview of the Process for Multimaster Installation

This topic just documents the high-level tasks that you perform for a multimaster installation (installing a second core or third core). This topic does *not* provide the actual steps to complete these tasks.

For the complete steps to complete these tasks:

- See “Steps for Creating a Multimaster Mesh and Installing a Second Core” on page 113 in Chapter 8 for more information.
- See “Steps for Adding a Third Core or More to a Multimaster Mesh” on page 122 in Chapter 8 for more information.

The multimaster installation process consists of the following high-level tasks:

1. Installing a standalone core by following the process for a standalone installation

See "Overview of the Standalone Installation Process" on page 75 in Chapter 5 for more information.

2. Running the first Opsware Installer script a second time to update these Opsware System components in the standalone core to support multimaster operation:
   - The Model Repository (truth)
   - The Data Access Engine (spin)

     If an Opsware core has multiple Data Access Engines installed, you must upgrade all of them.
   - Opsware Command Center (occ)
   - Software Repository (word)
   - Command Engine (way)
3. Installing the Opsware core in multimaster mode in the subsequent facilities
4. Performing database synchronization tasks by importing the exported data from the Model Repository at the first facility

   In a multimaster installation, the first Model Repository that you set up is referred to as the *source* (the script interface uses the term *master*). Subsequent Model Repository databases are referred to as *targets* (the script interface uses the term *slave*).

   The target databases are only target databases in the sense that, for the duration of the installation process, they copy data from the source Model Repository. After the Model Repository databases are up and running, each Model Repository instance functions as a master (that is, it can be accessed for both read and write operations).
5. Configuring the TIBCO Rendezvous routing daemon (rvrd), which provides secure communications between cores in multiple facilities

   See "TIBCO rvrd Configuration" on page 138 in Chapter 9 for more information.

If you are installing an Opsware component on a server where an Opsware component was previously installed, you must deactivate the server in the Opsware Command Center first. Otherwise, if you try to install Opsware core components on the server, the installation will fail. See the *Opsware System 4.5 User's Guide* for information about the steps to deactivate a managed server.

Overview of Installing a Second Core in a Multimaster Mesh

Before you begin the multimaster installation, you *must* already have one Opsware System core installation completed. Multimaster installation involves upgrading an existing core and then setting up additional Opsware System cores at the facilities that will make up your multimaster mesh.

You complete the multimaster upgrade of the first facility before you create other Opsware System cores at other facilities.

Before you upgrade the standalone core to multimaster and install the second, target facility, you must have met the following requirements:

- Satisfied the installation prerequisites for the second core, which consists of installing and configuring an Oracle database and setting up your network and domain name system to resolve Opsware host names.
- The `tnsnames.ora` file installed on the source core (the first facility you installed) must have a TNS entry added for the target core's Model Repository. Otherwise, the Multimaster Tools in the Opsware Command Center display the message "unable to connect" even after you correctly configure TIBCO for the target core.

  The `tnsnames.ora` file with the *same* directory path must exist on the servers where the Model Repository, Data Access Engine, and Opsware Command Center will be installed in the second Opsware core.

  See "Installation Requirements" on page 17 in Chapter 3 for more information. This section provides the exact prerequisites that must be met before you install a standalone Opsware core.

If you installed the Opsware System core at any secondary facilities and you want to include these facilities in your multimaster mesh, you must perform these actions:

1. Un-install the Opsware System core at the secondary facilities.

   See "Overview of Un-installing the Opsware System" on page 151 in Chapter 11 for more information.

2. Upgrade the components at the first facility to multimaster.
3. Install an Opsware System core at any secondary facility that you want to include in the multimaster mesh.

Steps for Creating a Multimaster Mesh and Installing a Second Core

This procedure describes how to upgrade the source core to multimaster mode, and then how to install a second (target) core so that you have a two core multimaster mesh.

If you already have a multimaster mesh and want to add an additional core, see See "Steps for Adding a Third Core or More to a Multimaster Mesh" on page 122 in this chapter for more information. Perform the following steps to create a multimaster mesh by installing a second core:

1. Mount the Opsware System software on all core servers by mounting the CD or an NFS-mounting directory that contains the CD contents.

   The Opsware Installer must have read/write root access to the directories where it installs Opsware components, even NFS-mounted network appliances.

   See "Installation Media for the Opsware Installer" on page 13 in Chapter 2 for more information. This topic provides information about the recommended way to run the Opsware Installer software.

2. Make sure that all users have logged out of the Opsware Command Center and that no jobs are in progress. To accomplish this task, log in to the Opsware Command Center as the Opsware administrator (the admin user) and click Sessions under Administration in the navigation panel.

3. On the Model Repository server in the standalone core, invoke the Opsware Installer with response file and the `--interview` option.

   ```
   /opsware_system/disk001/opsware_installer/install_opsware.sh
   -r <full_path_to_response_file> --interview
   ```

   You must specify the full path to the script. The directory path that this step shows assumes that you copied the Opsware System CDs to a local disk or network share using the required directory structure.

   You should run the Opsware Installer with the response file that you created for the standalone core. If the standalone response file is not available, invoke the Opsware Installer *without* any command line options, and the interview will automatically start.

   You can run the Opsware Installer from any directory on the server except for any of the directories in the path to the Opsware Installer script (in the `/opsware_system/disk001` directory or subdirectories). If you are running the Opsware Installer from a CD, you cannot run the installation while under the CD mount point.

The Welcome Menu appears for the Opsware Installer, which prompts you to select the type of installation.

4. Select option 4, "Convert a standalone Opsware core to a multimaster core."

   The Opsware Installer interview phase begins. In this phase, you specify information about the environment in which the Opsware core will run.

5. Complete the interview.

   See "Description of Required Information for Installation" on page 42 in Chapter 3 for more information. This section provides detailed information about what information you should enter at each prompt.

   When you run the interview, the path for the Windows OS media must exist on the server running the OS Provisioning Media Server component.

   When you enter all required information for installation, the Opsware Installer displays this message:

   ```
   NOTE: All parameters have values. Hit control-F to finish the interview.
   ```

   If you do not enter `control-F` and press `Enter` to continue to the next prompt, the Opsware Installer has you validate the data you entered previously by displaying the prompt again and showing the value in brackets [ ] that you previously entered.

   After providing all information in the interview, enter `control-F` to finish the interview.

6. On the server where the Data Access Engine is installed, stop the Data Access Engine by entering the following command:

   ```
   /etc/init.d/spin stop
   ```

   On the server where the Opsware Command Center is installed, stop the Web Services Data Access Engine by entering the following command:

   ```
   /etc/init.d/twist stop
   ```

7. When the component selection menu displays, select and install the "Model Repository (truth), Multimaster Additions" option.

8. Run the Opsware Installer on the Model Repository server again with the new response file.


```
/opsware_system/disk001/opsware_installer/install_opsware.sh
-r <full_path_to_new_response_file>
```

9 On each server where a standalone version of the Data Access Engine component is installed, select and install the "Data Access Engine (spin), Multimaster Component" option.

10 On the server where the Model Repository is installed, select and install the "Multimaster Infrastructure Components (vault)" option.

11 If you are upgrading the components on multiple servers, copy the response file to the other servers in this core.

12 In the standalone core (hereafter referred to as the source core), upgrade the remaining Opsware components. On each server where a standalone version of a component was installed, run the Opsware Installer with the response file and upgrade one component at a time (even if multiple components are installed on a server). You cannot upgrade components concurrently.

```
/opsware_system/disk001/opsware_installer/install_opsware.sh
-r <full_path_to_response_file>
```

The Opsware Installer menu does *not* present the list of components in the order in which you must install them. You *must* install the remaining components one at a time in the following order:

1. Command Engine (way), Multimaster Component
2. Software Repository (word), Multimaster Component
3. Opsware Command Center (occ), Multimaster Component

13 On the server where the Data Access Engine is installed, start the Data Access Engine by entering the following command:

```
/etc/init.d/vaultdeamon start
```

On the server where the Opsware Command Center is installed, start the Web Services Data Access Engine by entering the following command:

```
/etc/init.d/twist start
```

14 In the source core, log into the Opsware Command Center as the admin user by opening a browser and entering the IP address of the server running this component. The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

15 Use the Opsware Command Center to perform the following steps:

1. Create a facility for the target core by using the Opsware Command Center. Record the facility ID that gets generated because you will need the ID later during the installation. You must log in to the Opsware Command Center again to see the new facility.

   See "Adding the Target Facility in the Opsware Command Center" on page 128 in this chapter for more information.

2. Associate the appropriate customers with this facility so that servers managed at that facility are associated with the correct customer accounts.

   See "Associating Customers with a New Facility" on page 130 in this chapter for more information.

3. Using the System Configuration channel, set the configuration parameters `opsware.core.domain` and `truth.tnsname` for the target facility.

   See "Setting Configuration Parameters for a Target Facility" on page 131 in this chapter for more information.

4. Using the System Configuration channel, update the listeners configuration parameter by adding `vaultIn-<tnsname>` to the existing list. The TNSNAME should be the value that you just set for the target facility. Update the listener's configuration parameter by selecting "Model Repository, Multimaster Component" in the System Configuration page.

   See "Configuring the Multimaster Infrastructure for a Target Core" on page 132 in this chapter for more information.

16 Stop all Data Access Engines and the Multimaster Replication Engine in the source core.

Log in as root to the server where the Data Access Engine is running and enter the following command:

```
/etc/init.d/spin stop
```

If the Opsware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin stop` command on the Opsware Command Center servers.

Log in as root to the server where the Model Repository is running and enter the following command:

```
/etc/init.d/vaultdaemon stop
```


17 On the server running the Model Repository, wait for all transactions to be published. Examine the file `/var/lc/vault/log`.

If the log contains successive entries "QUERIED THE DATABASE" and does not contain recent "SENDING TRANSACTION" entries, the transactions from the installation have been published.

18 In the source core, run the Opsware Installer on the Model Repository server again by running the following command:

```
/opsware_system/disk001/opsware_installer/install_opsware.sh
-r <full_path_to_response_file>
```

19 Select and run the "Model Repository (truth), Export" option.

Depending on the amount of data, the export might take 20 minutes or more. To track progress of the export in a different window, run the command below. The log file name includes a generated number. Replace the following file name with the actual name of the log on this server.

```
tail -f /var/lc/install_opsware/truth/truth_exp_1234.log
```

20 In the source core, start all Data Access Engines and the Multimaster Replication Engine.

Log in as root to the server where the Data Access Engine is running and enter the following command:

```
/etc/init.d/spin start
```

If the Opsware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin start` command on the Opsware Command Center server.

Log in as root to the server where the Model Repository is running and enter the following command:

```
/etc/init.d/vaultdaemon start
```

After starting the Multimaster Replication Engine (vault), examine the logs for this component to verify that the Multimaster Replication Engine (vault) started properly. These logs are located in the following directory on the server running the Model Repository:

```
/var/lc/vault/
```

Where the files are `log`, `log.1`, `log.2`, `log.3`, etc.

21 Copy the Model Repository data export file, `truth_data.tar`, to the server where you will install the Model Repository in the target facility core.

By default, the file is located in the directory `/tmp`. The Opsware Installer interview prompted for a location to save this file; therefore, it might be located in another directory. Later during the installation, you will need to provide the directory where you copied this file to.

The Oracle user needs read access to the `truth_data.tar` file on the Model Repository host in the target core.

22 Copy the database of cryptographic material from the following directory on the server in the source core that is running the Data Access Engine:

```
/var/lc/crypto/cadb/realm/opsware-crypto.db.e
```

Copy the cryptographic material to every server in the target facility core. If necessary, first create the directory `/var/lc/crypto/cadb/realm` on each core server. The directory and database need to be readable by the root user.

23 On the Model Repository server in the target facility core, run the Opsware Installer without command line arguments. Do **not** copy the response file from the source core because many of the prompts need different values for the target facility core.

```
/opsware_system/disk001/opsware_installer/install_opsware.sh
```

24 Select option 3, “Multimaster Opsware Core - Subsequent Core.”

25 Complete the interview for the target facility core. The following values must match what was entered earlier.

- The data center ID must match the ID generated by the Opsware Command Center when the target facility was created in the source core.
- The facility name and short name must match the values you entered in the Opsware Command Center when the target facility was created in the source core.
- The authorization domain (the `truth.authDom` parameter) must match the value provided for the source core.
- The facility subdomain (`truth.dcSubDom` parameter) must match the value entered in the Opsware Command Center for `opsware.core.domain` for the target facility.
- The `truth.servicename` must match the value entered in the Opsware Command Center for `truth.tnsname` for the new facility.

- Passwords must match the values provided during the interview for the source core.
- The path to the data export file, `truth_data.tar`, in the target core must match the path you used when exporting the data in the source core.

After providing all information in the interview, enter `control-F` to finish the interview.

26 When the component selection menu displays, select and install the "Model Repository, Consumer Multimaster Component (truth slave)" option.

The installation process includes importing the data exported from the source core, which can take 30 minutes or more depending on the amount of data.

To track the progress of the import in a different window, run the following command. The log file name includes a generated number, so replace the file name shown with the actual name of the log on this server.

```
tail -f /var/lc/install_opsware/truth/truth_imp.log
```

27 If you are installing the target facility core on multiple servers, copy the response file to the other servers in this core.

28 Install the remaining Opsware components on the server designated for each component by running the Opsware Installer with the response file. You must install each component separately.

```
/opsware_system/disk001/opsware_installer/install_opsware.sh
-r <full_path_to_response_file>
```

You must install the OS Provisioning Build Scripts on the server that was specified during the interview at the prompt asking for the IP address or host name of the Build Manager.

The Opsware Installer menu does *not* present the list of components in the order in which they must be installed. You *must* install the remaining components one at a time in the following order:

1. Data Access Engine (spin), Multimaster Component
2. Multimaster Infrastructure Components (vault)

After you install the Multimaster Infrastructure Components (vault) on the server running the Model Repository, you must configure TIBCO communication between the cores. See "TIBCO rvrd Configuration" on page 138 in this chapter for more information.

3. Command Engine (way), Multimaster Component
4. Software Repository (word), Multimaster Component
5. OS Provisioning Build Scripts
6. OS Provisioning Boot Server
7. OS Provisioning Media Server
8. Opsware Documentation
9. Opsware Command Center (occ), Multimaster Component

If the following message appears while installing an Opsware component, you forgot to copy the database of cryptographic material to the server where you are installing the component:

```
Database with cryptographic material not found.
Would you like Opsware Installer to generate new database of
cryptographic material?
```

29 Reboot the server running the OS Provisioning Boot Server component and the server running the OS Provisioning Media Server component.

If the Boot Server and Media Server are installed on a host where other Opsware components are installed (for example, all components are installed on a single server), you must restart the processes for these components as well. When restarting multiple Opsware components, you must restart them in the correct order.

See the *Opsware System 4.7 Administration Guide* for information about the correct restart sequence for Opsware System components.

30 (Optional) Install additional instances of the Data Access Engine, OS Provisioning Media Server, and Opsware Command Center depending on how you need to scale the Opsware System for performance.

See "Overview of Additional Instances of Opsware Components" on page 71 in Chapter 4 for more information.

31 Reassign the Data Access Engine to the multimaster central role.

See “Designating the Multimaster Central Data Access Engine” on page 133 in this chapter for more information.

32 Configure system parameters for the new core so that email addresses and contact information is properly configured.

See “Opsware System Configuration Parameters” on page 85 in Chapter 6 for more information.

33 Configure the OS Provisioning Subsystem for the target facility.

See “Overview of Network Configuration for OS Provisioning” on page 97 in Chapter 7 for more information.

Overview of Expanding an Opsware Multimaster Mesh

You must use the first core in the mesh as the source core for all new cores. The first core was the core that was initially installed as a standalone core, and then converted to multimaster.

Before you install a third or subsequent core in a multimaster mesh, you must have performed the installation prerequisites for the subsequent core, which consists of installing and configuring an Oracle database and setting up your network and domain name system to resolve Opsware host names.

See “Before You Install the Opsware System” on page 15 in Chapter 3 for more information. This section provides the exact prerequisites that must be met before you install a subsequent Opsware core.

You should have also determined which component distribution is required for the subsequent core based on the size of the managed environment at that facility.

See “Opsware Core Scalability for Performance” on page 65 in Chapter 4 for more information.

Before you install a third or subsequent core, the `tnsnames.ora` file installed on the source core (the first facility you installed) must have a TNS entry added for the target core’s Model Repository. Otherwise, the Multimaster Tools in the Opsware Command Center will display the message “unable to connect” even after you have correctly configured TIBCO for the target core.
Additionally, the `tnsnames.ora` file with the *same* directory path must exist on the

servers where the Model Repository, Data Access Engine, and Opsware Command Center will be installed in the subsequent Opsware core.

Steps for Adding a Third Core or More to a Multimaster Mesh

Perform the following steps to add a third core or more to an Opsware Multimaster Mesh:

1. Mount the Opsware System software on all core servers by mounting the CD or NFS-mounting a directory containing the CD contents.

   The Opsware Installer must have read/write root access to the directories where it installs Opsware components, even NFS-mounted network appliances.

   See "Installation Media for the Opsware Installer" on page 13 in Chapter 2 for more information. This topic provides information about the recommended way to run the Opsware Installer software.

2. Log in to the Opsware Command Center in the source facility as the admin user by opening a browser and entering the IP address of the server running this component. Enter the password you supplied during installation.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

3. Use the Opsware Command Center to perform the following tasks:

   1. Create a facility for the target core by using the Opsware Command Center. Record the facility ID that gets generated because you will need the ID later during the installation. You must log in to the Opsware Command Center again to see the new facility.

      See "Adding the Target Facility in the Opsware Command Center" on page 128 in this chapter for more information.

   2. Using the System Configuration channel, set the configuration parameters `opsware.core.domain` and `truth.tnsname` for the target facility.

      See "Setting Configuration Parameters for a Target Facility" on page 131 in this chapter for more information.

   3. Using the System Configuration channel, update the `vault.listener` configuration parameter by adding `vaultIn-<tnsname>` to the existing list. The TNSNAME should be the value you just set for the target facility.

See “Configuring the Multimaster Infrastructure for a Target Core” on page 132 in this chapter for more information.

4. Verify that all transactions have propagated to the other facilities by checking the Multimaster Tools page.

   See “Verifying Multimaster Transaction Traffic” on page 134 in this chapter for more information.

4 On the Model Repository server in every existing facility except the source facility, restart the Multimaster Replication Engine to pick up the new configuration.

Log in as root to the server where the Model Repository is running and enter the following commands:

```
/etc/init.d/vaultdaemon stop
```

```
/etc/init.d/vaultdaemon start
```

5 Stop the Data Access Engine in the source core.

Log in as root to the server where the Data Access Engine is running and enter the following command:

```
/etc/init.d/spin stop
```

If the Opsware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin stop` command on the Opsware Command Center server.

6 Log in to the Opsware Command Center in one of the existing facilities (*not* the source facility) and verify that all transactions have propagated from the source facility by checking the Multimaster Tools page.

See “Verifying Multimaster Transaction Traffic” on page 134 in this chapter for more information.

Traffic between facilities other than the source facility can continue without affecting the addition of the target facility.

7 Stop the Multimaster Replication Engine in the source core.

Log in as root to the server where the Multimaster Replication Engine is running and enter the following command:

```
/etc/init.d/vaultdaemon stop
```

8 Run the Opsware Installer on the Model Repository server in the source core by entering the following command. You must specify the full path to the script.

```
/opsware_system/disk001/opsware_installer/install_opsware.sh
-r <full_path_to_response_file>
```

The directory path that this step shows assumes that you copied the Opsware System CDs to local disk or network share using the required directory structure.

See "Installation Media for the Opsware Installer" on page 13 in Chapter 2 for more information.

You can run the Opsware Installer from any directory on the server except for any of the directories in the path to the Opsware Installer script (in the `/opsware_system/disk001` directory or subdirectories). If you are running the Opsware Installer from a CD, you cannot run the installation while under the CD mount point.

The Welcome Menu appears for the Opsware Installer, which prompts you to select the type of installation.

9 Select and run the "Model Repository (truth), Export" option.

Depending on the amount of data, the export might take 20 minutes or more. To track progress of the export in a different window, run the command below. The log file name includes a generated number, so replace the following file name with the actual name of the log on this server.

```
tail -f /var/lc/install_opsware/truth/truth_exp_1234.log
```

10 Start all Data Access Engines and the Multimaster Replication Engine in the source core.

Log in as root to the server where the Data Access Engine is running and enter the following command:

```
/etc/init.d/spin start
```

If the Opsware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin start` command on the Opsware Command Center server.

Log in as root to the server where the Model Repository is running and enter the following command:

```
/etc/init.d/vaultdaemon start
```


11 Copy the Model Repository data export file, `truth_data.tar`, to the Model Repository server in the target core.

By default, the file is located in the directory `/tmp`. The Opsware Installer interview prompted for a location to save this file; therefore, it might be located in another directory. Later during the installation, you will need to provide the directory where you copied this file to.

The Oracle user needs read access to the `truth_data.tar` file on the Model Repository host in the target core.

12 Copy the database of cryptographic material to every core server. The database of cryptographic material is located in the following directory on the server that is running the Data Access Engine:

```
/var/lc/crypto/cadb/realm/opsware-crypto.db.e
```

If necessary, first create the directory `/var/lc/crypto/cadb/realm` on each core server. The directory and database need to be readable by the root user.

13 On the Model Repository server in the target core, run the Opsware Installer without command line arguments. Do *not* copy the response file from the source core because many of the prompts need different values for the target core.

```
/opsware_system/disk001/opsware_installer/install_opsware.sh
```

You must install the Model Repository on the server where Oracle was installed.

See "Installation and Configuration Requirements for Oracle" on page 35 in Chapter 3 for more information.

14 Select option 4, "Multimaster Opsware Core - Subsequent Core."

15 Complete the interview. The following values must match what was entered earlier:

- The facility ID must match the ID that the Opsware Command Center generated when the target facility was created in the source core.
- The facility name and short name must match the values that you entered in the Opsware Command Center when the target facility was created in the source core.
- The authorization domain (the `truth.authDom` parameter) must match the value provided for the source core.
- The facility subdomain (the `truth.dcSubDom` parameter) must match the value entered in the Opsware Command Center for `opsware.core.domain` for the target facility.

- The `truth.servicename` must match the value entered in the Opsware Command Center for `truth.tnsname` for the new facility.
- Passwords must match the values provided during the interview for the source core.
- The path to the data export file, `truth_data.tar`, in the target core must match the path that you used when exporting the data in the source core.

After providing all information in the interview, enter `control-F` to finish the interview.

16 When the component selection menu displays, select and install the "Model Repository, Consumer Multimaster Component (truth slave)" option.

The installation process includes importing the data exported from the source core, which might take 30 minutes or more depending on the amount of data. To track progress of the import in a different window, run the command below.

```
tail -f /var/lc/install_opsware/truth/truth_imp.log
```

17 If you are installing the target core on multiple servers, copy the response file to the other servers in the core.

18 Install the remaining Opsware components on the server designated for each component by running the Opsware Installer with the response file. Each component must be installed separately.

```
/opsware_system/disk001/opsware_installer/install_opsware.sh
-r <full_path_to_response_file>
```

You must install the OS Provisioning Build Scripts on the server that was specified during the interview at the prompt asking for the IP address or host name of the Build Manager.

The Opsware Installer menu does *not* present the list of components in the order in which they must be installed. You *must* install the remaining components one at a time in the following order:

1. Data Access Engine (spin), Multimaster Component
2. Multimaster Infrastructure Components (vault)

After you install the Multimaster Infrastructure Components (vault) on the server running the Model Repository, you must configure TIBCO communication between the cores. See "TIBCO rvrd Configuration" on page 138 in Chapter 9 for more information.

3. Command Engine (way), Multimaster Component
4. Software Repository (word), Multimaster Component
5. OS Provisioning Build Scripts
6. OS Provisioning Boot Server
7. OS Provisioning Media Server
8. Opsware Documentation
9. Opsware Command Center (occ), Multimaster Component

If the following message appears while installing an Opsware component, you forgot to copy the database of cryptographic material to the server where you are installing the component:

```
Database with cryptographic material not found.
Would you like Opsware Installer to generate new database of
cryptographic material?
```

19 Reboot the server running the OS Provisioning Boot Server component and the server running the OS Provisioning Media Server component.

If the Boot Server and Media Server are installed on a host where other Opsware components are installed (for example, all components are installed on a single server), you must restart the processes for these components as well. When restarting multiple Opsware components, you must restart them in the correct order.

See the *Opsware System 4.7 Administration Guide* for information about the correct restart sequence for Opsware System components.

20 (Optional) Install additional instances of the Data Access Engine, OS Provisioning Media Server and Opsware Command Center depending on how you need to scale the Opsware System for performance.

See "Overview of Additional Instances of Opsware Components" on page 71 in Chapter 4 for more information.

21 Configure system parameters for the new core so that email addresses and contact information is properly configured.

See “Opsware System Configuration Parameters” on page 85 in Chapter 6 for more information.

22 Configure the OS Provisioning Subsystem for the subsequent facility.

See “Overview of Network Configuration for OS Provisioning” on page 97 in Chapter 7 for more information.

Overview of Target Facility Setup in Opsware Command Center

You perform the following procedure as part of the procedures to install a second or third core in a multimaster mesh.

Before you install a target core, you must complete certain tasks to configure the multimaster mesh to include the target core.

You use the Opsware Command Center running in the source core to create a facility for the target core, set the configuration parameters `opsware.core.domain` and `truth.tnsname` for the target facility, and update the listeners configuration parameter by adding `vaultIn-<tnsname>` for the target facility

See step 15 on page 116 in “Creating a Multimaster Mesh by Installing a Second Core” and step 3 on page 122 in “Adding a Third Core or More to an Opsware Multimaster Mesh” in this chapter for information.

Adding the Target Facility in the Opsware Command Center

You must add an entry for the target facility to the source facility. Use the Opsware Command Center installed at the source facility to complete this task.

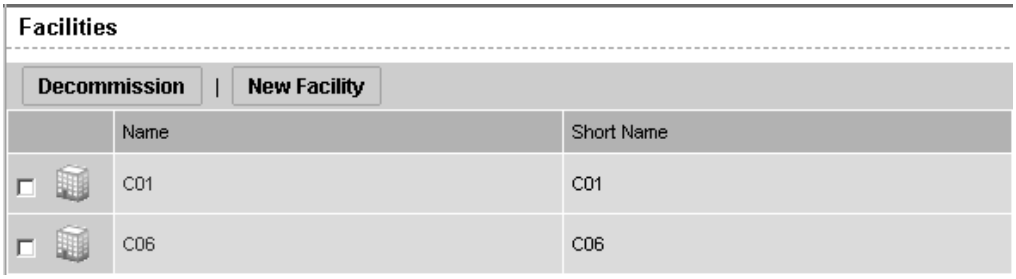
When you later run the Opsware Installer to install the core at the target facility, you *must* enter the *same* facility values that you supplied in the Opsware Command Center in this task. Perform the following steps to add the target facility in the Opsware Command Center:

1 Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2 From the navigation panel, click Facilities under Environment. The Facilities Page in the Opsware Command Center appears, as Figure 8-1 shows.

Figure 8-1: Facilities Page in the Opsware Command Center



3 Click the New Facility button to add a new facility. The Manage Facilities: New Facility page appears.

4 Complete the entries defining the target facility:

- Name (required)

  The name used internally by the Opsware System to uniquely identify the facility.

- Short Name (required)

  The name used in the display of the Node navigation path. The short name must be uppercase, less than 25 characters, and *cannot* contain spaces or special characters (although dashes and underscores are allowed).

5 Click Save to apply the changes.

6 Sign out from the Opsware Command Center and log in again to see the new facility added to the list. Record the facility ID that the Opsware Command Center generated. You need this ID when completing the interview while installing the target core.

When you add new facilities to your multimaster mesh, your Opsware users will not have the required (read/write) permissions to access this new facility. You must grant your users permissions for the new facility. Additionally, you should update the User Groups "Basic," Intermediate," and "Advanced" so that they also include the read/write permission for the new facility. See the *Opsware System 4.7 Administration Guide* for information about granting users Opsware privileges.

Associating Customers with a New Facility

You should associate the appropriate customers with each new facility so that servers managed at that facility are associated with the correct customers accounts. Perform the following steps to associate customers with a new facility:

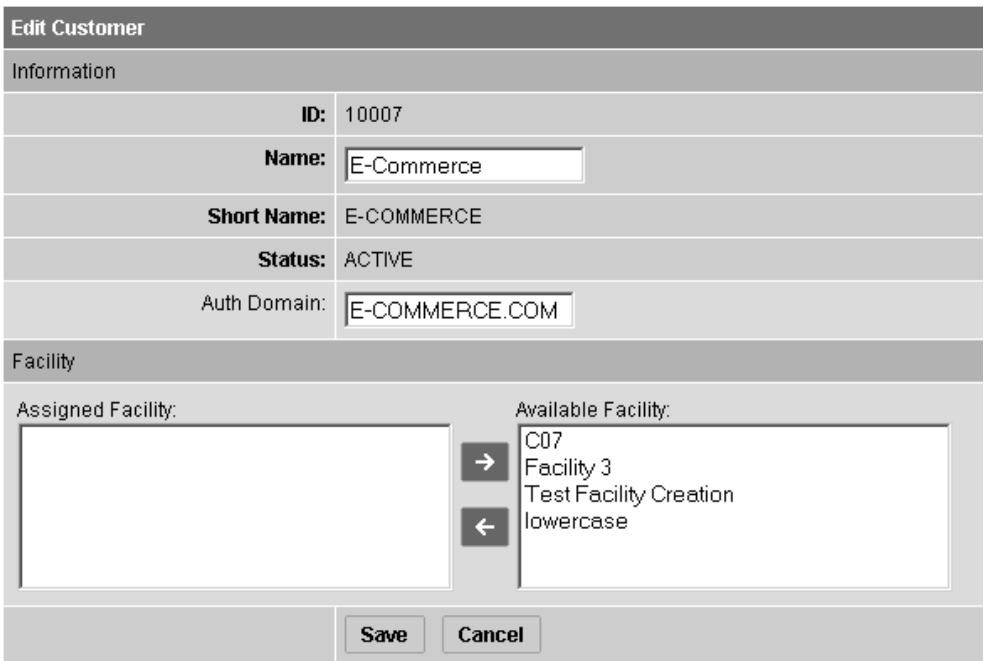
1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center component.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click Customers under Environment.

3. Click the link for the customer name that you want to associate with the facility. The Edit Customer Properties page appears, as Figure 8-2 shows.

Figure 8-2: Edit Customer Properties Page



4. In the Available Facility list, select the facility you want to associate with the customer and click the left arrow. The facility moves to the Assigned Facilities list.

5. Click the Save button.

6 Repeat Steps 3 through 5 to associate additional customers with the new facility.

Setting Configuration Parameters for a Target Facility

Using the Opsware Command Center installed at the source core, you must set values for the following configuration parameters for the target facility:

- `truth.tnsname` (set to the TNSNAME set by your database administrator for your Model Repository database)
- `opsware.core.domain` (set to the DNS subdomain for your facility)

Even if you have installed an Opsware Command Center at a subsequent facility, you must use the Opsware Command Center at the source facility to make these changes. Perform the following steps to set configuration parameters for a target facility:

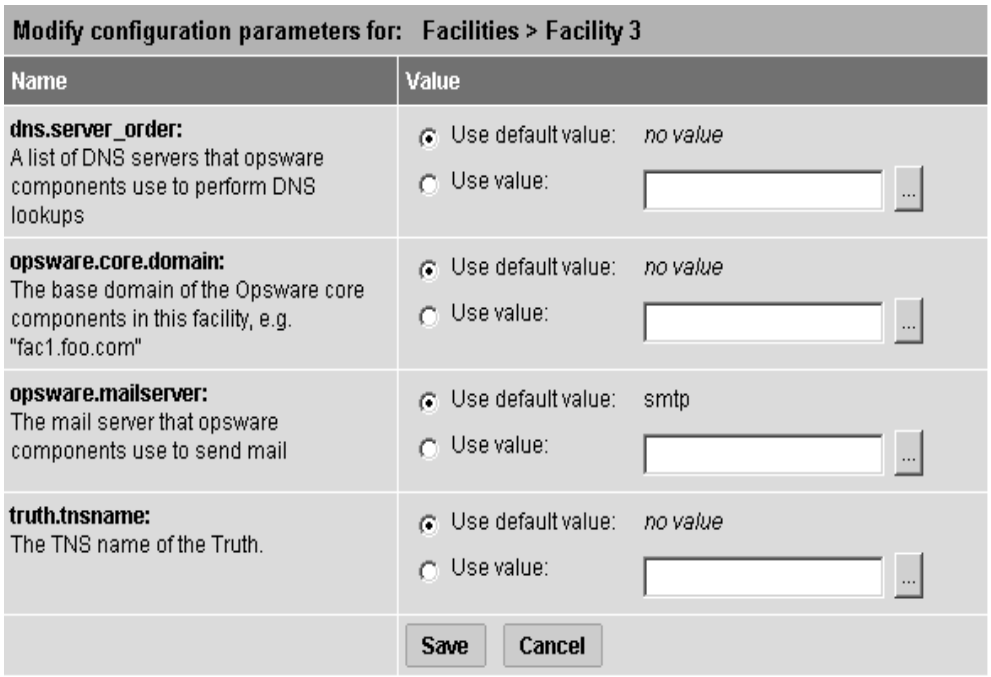
1 Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center component.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2 From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3 Under Select a Product, click the name of the facility (the target facility that you will install, not the source facility). The configuration page for the facility appears, as Figure 8-3 shows.

Figure 8-3: Configuration Page for a Facility



4 Enter the correct values for the `truth.tnsname` and `opsware.core.domain` parameters.

5 Click Save to apply the changes.

Configuring the Multimaster Infrastructure for a Target Core

After you have added the facility, you must append a value to the listeners parameter of the Multimaster Infrastructure Component. This value is taken from the target facility (the next facility you will be adding to your multimaster mesh.) Perform the following steps to configure the multimaster infrastructure for a target core:

1 Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center component.

The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.
3. Under Select Product, click Model Repository, Multimaster Component.
4. Append the following value for the listeners parameter:
   `vaultIn-<targettns>`
   Where *<targettns>* is the TNSNAME for the Model Repository instance in the target core. (This is a comma-separated list.)
5. Click Save to apply the changes.

Designating the Multimaster Central Data Access Engine

An Opsware multimaster mesh of cores has *only one* multimaster central Data Access Engine. Therefore, you only need to perform this procedure once (usually when you are adding a second core to a multimaster mesh); unless, you are changing which Data Access Engine is designated the multimaster central. For example, you might designate a different multimaster central Data Access Engine based on bandwidth requirements in a facility.

Use the new core OCC to move the Data Access Engine server for the new core from the Services ➤ Opsware ➤ Spin role to the Services ➤ Opsware ➤ Spin ➤ MultimasterCentral role.

If multiple Data Access Engine servers are in the new core, only one server should be selected as MultimasterCentral. Perform the following steps to designate the multimaster central data access engine:

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.
   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.
2. From the navigation panel, click Opsware Software under Administration. The Opsware Software page appears.
3. Click the spin link.
4. Click the Servers tab.
5. Select the check box for the Data Access Engine server for the new core.

6 From the Server menu, choose Re-Assign Node.

7 Select the radio button for the ServiceLevels | Opsware | spin | node.

8 Click the Select button.

9 Navigate the node hierarchy by clicking each node:

1. Opsware
2. Spin
3. Multimaster Central

10 Click the Re-Assign button.

11 Restart the MultimasterCentral Data Access Engine.

```
/etc/init.d/spin restart
```

Overview of Multimaster Transaction Traffic

You can examine the state of the multimaster mesh to discern problems. You can diagnose the state of the multimaster architecture by viewing the Multimaster State page. This page is available in all the Opsware Command Centers. The Multimaster State page servers these functions:

- Presents an overview of the health of the multimaster mesh by automatically checking all facilities.
- Shows the state of the last five transactions from each facility to each other facility, plus all conflicting transactions and all unpublished transactions. Each state is represented by a different color to allow users to determine the overall status of the system.

  A transaction is a unit of change to a Truth database that consists of one or more updates to rows and has a globally unique transaction ID.
- Shows the time the data was generated and cached by the Opsware Command Center. Click the Refresh button to refresh the cached data.
- Links each conflicting transaction ID to the Transaction Differences page for that transaction.

Verifying Multimaster Transaction Traffic

You use the Opsware Command Center to verify the transaction traffic with the target facility. Perform the following steps to verify multimaster transaction traffic:

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

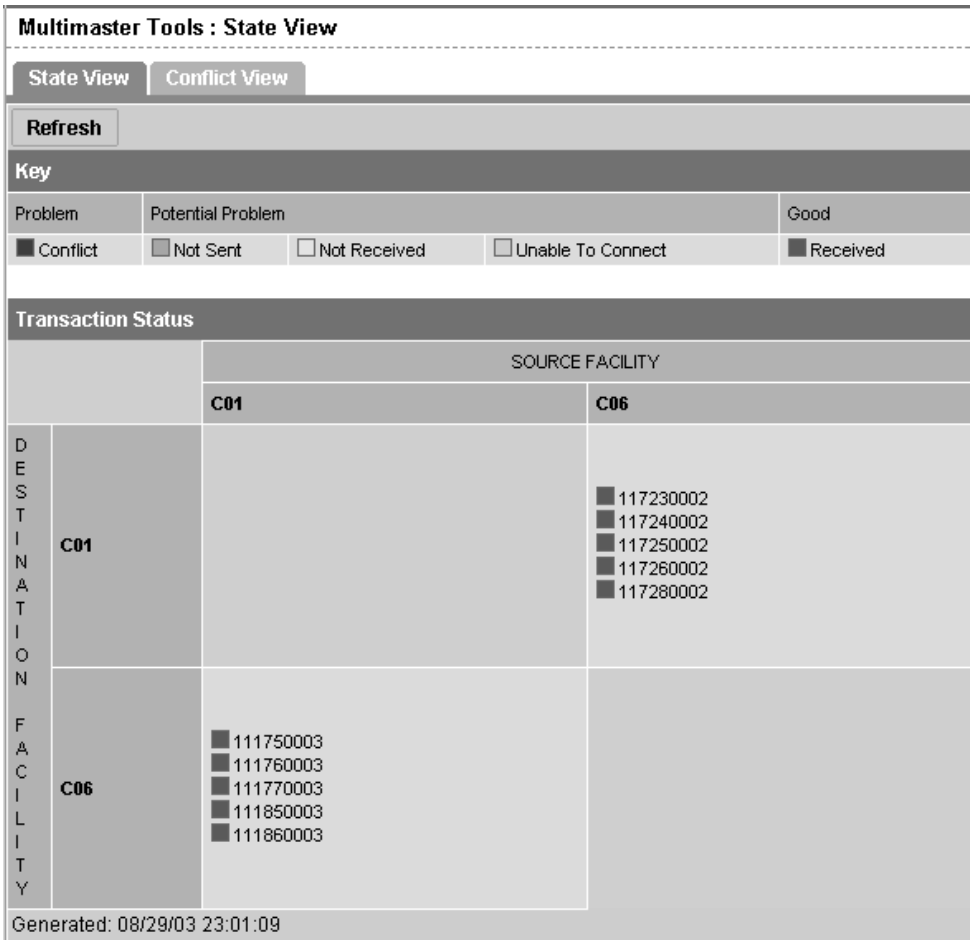
   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click Multimaster Tools under Administration. A status window with a list of transactions appears, as Figure 8-4 shows.

The color of the status box beside the transactions indicates the status of the transactions. Look for green status transactions at all facilities in the multimaster mesh. It is normal for some of the transactions to have an orange status (not sent).

If the transactions with the target facility are green, the new Opsware core is integrated into the multimaster mesh.

Figure 8-4: Multimaster Tools View of the Mesh State



Chapter 9: TIBCO Configuration for Multimaster

IN THIS CHAPTER

This chapter describes how to configure the TIBCO routing daemon as part of performing a multimaster installation by performing the following tasks in the TIBCO Web interface:

- Defining routers and local networks
- Adding neighbors and setting up encrypted communication

When running in multimaster mode, the Opsware System uses the TIBCO Certified Messaging system to transport transaction data (messages) between Model Repositories at different facilities. The Opsware System uses the TIBCO messages to keep the Model Repositories synchronized.

Additionally, the multimaster Software Repository uses the TIBCO message bus to request distributed files (though the Opsware System actually sends the files over HTTPS).

Requirements for TIBCO Configuration

Configuring the TIBCO Rendezvous routing daemon (rvrd) provides secure communications between cores in multiple facilities.

Before you configure TIBCO, you must have installed a source and target core by completing either of the following tasks:

- See “Steps for Creating a Multimaster Mesh and Installing a Second Core” on page 113 in Chapter 8 for more information.
- See “Steps for Adding a Third Core or More to a Multimaster Mesh” on page 122 in Chapter 8 for more information.

TIBCO rvrd Configuration

The Opsware Installer installs TIBCO as part of installing the multimaster infrastructure components.

You must configure the TIBCO rvrd at the target facility and source facility so that the Opsware System cores can communicate with each other.

TIBCO rvrd is configured though the TIBCO Web client. This guide contains basic information about setting up TIBCO to work with Opsware multimaster deployments.

See the following TIBCO Rendezvous documentation for detailed information about how to use the TIBCO Web client to configure TIBCO rvrd:

- *TIBCO Rendezvous Installation Guide*
- *TIBCO Rendezvous Concepts*

If you encounter an error while using the TIBCO Web client, close your browser and log in again to the TIBCO Web client by using Netscape Communicator 4.74. Errors might occur while accessing the TIBCO Web client with Netscape 7 or Internet Explorer.

Finding the Network Configuration Value

Before you configure TIBCO rvrd, you need to find out the value of the network configuration parameter in the Opsware Command Center. Perform the following steps to find the network configuration value:

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

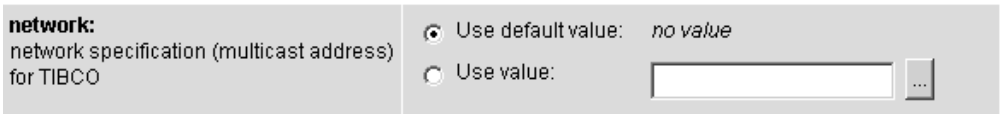
   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the Navigation Panel, click System Configuration under Administration. The Select a Product page appears.

3. Under Select a Product, click Model Repository, Multimaster Component. The Model Repository, Multimaster Component configuration page appears.

4 Copy the value from the network configuration parameter. It is possible for this parameter to have no value specified. See Figure 9-1.

Figure 9-1: Network Parameter for TIBCO in the Opsware Command Center



Configuring TIBCO rvrd for the Multimaster Mesh

You must now configure TIBCO rvrd for the target facility and source facility. You must do this at the TIBCO Web client at both facilities.

To configure TIBCO for the source facility, log in to the TIBCO Web client running on the Model Repository installed in the source core.

To configure TIBCO for the target facility, log in to the TIBCO Web client running on the Model Repository installed in the target core. Perform the following steps to configure TIBCO rvrd for the Multimaster Mesh:

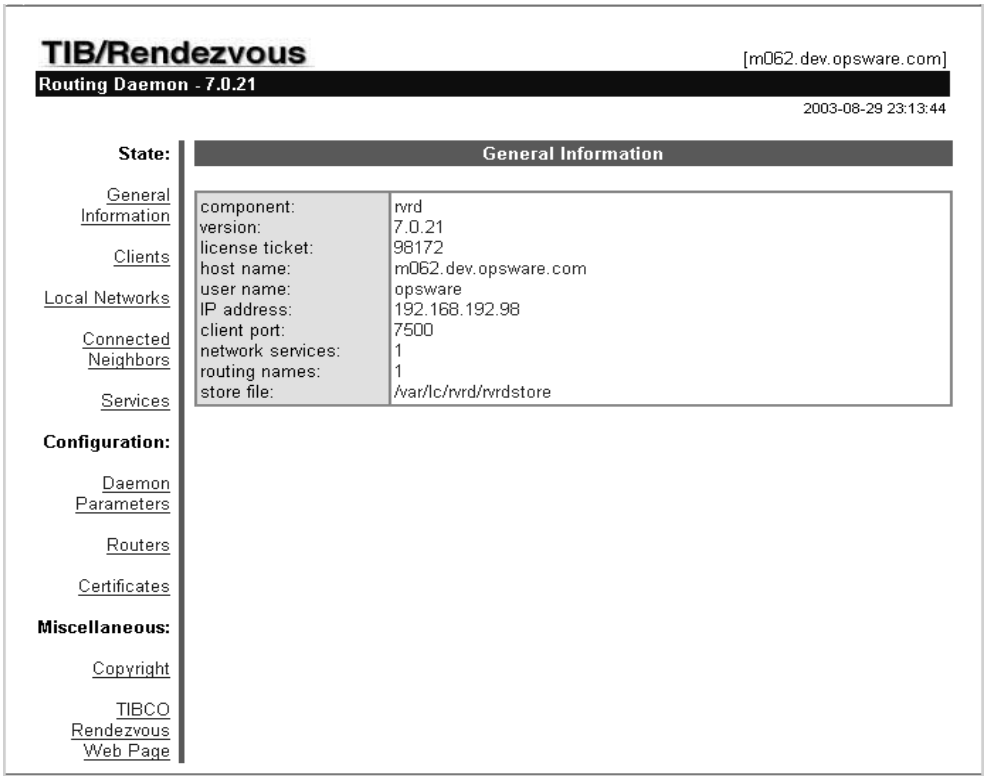
1 Access the TIBCO Web client by entering the following address in your Web browser:

`http://<Model_Repository_hostname>:7580`

Where <*Model_Repository_hostname*> is the fully-qualified host name or IP address of the server where the Model Repository is installed.

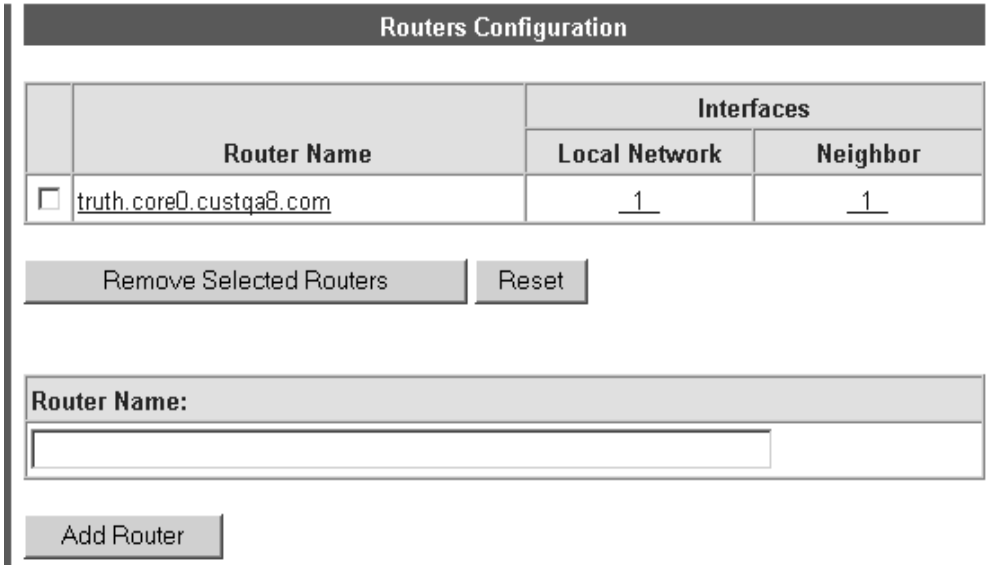
The TIB/Rendezvous General Information page appears, as Figure 9-2 shows.

Figure 9-2: TIB/Rendezvous General Information Page



2 From the left navigation panel, click Routers under Configuration. The TIBCO Routers Configuration page appears, as Figure 9-3 shows.

Figure 9-3: TIBCO Routers Configuration Page



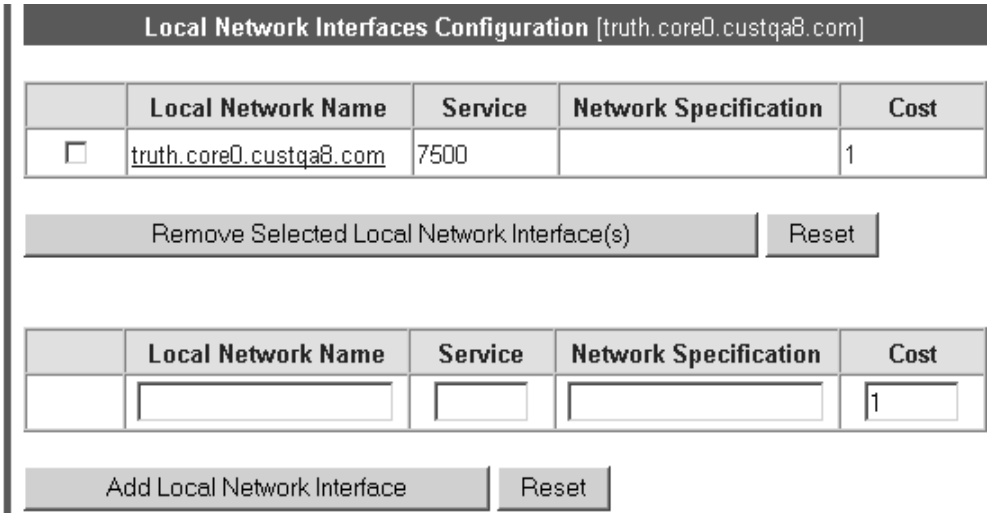
3 In the Router Name field, enter a name for the router (Opsware Inc. recommends that you use the Model Repository host name of the facility you are configuring).

4 Click the Add Router button. The router appears in the table on the page.

When you specify the fully-qualified host name of the server where the Model Repository is installed, you need to make sure that your browser can resolve the host name so that the link in the Router Name field functions correctly.

5 In the Local Network column under Interfaces, click the number link for the router you just added. The Local Network Interfaces Configuration page appears, as Figure 9-4 shows.

Figure 9-4: Local Network Interfaces Configuration Page



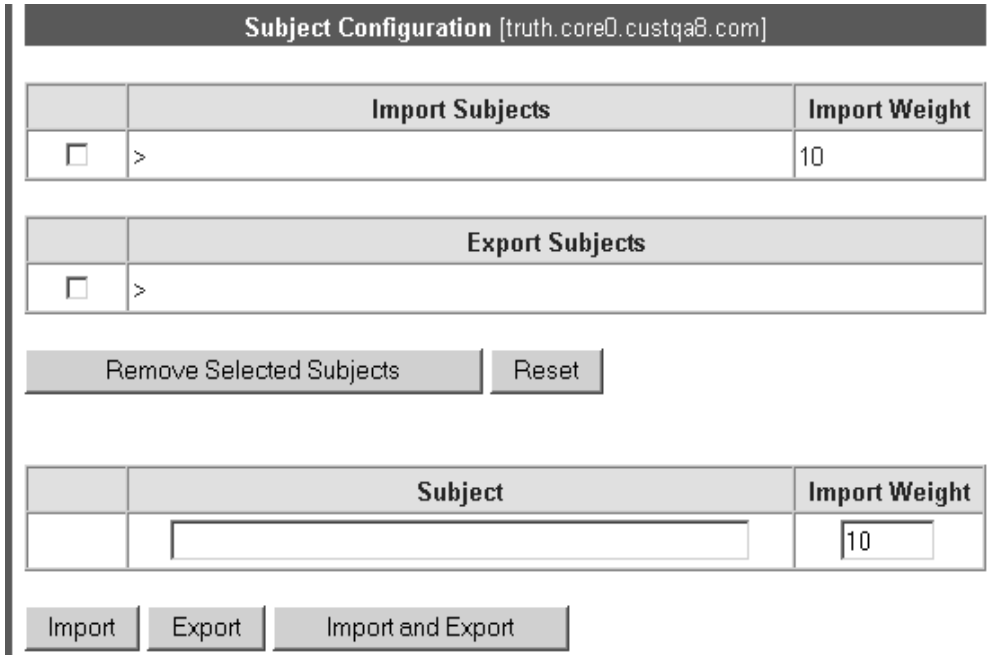
6 Define a new network by providing the following data in the fields:

1. In the Local Network Name field, enter the network name. In most cases, the network is given the same name as the Model Repository host name.
2. In the Service field, set the service to 7500.
3. In the Network Specification field, set the network specification to match the value of the Model Repository, Multimaster Component's network configuration parameter that you found in Opsware Command Center. (If it was blank, do not enter a value.)
4. Click the Add Local Network Interface button.

   The new local network appears in the table in the page.

7 Click the link for the new local network name. The Subject Configuration page appears, as Figure 9-5 shows.

Figure 9-5: Subject Configuration Page



8 In the Subject field, enter a greater than symbol (>) and click the Import and Export button. The greater than symbol appears in the Import Subjects and Export Subjects tables in the page.

9 Repeat the previous steps for the other facility (or facilities) in the multimaster mesh.

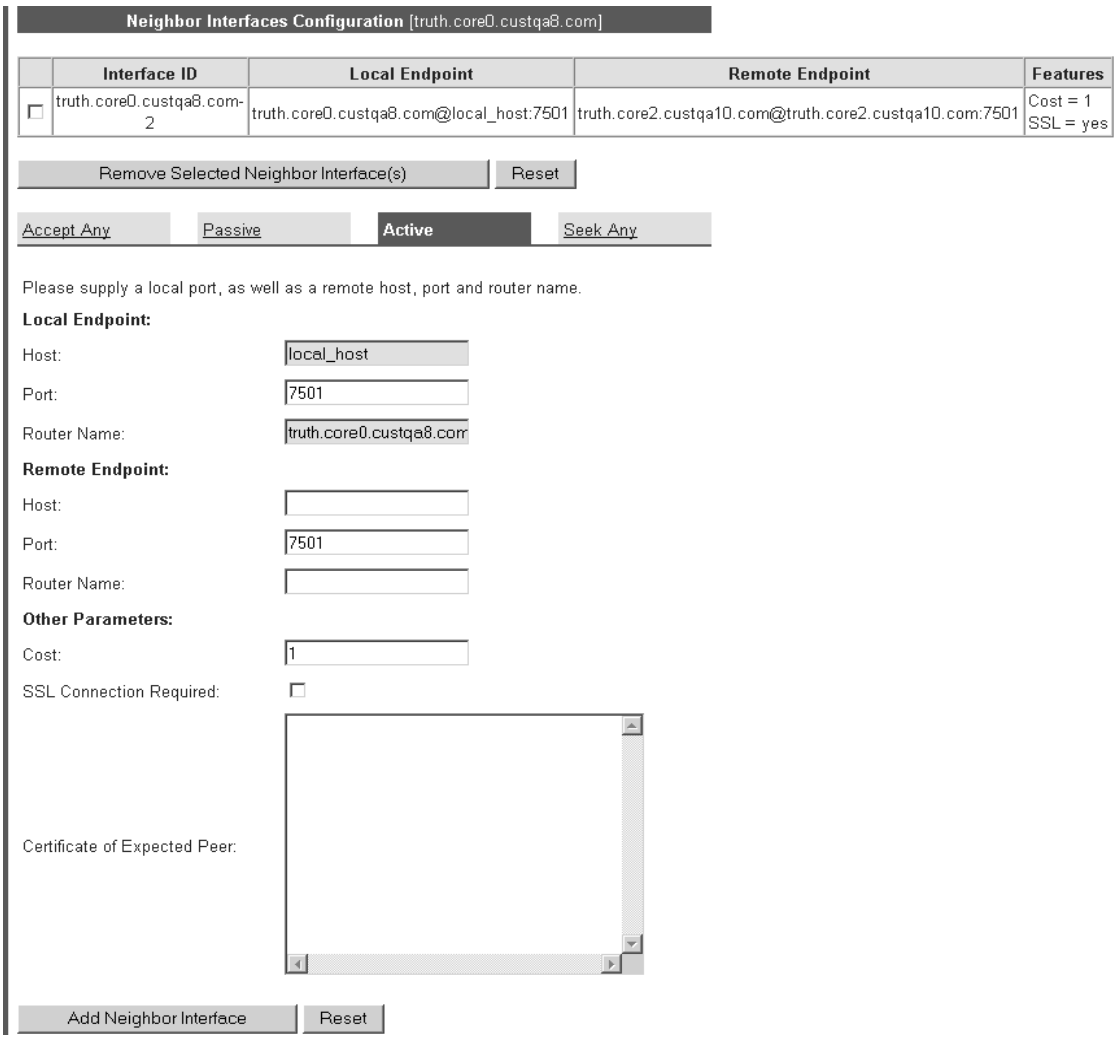
Adding Neighbors and Setting up Encrypted Communication

You must now add neighbors and set up encrypted communication in the TIBCO rvrd configuration page. You must do this at the TIBCO Web client at both facilities (for example, you must use the TIBCO Web client at the source facility to add the target facility as a neighbor, and you must use the TIBCO Web client at the target facility to add the source facility as a neighbor). Perform the following steps to add neighbors and set up encrypted communication:

1 From the left navigation, click Routers under Configuration. The Routers Configuration page appears.

2 In the Neighbor column of the table, click the number link for the router you added in the previous procedure. The Neighbor Interfaces Configuration page appears, as Figure 9-6 shows. You must define a neighbor for each facility in the mesh, except for the current facility (for example, do not include the current facility in the list).

Figure 9-6: Neighbor Interfaces Configuration Page



3 In the Host field under the Remote Endpoint section, enter the host name of the server running the neighbor's Model Repository database.

4 In the Port field under the Local Endpoint and Remote Endpoint sections, set both ports to 7501.

5 In the Router Name field under the Remote Endpoint section, enter the router name for the other facility. For example, if you used the host name of the Model Repository server when you created the router, you should use the same name here.

You must now copy the certificate(s) from the other facilities in the multimaster mesh to the facility you are configuring by adding a neighbor there. The certificates are created and available in the TIBCO Web client interface.

6 From a second browser window, log in to the TIBCO Web client at the other facility (or facilities) in the multimaster mesh.

7 From the left navigation panel, click Certificates. A Web page appears that contains certificate information for that facility.

8 Under the Certificate List section, select the data from the Add from Text field and copy it, as Figure 9-7 shows.

Figure 9-7: Add From Text Field in the Certificate List Section

9 Return to the open browser window for the facility in which you were configuring neighbors.

10 In the Certificate of Expected Peer text box on the Neighbor Interfaces Configuration page, paste the certificate.

11 Click the SSL Connection Required check box.

12 Click the Add Neighbor Interface button. The Local and Remote endpoints are added to the table in the page.

13 Repeat the previous steps for the other facility (or facilities) in the multimaster mesh.

To see if the setup has been successful for a facility, click Connected Neighbors in the left navigation. You should see links for the rvrd interface for the neighbor. Click the link. If the link is working, then the routing daemons are communicating with each other.

Chapter 10: Software Repository Replicator

IN THIS CHAPTER

After you install an Opsware core in multimaster mode, you can set up replication for the Software Repository in a facility.

This chapter provides the following information about working with the Software Repository Replicator to set up replication for the Software Repository:

- Configuring the Software Repository Replicator
- The prerequisites you must meet for using the Software Repository Replicator
- A sample configuration for the Software Repository Replicator

Overview of the Software Repository Replicator

The Software Repository Replicator provides backup functionality for Software Repositories running in a multimaster mesh. In most deployments, the Software Repositories do not all have the same content. If one of the Software Repositories becomes unavailable, this might result in some packages not being available until the Software Repository is back online.

Using the Software Repository Replicator allows you to have redundant copies of Software Repositories and thereby helps to ensure that all packages remain available even when a Software Repository goes offline.

Prerequisites for Using the Software Repository Replicator

Before you set up the Software Repository Replicator, you must meet the following prerequisites:

- SSH must be installed on the source and target Software Repositories.
- Port 22 must be open on the firewalls.
- Passwordless SSH as root must be enabled between the source and target repositories.

Software Repository Replicator Configuration

By default, the Opsware Installer installs the software you need to set up Software Repository replication when you install the multimaster Software Repository.

From the source core, use the `replicator.conf` file found in the `/cust/word/etc/` directory to configure the Software Repository Replicator.

To set up Software Repository replication, you do *not* need to modify the `replicator.conf` files in the target cores. However, you must specify to replicate the directory `/cust/word/etc/` to all the target cores. You specify which target cores to replicate to by entering them in the host chain section of the `replicator.conf` file. When you specify replication to these target cores, the `replicator.conf` file will propagate to the Software Repositories in the target cores.
See the bullet about defining host chains on page 149. See “Sample Software Repository Replicator Configuration” on page 150 in this chapter for information about an example of how to specify target cores in a host chain.

In this file, you must specify the following settings:

- The values for `User`, `Timestampdir`, and `SSH_PATH`.

  The Software Repository Replicator keeps timestamps of when it runs.

- For each directory that you want to replicate, specify the Directory or WordDirectory tag.

  Before you set up replication for the Software Repository, you need to determine which directories to replicate. This installation guide does not document the entire file system directory hierarchy for the host running the Software Repository.

  To determine which directories you should consider replicating (and the configuration to accomplish this), contact your Opsware Support Representative for assistance making this determination.

  The Software Repository Replicator parses the Directory tags, and these are ignored by the Software Repository. Therefore, you can use the Directory tag to replicate files that are not served by the Software Repository. WordDirectory tags are parsed by both the Package Replicator and the Software Repository.

  You should specify these tags for each directory you want to replicate because the Software Repository Replicator is not the only process that parses the

`replicator.conf` file. Some of the other processes that parse the `replicator.conf` file only use WordDirectory as a backup repository and ignore entries labeled "Directory."

The directory `/cust/word/mmword_local` is a symlink; therefore, you need to replicate its target `/cust/word/<facility_name>`.

Do *not* replicate the directories for `mmword_cache` and `mmword_local`.

The Software Repository should ignore directories that are not actual software repositories while serving files (for example, files should not be served from the

`/cust/word/etc/` directory.)

- Specify the replication rate in seconds.

  Define host chains. Make sure that the host names you specify are the actual host names (that is, the same that the hostname command returns).

  For example, `hostA hostB hostC` means that a directory will be replicated from hostA to hostB to hostC.

  For example `hostA hostB`, `hostA hostC` means that a directory a directory will be replicated from hostA to hostB and from hostA to hostC.

  In these examples, if you want the packages on each Software Repository host backed up, all the hosts have to be in the same multimaster mesh.

  Verify that you can use passwordless SSH to connect from the source host to the destination host as it is specified for each host chain in the `replicator.conf` file (that is, if you specify FQDN, try to connect with SSH with FQDN even if `host.subdomain` resolves to the correct location.)

After you configure the Software Repository Replicator, you must re-start the replicator so that it will automatically re-read its configuration file. At each destination core, wait the time period you specified in the `replicator.conf` file before you re-start the replicator.

To re-start the replicator, enter the following command on the server running the Software Repository component:

```
/etc/init.d/replicator [start/stop]
```

Sample Software Repository Replicator Configuration

```
User: root
Timestampdir: /var/lc/replicator
SSH_PATH: /lc/bin/ssh
Directory: 60 /cust/word/etc
Chain: theword01.subdomain1.domain.com
     theword01.subdomain2.domain.com
Chain: theword01.subdomain1.domain.com
     theword01.subdomain3.domain.com
WordDirectory: 60 /cust/word/facility1
Chain: theword01.subdomain1.domain.com
     theword01.subdomain2.domain.com
WordDirectory: 60 /cust/word/facility2
Chain: theword01.subdomain2.domain.com
     theword01.subdomain3.domain.com
WordDirectory: 60 /cust/word/facility3
Chain: theword01.subdomain3.domain.com
theword01.subdomain1.domain.com
```


Chapter 11: Opsware System Uninstallation

IN THIS CHAPTER

This chapter provides the following information:

- How to un-install a standalone Opsware core
- How to un-install an Opsware core that is part of a multimaster mesh
- How to un-install all cores running in a multimaster mesh so that the entire Opsware System is un-installed

Overview of Un-installing the Opsware System

You might need to un-install an Opsware core in the following scenarios:

- You have an Opsware core in a lab setting before installing the Opsware System in a production environment. You might want to un-install the Opsware core after you finish testing it.
- You are consolidating facilities and want to un-install an Opsware core in one facility in preparation to moving it to another facility.

Un-installing the Model Repository permanently deletes all data in the database. Therefore, when you un-install an Opsware core, you have the choice of whether to preserve the Opsware System data in the Model Repository database. If you choose to preserve the data in the Model Repository, the Opsware Installer stops the un-installation.

Stopping the un-installation gives you the opportunity to back up the data in the Model Repository. After you begin the Model Repository un-installation, the Opsware Installer will not preserve any data in the Model Repository.

You also have the opportunity to preserve or to remove all the packages stored on the Software Repository.

You also have the opportunity to preserve the database of cryptographic material for the Opsware core. If you indicate that you want to preserve crypto, the database of cryptographic material will be saved, otherwise it will be deleted when the un-installation finishes.

Before you un-install an Opsware core, Opsware Inc. recommends that you back up the Oracle database running on the server where the Model Repository is installed. See your Oracle documentation for the steps required to back up an Oracle database.

Un-installing a Standalone Core

Perform the following steps to un-install a standalone core:

1. Before you un-install the Opsware core components from the servers running them, you should deactivate the servers in the Opsware Command Center. See the *Opsware System 4.5 User's Guide* for the steps to deactivate a managed server. Otherwise, if you try to re-install an Opsware core component on one of the servers later, the installation will fail.
2. Make sure all users have logged out of the Opsware Command Center and that no jobs are in progress. To accomplish this task, log into the Opsware Command Center as the Opsware administrator and click Sessions under Administration in the navigation panel.
3. Stop the Opsware Command Center by logging on as root to the server where the Opsware Command Center is running and by entering the following command:

   ```
   /etc/init.d/owm.server stop
   ```

4. Stop all Data Access Engines running in the Opsware core.

   Log on as root to the server where the Data Access Engine is running and enter the following command:

   ```
   /etc/init.d/spin stop
   ```

5. If the Opsware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin stop` command on the Opsware Command Center server.
6. Un-install the Opsware components on the servers where they are installed. Each component must be un-installed separately.

   ```
   /opsware_system/disk001/opsware_installer/uninstall_
   opsware.sh -r <full_path_to_response_file_for_this_core>
   ```

   The Opsware Installer menu does *not* present the list of components in the order in which they must be un-installed. You *must* un-install the components one at a time in the following order:

1. Opsware Command Center (owc)
2. OS Provisioning Media Server
3. OS Provisioning Boot Server
4. OS Provisioning Build Scripts
5. Software Repository (word)
6. Command Engine (way)
7. Access & Authentication Directory (cast)
8. Data Access Engine (spin)
9. Model Repository (truth)

Recovering from un-installing some components is extremely difficult; therefore, the Opsware Uninstaller might enter a mini interview to confirm un-installation.

7 Get a list of remaining packages on each core server by entering the following command:

```
/lc/bin/rpm -qa
```

8 Use RPM to un-install the remaining packages from each server by entering the following command.

```
/lc/bin/rpm -e <list_of_packages_from_previous_step>
```

Enter the packages as a space delimited list.

9 Remove the following directories and whatever files or subdirectories they contain from each core server. Performing this step removes all Opsware Installer logs in the directory `/var/lc/install_opsware`.

- `/lc`
- `/opt/OPSW` (depending on your environment, directory might *not* be present)
- `/var/lc`

If you indicated at the prompt that you want to preserve crypto (the database of cryptographic material), you should not delete the `/var/lc` directory. Deleting the `/var/lc` directory deletes the database of cryptographic material.

Un-installing One Core in a Multimaster Mesh

When un-installing a core from a multimaster mesh, you should not un-install the source core unless you are planning to un-install the entire mesh.

See “Un-installing an Entire Multimaster Mesh of Opsware Cores” on page 157 in this chapter for more information

Perform the following steps to un-install one core in a multimaster mesh:

1. Make sure all users have logged out of the Opsware Command Center and that no jobs are in progress. To accomplish this task, log into the Opsware Command Center as the Opsware administrator and click Sessions under Administration in the navigation panel.
2. Log in to any Opsware Command Center that is still online to perform the following tasks:
   1. First decommission all the servers in the core that you are uninstalling and then decommission the facility.
      - To decommmission the facility, from the navigation panel, click Facilities under Environment.
      - In the Facilites page, select the facility. The Facilities: Edit Facility page appears.
      - Update the “Is this facility in use” field in Facility Information to No. Click Save.
   2. Using the System Configuration channel, update the `listeners` configuration parameter by removing the entry for the core that is being un-installed. Update the listeners parameter by selecting “Model Repository, Multimaster Component” in the System Configuration page.
   3. If a Data Access Engine that is being un-installed is currently serving as the multimaster central role, a Data Access Engine in another core must be selected to serve as Multimaster Central.

      The Data Access Engine server that is being un-installed must be moved back to the Services | Opsware | spin node, and a Data Access Engine server that is not being un-installed must be moved to the Services | Opsware | spin | Multimaster Central node.

      See “Reassigning the Data Access Engine to a Secondary Role” on page 72 in Chapter 4 for more information

4. Verify that all transactions have propagated to the other facilities, except for the facility that is being un-installed.

   See "Verifying Multimaster Transaction Traffic" on page 134 in Chapter 8 for more information.

3. Restart the Multimaster Replication Engine in all cores except the core that is being un-installed by entering the following command as root on the server running the Model Repository:

   ```
   /etc/init.d/vaultdaemon stop
   ```

   ```
   /etc/init.d/vaultdaemon start
   ```

4. Stop the Opsware Command Center in the core that is being un-installed by entering the following command as root:

   ```
   /etc/init.d/owm.server stop
   ```

5. In the core that is being un-installed, stop all Data Access Engines.

   Log in as root to the server where the Data Access Engine is running and enter the following command:

   ```
   /etc/init.d/spin stop
   ```

6. If the Opsware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin stop` command on the Opsware Command Center server.

7. Stop the Multimaster Replication Engine in the core that is being un-installed by entering the following command as root on the server running the Model Repository:

   ```
   /etc/init.d/vaultdaemon stop
   ```

8. Restart the Data Access Engine that is serving as Multimaster Central by entering the following command as root:

   ```
   /etc/init.d/spin stop
   ```

   ```
   /etc/init.d/spin start
   ```

9. Un-install the Opsware components on the servers where they are installed. Each component must be un-installed separately.

   ```
   /opsware_system/disk001/opsware_installer/uninstall_
   opsware.sh -r <full_path_to_response_file_for_this_core>
   ```

The Opsware Installer menu does *not* present the list of components in the order in which they must be un-installed. You *must* un-install the components one at a time in the following order:

1. Opsware Command Center (owc), Multimaster Component
2. OS Provisioning Media Server
3. OS Provisioning Boot Server
4. OS Provisioning Build Scripts
5. Software Repository (word), Multimaster Component
6. Command Engine (way), Multimaster Component
7. Access & Authentication Directory (cast)
8. Data Access Engine (spin), Multimaster Component
9. Model Repository (truth), Multimaster Additions

Recovering from un-installing some components is extremely difficult; therefore, the Opsware Uninstaller might enter a mini interview to confirm un-installation.

10 Get a list of remaining packages on each core server by entering the following command:

```
/lc/bin/rpm -qa
```

11 Use RPM to un-install the remaining packages from each server by entering the following command:

```
/lc/bin/rpm -e <list_of_packages_from_previous_step>
```

Enter the packages as a space delimited list.

12 Remove the following directories and whatever files or subdirectories they contain from each core server. Performing this step removes all Opsware Installer logs in the directory `/var/lc/install_opsware`.

- `/lc`
- `/opt/OPSW` (depending on your environment, directory might *not* be present)
- `/var/lc`

If you indicated at the prompt that you want to preserve crypto (the database of cryptographic material), you should not delete the `/var/lc` directory. Deleting the `/var/lc` directory deletes the database of cryptographic material.

Un-installing an Entire Multimaster Mesh of Opsware Cores

Perform the steps in this procedure only when you want to un-install all cores in a multimaster mesh:

1. Make sure that all users have logged out of the Opsware Command Center and that no jobs are in progress. To do this task, log in to the Opsware Command Center as the Opsware administrator and click Sessions under Administration in the navigation panel.
2. Stop the Opsware Command Center by logging on as root to the server where the Opsware Command Center is running and enter the following command:

   ```
   /etc/init.d/owm.server stop
   ```

3. Stop the Data Access Engine.

   Log in as root to the server where the Data Access Engine is running and enter the following command:

   ```
   /etc/init.d/spin stop
   ```

   If the Opsware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin stop` command on the Opsware Command Center server.

4. Stop the Multimaster Replication Engine in all cores by logging in to the servers running the Model Repositories and entering the following command as root:

   ```
   /etc/init.d/vaultdaemon stop
   ```

5. In each core, un-install the Opsware components on the servers where they are installed. Each component must be un-installed separately.

   ```
   /opsware_system/disk001/opsware_installer/uninstall_
   opsware.sh -r <full_path_to_response_file_for_this_core>
   ```

   The Opsware Installer menu does *not* present the list of components in the order in which they must be un-installed. You *must* un-install the components one at a time in the following order:

1. Opsware Command Center (owc), Multimaster Component
2. OS Provisioning Media Server
3. OS Provisioning Boot Server
4. OS Provisioning Build Scripts
5. Software Repository (word), Multimaster Component
6. Command Engine (way), Multimaster Component
7. Access & Authentication Directory (cast)
8. Data Access Engine (spin), Multimaster Component
9. Model Repository (truth), Multimaster Additions

Some of these components might exist only in the source core. Recovering from un-installing some components is extremely difficult; therefore, the Opsware Uninstaller might enter a mini interview to confirm un-installation.

6 In each Opsware core, get a list of remaining packages on each server that is running an Opsware component by entering the following command:

```
/lc/bin/rpm -qa
```

7 In each Opsware core, use RPM to un-install the remaining packages from each server that is running an Opsware component by entering the following command:

```
/lc/bin/rpm -e <list_of_packages_from_previous_step>
```

Enter the packages as a space delimited list.

8 In each Opsware core, remove the following directories and whatever files or subdirectories they contain from each server that is running an Opsware component. Performing this step removes all Opsware Installer logs in the directory `/var/lc/install_opsware`.

- `/lc`
- `/opt/OPSW` (depending on your environment, directory might *not* be present)
- `/var/lc`

If you indicated at the prompt that you want to preserve crypto (the database of cryptographic material), you should not delete the `/var/lc` directory. Deleting the `/var/lc` directory deletes the database of cryptographic material.

Index

L

M

N

O

P

R

S

T

U

V

W

