Oracle® Communications MetaSolv Solution

Installation Guide

Release 6.3

E69836-06

January 2020

ORACLE®

Oracle Communications MetaSolv Solution Installation Guide, Release 6.3

E69836-06

Contents

Preface

1   Installation Overview

2   Setting Up The MSS Database

3   Preparing For the Application Server Installation

4   Installing and Deploying MetaSolv Solution on a Single Server

5   Installing and Deploying MetaSolv Solution on a Clustered Server

6 Upgrading Oracle Communications MetaSolv Solution

7 Installing The Client Workstation

8   Performing Post-Installation Tasks

9   Configuring JDBC Active GridLink Data Sources

10   Performing Maintenance and Troubleshooting

A   Proxy Server Setup

B   Oracle Communications MetaSolv Solution Components

C   Planning Worksheets

D Configuration Values

E Load Balancer Configuration Example

F Tuning Servers For Performance

G Configuration Files

Preface

This guide contains the procedures and information you need to install and initially configure Oracle Communications MetaSolv Solution (MSS) and its utility programs.

This guide includes some information on third-party software products used by MSS. However, this information is limited to information needed to install and perform initial configuration tasks. If you need additional information on a third-party software application, consult the documentation provided by the product's manufacturer.

Audience

This guide is for individuals responsible for installing or maintaining MSS and ensuring the software is operating as required. This guide assumes the installer has an Oracle DBA and WebLogic administrator background, with a working knowledge of Java JEE.

Related Documents

For more information, see the following documents in the MSS documentation set:

- *MSS Planning Guide:* Describes information you need to consider in planning your MSS environment prior to installation.
- *MSS System Administrator's Guide:* Describes postinstallation tasks and administrative tasks such as maintaining user security.
- *MSS Security Guide:* Provides guidelines and recommendations for setting up MSS in a secure configuration.
- *MSS Database Change Reference:* Provides information on the database changes in MSS releases.
- *MSS Network Grooming User's Guide:* Provides information about the MSS Network Grooming tool.
- *MSS Address Correction Utility User's Guide:* Provides information about the MSS Address Correction utility.
- *MSS Technology Module Guide:* Describes each of the MSS technology modules.
- *MSS Data Selection Tool How-to Guide:* Provides an overview of the Data Selection Tool, and procedures on how it used to migrate the product catalog, equipment specifications, and provisioning plans from one release of your environment to another.
- *MSS CORBA API Developer's Reference:* Describes how MSS APIs work, high-level information about each API, and instructions for using the APIs to perform specific tasks.

- *MSS Custom Extensions Developer's Reference:* Describes how to extend the MSS business logic with custom business logic through the use of custom extensions.

- *MSS Web Services Developer's Guide:* Describes the MSS Web Services and provides information about the MSS Web Service framework that supports web services, the various web services that are available, and how to migrate existing XML API interfaces to web service operations.

- *MSS EJB API Developer's Reference:* Provides an overview of the MetaSolv Solution EJB APIs and instructions for using the APIs to perform tasks.

For step-by-step instructions for tasks you perform in MSS, log in to the application to see the online Help.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Installation Overview

This chapter provides a high-level overview of the steps needed to perform an Oracle Communications MetaSolv Solution (MSS) installation.

Installation Process

This section provides an overview of the installation process. The chapters that follow provide full information on each step. Figure 1-1 shows the high-level installation process.

Figure 1-1   Overview of the MSS Installation Process
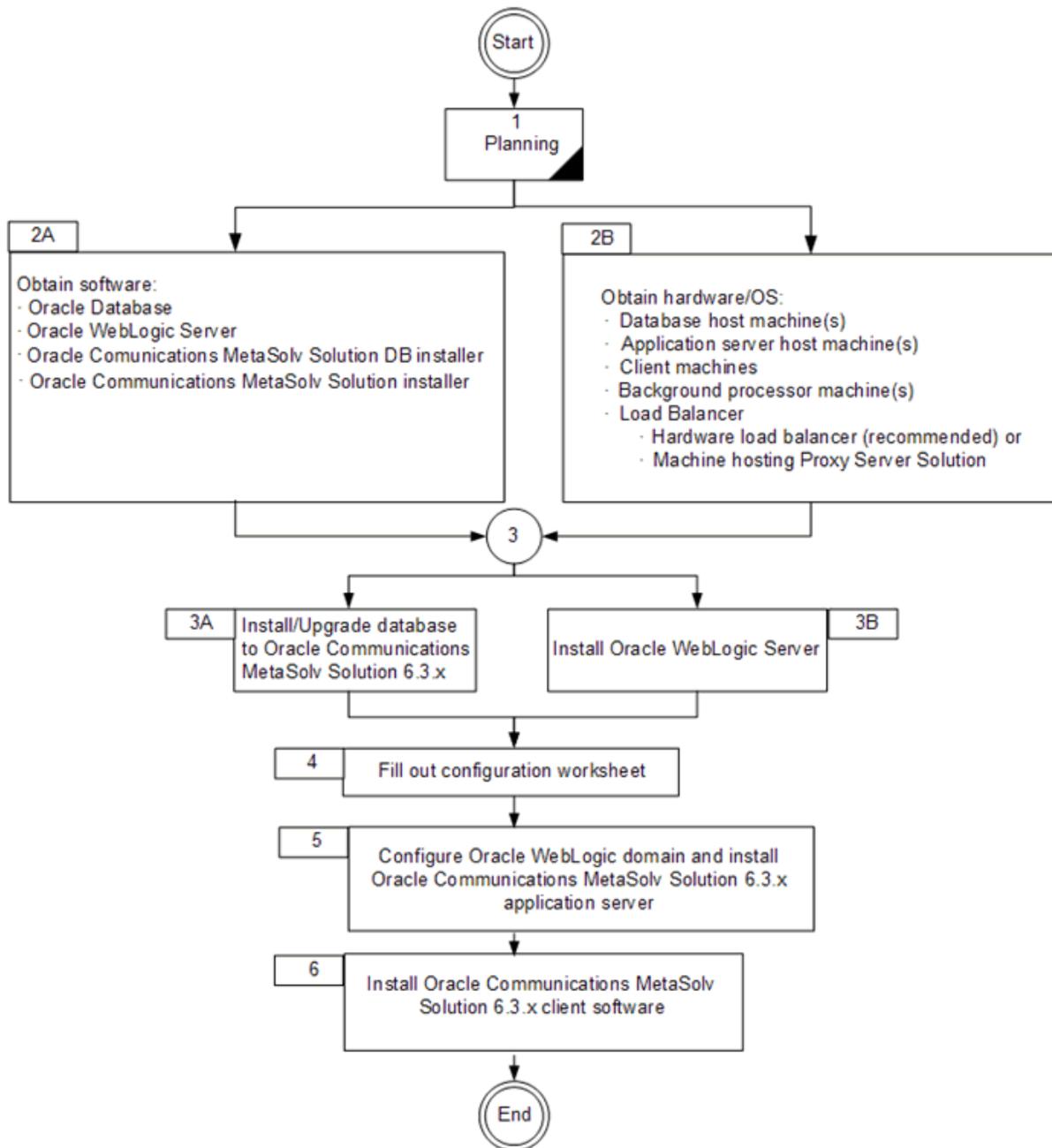
The Oracle database client software is required for MSS utilities, NPA/NXX Split utility, and Location and Routing Gateway (LERG). After the Oracle WebLogic domain is configured, the MSS installer identifies the configuration and sets the appropriate parameters for the installation.

See "Software Requirements" for information on the required software versions.

Software Requirements

MSS consists of an application that is installed on a WebLogic server and client workstations. It connects with the Oracle database to store all relevant information. Table 1-1 provides the version information of the required software for MSS.

Table 1-1   Required Software Versions

Product	Version
Oracle WebLogic Server	12*c*R2 • 12.2.1.2 (not supported from patch 6.3.0.1003 on) • 12.2.1.3 (supported from patch 6.3.0.643.3 on) • 12.2.1.4 (supported from patch 6.3.0.1003 on)
Oracle Database	• 12cR1 (12.1.0.2.1) • 12cR2 (12.2.0.1.0) - supported from patch 6.3.0.639 on • 18c (18.3.0.0.0) - supported from patch 6.3.0.982 on
Oracle Database Client	12*c* or 18*c*
Java Development Kit (JDK)	8 (with latest critical patch update)
JacORB	3.9 (installed with the MSS installation)

If You Are a New Customer

The current release requires the following installation tasks:

- **Database**: Install the Oracle database. See "Setting Up The MSS Database" for complete information.
- **Application Server**: Install the Oracle WebLogic application server:
  – For more information about Oracle WebLogic Server 12cR2 (12.2.1.3.0), visit the Oracle WebLogic Server Product Documentation website at:

    `http://docs.oracle.com/middleware/12213/wls/index.html`

  – For more information about Oracle WebLogic Server 12cR2 (12.2.1.4.0), visit the Oracle WebLogic Server Product Documentation website at:

    `https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/index.html`

  See "Software Requirements" for information on required software versions.

- **Client Workstation**: See "Installing The Client Workstation" for information on installing individual workstations.

If You Are an Existing Customer

The upgrade path for the MSS database differs from the path for the application server. This section explains the upgrade path for each component.

Database Upgrade Path

Figure 1-2 shows the upgrade path for the MSS database if you are on a pre-6.3.*x* version.

Figure 1-2   MSS Database Upgrade Path
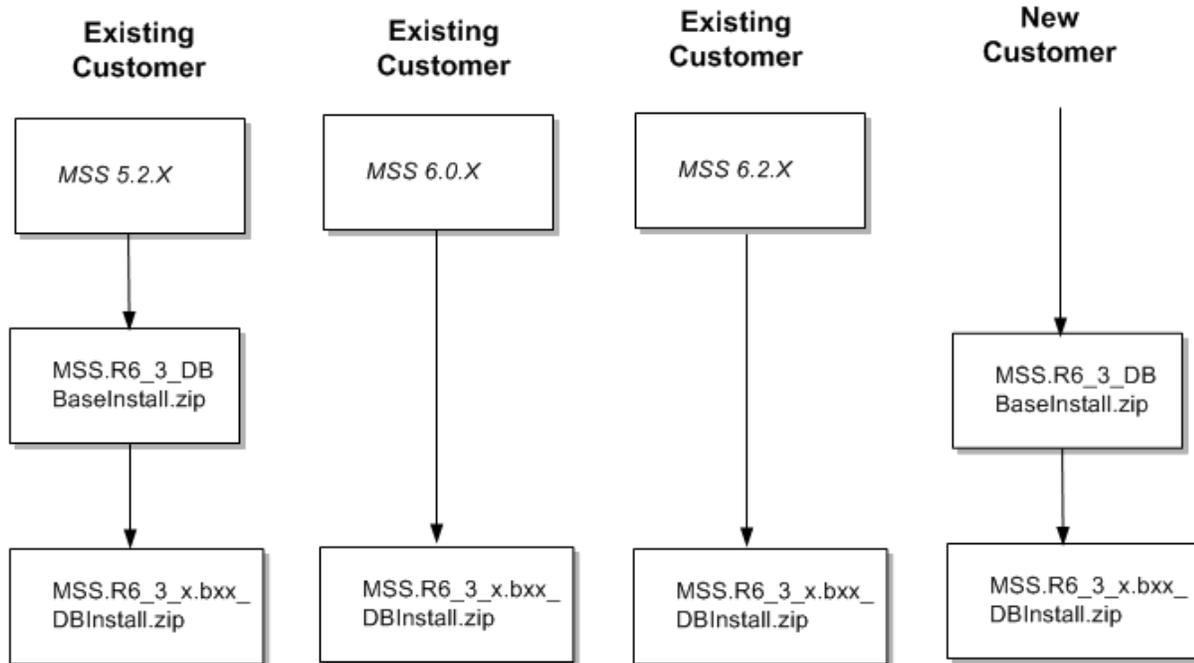
Application Server Upgrade Path

Due to platform changes made in MSS 6.3.*x*, it is necessary to perform a full installation of the application server the first time you take this release.

Refer to "Installing and Deploying MetaSolv Solution on a Single Server " or "Installing and Deploying MetaSolv Solution on a Clustered Server".

The upgrade option in the installer can be used to install subsequent maintenance releases and patches. Refer to the specific maintenance release or patch file for detailed instructions. If you are installing a patch, refer to "Upgrading Oracle Communications MetaSolv Solution".

Related Software Dependencies

ASR and LSR require the following actions:

- If you use ASR or LSR, you must reinstall the ASR or LSR software after the new version of MSS is installed.

- If you have LSR 6 or LSR 9 orders currently open, those orders will be view only in MSS 6.3.*x*. To avoid this situation, close any open orders before you move to MSS 6.3.*x*, or upgrade the orders to LSOG 10 before or after installing MSS 6.3.*x.*

Downloading the Installation Files

Before you begin the installation, download the MSS files for the platform you are using from the Oracle software delivery website:

http://edelivery.oracle.com

Identifying the Installation Files

This section explains which installation files you need to download from the Oracle software delivery website. Generic file names are used to identify the files in this section. Figure 1-3 shows the naming format used on the Oracle software delivery website.

Figure 1-3   File Naming Format
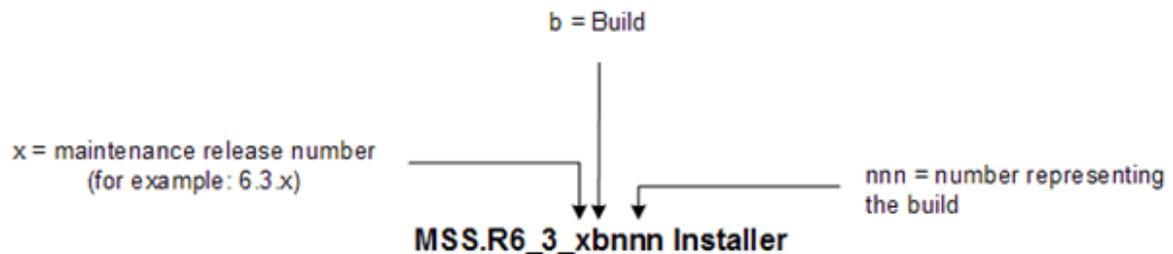
Where to Download the Files

Download the application server/client installation files to the appropriate platform (Windows, Sun Solaris, or Linux) directly to the application server machine you intend to install on. The client files are downloaded and installed from the application server machine.

Data Migration

If you are moving to MSS 6.3.x from a pre-MSS 6.0 release, it might be necessary for you to perform a data migration. The Broadband Module available before MSS 6.0 has been discontinued, and customers who use the Broadband Module must migrate data to use Oracle's network templates, which replace the broadband functionality. Two tools are available to assist with the migration effort:

- Pre-Migration Analysis Tool (PMAT): This tool can be run against your pre-MSS 6.0 database to determine the amount of data that potentially may need to be converted. This includes circuits (bandwidth, virtual, facilities, specials), product catalog, and orders. This tool is located on the Oracle software delivery website.

- Next-Generation Migration Tool: This tool is part of MetaSolv Solution Utilities. This tool automates the process of migrating network elements, migrating network

systems, migrating connections, and the circuit conversion to next gen connections and any related order conversion.

Refer to *MetaSolv Solution 6.0 Migration Guide* on the Oracle Help Center.

Basic Installation Steps

Each of the steps shown here for installing MSS contains additional tasks and information that you must know to proceed with the installation. The chapters in this book discuss each basic step.

1. Plan the installation by completing the following tasks:

   a. Plan for the hardware and software you will need to implement MSS.

      See *MetaSolv Solution Planning Guide* for information on minimum technical requirements.

   b. Complete the pre-installation checklist in this chapter.

      The checklist contains planning tasks that should be done before you begin the installation process.

2. Obtain the appropriate hardware and software.

3. Prepare the database and application server environments by completing the following tasks:

   a. Install Oracle Database. See "Software Requirements" for information on required software versions.

   b. Install the MSS 6.3.*x* database.

      To complete this step, you must run the appropriate MSS database scripts. If you do not currently have the recommended release of the database installed, see "Setting Up The MSS Database" for information on getting your database to the current release level so that you can apply the current maintenance release.

      See "Software Requirements" for information on required software versions.

   c. Install third-party software on machines that will host the application server.

      To complete this step, you must:

      Install Oracle WebLogic Platform on each machine hosting MSS. You can install your system in different configurations, but each machine must have Oracle WebLogic software installed. See "Software Requirements" for information on required software versions.

4. Complete the worksheets that define properties for the installation machines.

   Worksheets are included for each installation configuration type that MSS provides. The worksheets let you identify, in advance, information that is needed during the installation.

5. Install and deploy MSS on the Oracle WebLogic application servers by completing the following tasks:

   a. Create the Oracle WebLogic domain and define the administration server and its clustered servers, or the single server.

When you create the domain and define the server(s) that belong to the domain, the Oracle WebLogic software creates the necessary files on the servers you indicate.

b. Install and deploy MSS.

To complete this step, you must:

- Run the installer to copy MSS files to every machine that will host Oracle WebLogic application server(s).

- In the situation where the administration server is on a separate machine, it is not necessary to load MSS on that machine.

- Deploy MSS from the single server or administration server to the managed servers.

6. Install on the client workstation.

You must perform an initial client installation to perform post-installation tasks that require the use of the client.

To complete this step, you must:

a. Install the client on a workstation.

See "Installing The Client Workstation" for more information.

b. Install utilities or any other MSS components.

7. Complete the post-installation tasks.

Tasks include:

- Loading graphics to the database from a utility program.

- Running a client utility to determine the health of the database.

- Customizing the application with your company logo (optional).

- Setting up user authentication.

Pre-installation Checklist

The following list indicates the information you need to research and understand before you start the installation process for MSS and the third-party software it requires. As you identify names, IP addresses, and so on, keep a written record of the information. You will need it during the system installation.

- See *MetaSolv Solution Planning Guide* for the proper hardware and software for the application server, database server, and client machines.

- Back up any customized reports and stored procedure exits. See the discussion on customizing the application in the *MetaSolv Solution System Administrator's Guide* for more information.

- Identify the following:

  – Application server machines, names, and IP addresses.

  – Database server machine, name, IP address, database SID name, and database port (default = 1521).

  – See "Planning Worksheets" for help identifying and completing this information for the installation type you select.

- Do a DNS and reverse DNS lookup for each application server machine from a user workstation.

  – DNS lookup: From a user workstation, use the `nslookup` command for the application server machine DNS name.

    For example: **`nslookup serversun`**1

  – Reverse DNS lookup: From a user workstation, use the `nslookup` command for the application server machine IP address.

    For example: **`nslookup 192.0.2.225`**

  If the name or IP address is not found, contact your system administrator.

- Test network connectivity between the following machines:

  – Application server machine to the database server machine

  – Log on to the application server machine and ping the database server machine using either the DNS name or the IP address. Do this for each application server machine.

  – Database server machine to the application server machine

  – Log on to the database server machine and ping the application server machine using either the DNS name or the IP address. Do this for each application server machine.

- (Optional) Before you install MetaSolv Solution in an IPv6 domain, ensure that your firewall configuration supports IPv6 addresses. If your firewall configuration does not support IPv6 addresses, you must enable HTTP tunneling in the WebLogic Server Administration Console. See "Enabling HTTP Tunneling" for more information.

- If your firewall does network address translation (NAT) and MSS end users reside outside the firewall, define an external DNS name for the Oracle WebLogic Server. Contact your network/transport and system administrator groups to verify and define the external DNS, if necessary.

To add an external DNS name:

1. Log in to the Oracle WebLogic Administration Server Console.

2. In the Change Center pane, click **Lock & Edit**.

3. In the Domain Structure tree, expand **Environment** and then select **Servers**.

   The Summary of Servers pane appears.

4. Click the *server_name* (admin server).

   The Settings for *server_name* pane appears.

5. Click the **General** tab and then click the **Advanced** link.

   The following Figure 1-4 pane appears.

Figure 1-4   Display After Clicking the Advanced Link

6. Enter the address into the **External Listen Address** field and click **Save**.

    a. If you are using an external load balancer, the following conditions must be met:

        •   **Server affinity**: Sticky Session must be enabled.

        •   **Cookie persistence**: The load balancer must NOT modify WebLogic cookies.

    b. Choose the installation configuration you plan to use for the application server(s):

        •   **Single server:** You can have multiple single server instances.

        •   **Clustered servers:** This configuration provides failover benefits.

    c. Download the MSS 6.3.*x* files from the Oracle software delivery website.

    d. If cluster is configured, create a DNS entry including all clustered managed servers' listening IP addresses in the same cluster. This DNS entry will be used as Cluster Address for the cluster during domain configuration in production environment.

    e. (Optional) If you are creating the cluster in an IPv6 domain in a dual-stack machine, ensure that you specify the IPv6 address and the system name in the **etc/hosts** file, as follows:

        ```
        IPv6address          ipv6machine@example.com        ipv6machine
        ```

    f. If you are connecting to an IPv6 server for accessing MSS client application, ensure that you specify the server's IPv6 address in the client machine's **etc/hosts** file, as follows:

        ```
        IPv6address          ipv6machine@example.com        ipv6machine
        ```

Installing on a UNIX/Linux Platform

The following list contains special tasks required for graphics on a UNIX/Linux machine:

- To run the installation using a graphical user interface:
    - On a workstation, start an X-Windows emulator.
    - On the UNIX machine, set the `DISPLAY` environment variable to send the graphical display to the workstation.
    - `$DISPLAY=`*mymachinename*`:0.0;export DISPLAY`

- Enable xhost for application servers that run on a UNIX/Linux machine.

    To enable the lookup of graphic settings on the application server, you must enable xhost on the machine. Run the following command on the application server machine while logged on as **root**:

    ```
    xhost +
    ```

Directory Placeholders Used in This Guide

The following placeholders are used in this guide:

Table 1-2   Placeholder Directories in This Guide

Placeholder	Directory Description
MW_HOME	The directory location where Oracle Fusion Middleware components are installed. This directory contains the base directory for WebLogic Server. For example: MW_HOME=/opt/Oracle/Middleware/Oracle_Home
MSLV_HOME	The directory location where MSS software is installed. MSS requires each server directory and its WebLogic domain directory to be placed in the MSLV_Home directory. For example: MSLV_HOME=/opt/m63Single/single
m63domain	The directory location that contains the configuration for the domain into which MSS is installed.
mslv01	The directory location which is the MSS server home directory.

See "Directory Structure" for additional examples of directory values.

2
Setting Up The MSS Database

This chapter assumes that you already have Oracle Database installed on the database server. Consult the Oracle Database online documentation for questions on how to install the database software.

Oracle Communications MetaSolv Solution (MSS) supports the Oracle Database multitenant architecture, which enables you to run the MSS database instance as a pluggable database (PDB) within a container database (CDB). For information about the Oracle Database multitenant architecture, see *Oracle Database Administrator's Guide*.

This chapter explains how to install a new database or bring your existing database to the 6.3.*x* GA level. Specifically, the chapter covers how to:

- Extract the database scripts.
- Create tablespaces (only for new users).
- Run the upgrade or installation scripts to make specific changes to bring the database structure to the Oracle Communications MetaSolv Solution (MSS) 6.3.*x* level.
- Drop the **app_data** tablespace (only for users who are upgrading).

Some sections apply to new customers who have never installed an MSS database before, and some apply to existing customers who have previously installed the database but need to bring the database up to the current level.

Getting the Database to the Current GA Level

The MSS database upgrade and installation files enable you to get the database to the current MSS GA level.

If you are currently at MSS 5.2.x, you must first extract and run the MSS R_3_DBBaseInstall.zip script first, and then extract and run the MSS.R6_3_x.bxx_DBInstall.zip script.

If you are currently at MSS 6.0.x or MSS 6.2.x, you are required to extract and run only the MSSR6_3_x_bxx_DBInstall.zip script.

If you are installing MSS 6.3.x for the first time, you must first extract and run the MSS R_3_DBBaseInstall.zip script first, and then extract and run the MSS.R6_3_x.bxx_DBInstall.zip script.

The MSS R_3_DBBaseInstall.zip script sets up the database structure and the MSS.R6_3_x.bxx_DBInstall.zip script installs the MSS 6.3.x database.

Figure 2-1 depicts the upgrade and installation paths for setting up an MSS 6.3.*x* database.

Figure 2-1   MSS Database Upgrade and Installation Paths
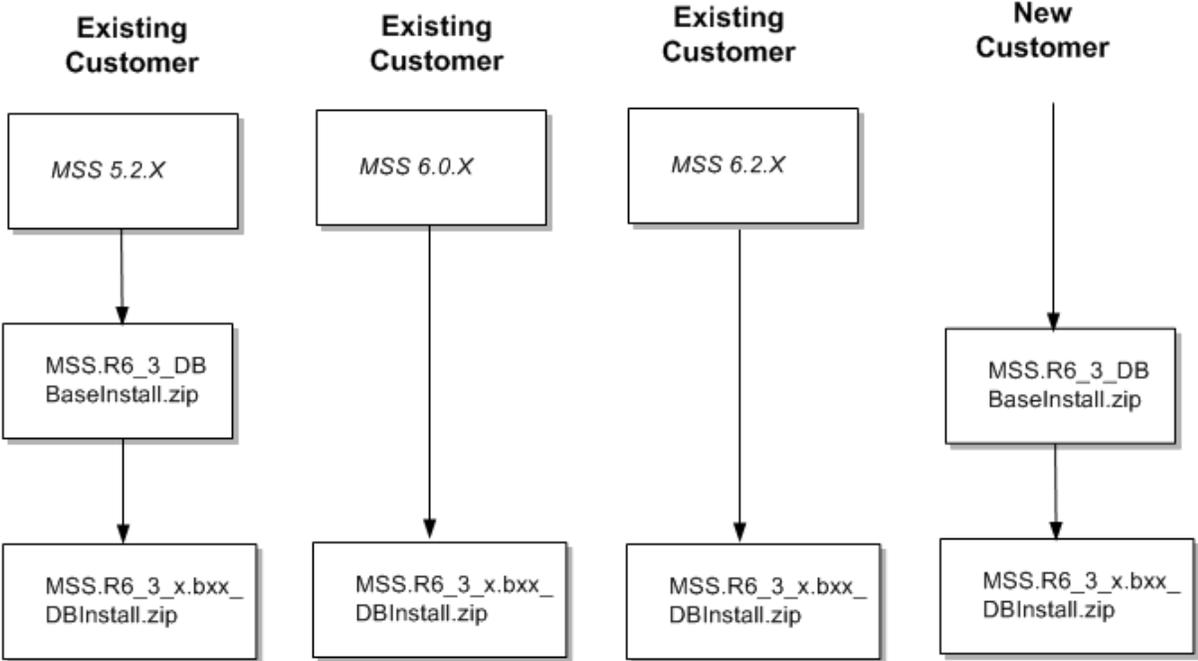
Database Space Requirements

The database installation requires approximately 2.5 GB of free space. This default size is based on a production database supporting 100,000 circuits. The specific space requirements are shown in Table 2-1.

Table 2-1   Space Requirements for Installation Files

File Name	Size
DATA	1325 MB
INDEXES	700 MB
SYSTEM	200 MB
TEMP	100 MB
SYSAUX	200 MB
Total Size	**2.5 GB**

Prerequisites

- Ensure that you have installed Oracle Database on the database server machine. Work with Oracle Global Customer Support to determine the recommended Oracle database software patch level for your intended platform and version combination.

  See "Software Requirements" for information on required software versions.

- Ensure that you set the recommended database initialization parameters for the Oracle Database version that you are using. Table 2-2 lists the recommended initialization parameter settings.

- For technical bulletins that pertain to this release, click the **Knowledge** tab on the My Oracle Support website:

  https://support.oracle.com

Table 2-2   Oracle Database Recommended Initialization Parameter Settings

Oracle Database Version	Initialization Parameter	Recommended Value	Example
12cR1	O7_DICTIONARY_ACCESSIBILITY[1] _grant_secure_role[1] optimizer_features_enable[2] optimizer_adaptive_features[3]	TRUE TRUE 12.1.0.2.1 FALSE	• O7_DICTIONARY_ACCESSIBILITY=TRUE • _grant_secure_role=TRUE • optimizer_features_enable=12.1.0.2.1 • optimizer_adaptive_features=FALSE
12cR2	O7_DICTIONARY_ACCESSIBILITY[1] _grant_secure_role[1] _enable_secure_sub_role[1]	TRUE TRUE TRUE	• O7_DICTIONARY_ACCESSIBILITY=TRUE • _grant_secure_role=TRUE • _enable_secure_sub_role=TRUE
18c	O7_DICTIONARY_ACCESSIBILITY[1] _grant_secure_role[1] _enable_secure_sub_role[1]	TRUE TRUE TRUE	• O7_DICTIONARY_ACCESSIBILITY=TRUE • _grant_secure_role=TRUE • _enable_secure_sub_role=TRUE

[1] This parameter ensures that the install script completes successfully.

[2] This parameter must be set to the version of the database.

[3] This parameter optimizes database performance.

Extracting the MSS Database Scripts

The first set of scripts that need to be run reside in the **MSS.R6_3_DBBaseInstall.zip** file. You can extract the contents of this ZIP file to the directory of your choice. This ZIP file contains database scripts used to set up the structure for an MSS 6.3.*x* database.

See "Getting the Database to the Current GA Level" for information about which MSS database scripts you need to run and in what sequence, depending on the MSS version you are currently at.

To extract the MSS database scripts to the database server machine, do the following:

1. Extract the **MSS.R6_3_DBBaseInstall.zip** file into a directory. Oracle recommends extracting the scripts to a directory on your database server.

   The second set of scripts that you must run reside in the **MSS.R6_3_0.b***xxx***_DBInstall.zip** file (where *xxx* is the build number). This ZIP file contains database scripts used to upgrade an existing MSS 6.0.2 or higher database to MSS 6.3.*x*.

2. Extract the **MSS.R6_3_0.b**xxx_**DBInstall.zip** file into a directory. Oracle recommends extracting the scripts to a directory on your database server.

Creating Tablespaces (New Customers Only)

If you are setting up your database for the first time, you must create tablespaces using the scripts extracted from the **MSS.R6_3_DBBaseInstall.zip** file.

The **a_tblspc.sql** file, located in the directory where you installed the database scripts, creates tablespaces. You must modify the file and run it to create tablespaces. Make sure you have write privileges for the file and modify the following information:

- Path to the datafile
- Tablespace size

> **Note:**
>
> All tablespace sizes must be equal to or greater than the space requirements listed in Table 2-1.

The following UNIX/Linux example shows the line you must modify.

```
REM * Create a table space for DATA.
create tablespace DATA datafile '...'  size   1325M
create management local SEGMENT SPACE MANAGEMENT AUTO;
```

To run **a_tblspc.sql**, do the following:

1. Log on to the database server as a user with database administrator privileges and start SQL*Plus.

   User ID: *system*

   Password: *manager*

   Host String: *Database_name_of_the_Oracle_instance*

2. Run **a_tblspc.sql**.

Running the Installation Scripts (New Customers Only)

Each script writes an audit log to a subdirectory called **Audits**. The **Audits** subdirectory is located in the same directory as the database installation scripts.

Prerequisites

Before running the installation scripts, extracted from the **MSS.R6_3_DBBaseInstall.zip** file:

- The script file **_instmss.sql** is for new installations only. You must have database administrator privileges to complete this procedure.
- The following script files create database users and you need to supply passwords for these application users. Modify the script files by replacing occurrences of <PASSWORD HERE> with a password.

   – db/inst_60/app_users.sql

   – db/inst_60/a_users.sql

> **Note:**
>
> In Oracle Database 12c the passwords are case-sensitive.

To begin the installation, do the following:

1. In SQL*Plus, run _**instmss.sql** and complete the following information:

   a. Enter the operating system for the SQL*Plus client (the machine you are running the scripts from) and press ENTER.

   This value is either **UNIX/Linux** or **Windows**. **Windows** is the default.

   b. Enter the full directory path for the SQL script files.

   The path must include the trailing virgule (/ for UNIX and Linux or \ for Windows), and you must be able to write to the directory. If you enter an invalid path or a protected directory, SQL*Plus exits.

   The path length is limited by SQL*Plus and the operating system.

   c. Enter the database name.

   d. Enter each of the following passwords and press ENTER after each one:

   ASAP, **EBOND**, **EDI**, **JOB**, and **SYS_ERROR**

   If a password fails, SQL*Plus exits. If this happens, review **a_getpas.log** for errors.

   This step initiates the installation process. When the installation is complete, you receive an **Install Complete** message.

   If this message does not appear, the installation process was not successful and must be restarted beginning with step 1. Prior to restarting, back up the Audits directory. If you restart the installation process, ORA- messages appear for every item that failed.

2. Search the files in the **Audits** directory for **ORA**-.

3. When the installation is complete, run the **mdl_cur.sql** script.

   This process can take up to 30 minutes to complete. The **mdl_cur.sql** spools a report in the **Audits** directory called **mdl_cur.txt**. The report verifies the database structure by identifying missing tables or columns, extra tables or columns, and differences with column data types as compared to the database. If no ORA- messages are found and the **mdl_cur.txt** file is clean, the installation completed successfully.

4. Run the **mdl_cmp.sql** script.

   This script spools a report in the **Audits** subdirectory called **mdl_cmp.txt.** The report indicates extra or missing indexes, primary keys, foreign keys, and sequences. This script gives the option to fix problems or only report the differences. When you run the script, you can compare the differences for individual sections or for all sections. The default is to compare all sections.

5. Install the MSS 6.3.*x* database, using the scripts extracted from the **MSS.R6_3_0.DBInstall.zip** file.

ORACLE

For complete instructions on installing the MSS 6.3.*x* database, refer to the following sections, in "Upgrading Oracle Communications MetaSolv Solution" of this guide:

- Upgrading Oracle Communications MetaSolv Solution
- Updating Stored Procedures
- Running Reports

Running the Upgrade Scripts (Existing 5.2.*x* Customers Only)

This section explains how to upgrade an existing MSS 5.2.*x* database to an MSS 6.3.*x* database.

Prerequisites

Before upgrading the database, complete the following tasks:

- Back up the existing MSS database.
- Empty the job queue for the Background Processor.

  Use Job Queue Manager to verify that the job queue is empty Oracle recommends that no other jobs run in the background during the upgrade.

- Confirm that the user IDs ASAP, EBOND, EDI, JOB, and SYS_ERROR exist on the instance, and that ASAP has DBA-level authority.
- Perform a test run of the upgrade process on a copy of the production database.
- Update your database statistics to ensure the upgrade conversions perform as tested. Refer to the Oracle Database online documentation for more information on the Analyze command.
- The following script file creates database users and you need to supply passwords for these application users. Modify the script file by replacing occurrences of <PASSWORD HERE> with a password.

  db/upg_60/app_users.sql

> ✎ **Note:**
>
> In Oracle Database 12c the passwords are case sensitive.

Running the Upgrade Scripts

To upgrade the database

1. Log on to the database server as ASAP.

   Password: *ASAP_password*

   Host String: *Name_of_your_5.2_database*

2. Run the SQL scripts in the **precheck** folder. (optional)

These scripts generate information on the data to be converted during the upgrade.

3. Run the **mdl_pri.sql** script.

   a. Enter the operating system (either UNIX or Windows) for the SQL*Plus client.

   > **Note:**
   >
   > If you are using a Linux operating system, enter UNIX.

   b. Enter the full directory path for the SQL script files.

   The path must include the trailing virgule (/ for UNIX and Linux or \ for Windows), and you must be able to write to the directory. If you enter an invalid path or a protected directory, SQL*Plus exits.

   The path length is limited by SQL*Plus and the operating system.

   This script spools the **mdl_pri.txt** report to the Audits subdirectory, located in the SQL upgrade directory. The **mdl_pri.txt** report lists differences between your database and the data model. This report verifies the database structure by identifying missing tables or columns, extra tables or columns, and differences with column data types. Some differences listed will be commented if added in an MSS maintenance release. If you have any differences listed that are not commented, contact Oracle Global Customer Support before you proceed.

4. Run the **_upgmss.sql** script.

   a. Enter the operating system (either UNIX or Windows) for the SQL*Plus client.

   > **Note:**
   >
   > If you are using a Linux operating system, enter UNIX.

   b. Enter the full directory path for the SQL script files.

   The path must include the trailing virgule (/ for UNIX and Linux or \ for Windows), and you must be able to write to the directory. If you enter an invalid path or a protected directory, SQL*Plus exits.

   The path length is limited by SQL*Plus and the operating system.

   c. If this is your first time to run the upgrade script, select upgrade mode **1**.

   > **Note:**
   >
   > If your upgrade fails before you reach the message MAIN UPGRADE IS ABOUT TO BEGIN, fix the problem and rerun the upgrade in mode 1. If your upgrade fails after the main upgrade has started, fix the problem and rerun the upgrade in mode 3.

   Table 2-3 describes the upgrade modes.

Table 2-3   Upgrade Modes

Upgrade Modes	Description
Setup and run immediately	Upgrade mode 1 is the default setting and sets up the required framework of upgrade related tables, procedures, and data. Any framework-related objects from a previous upgrade, including the audit tables, are dropped and re-created. The upgrade continues immediately after setup.
Setup upgrade framework only	Upgrade mode 2 only sets up required upgrade framework objects; the upgrade does not continue after setup. This mode allows you to make custom changes to the upgrade process. For example, you might have a weekly scheduled job that performs the Oracle Analyze Statistics command. If so, you can set the override option for the Omega-Analyze Statistics process that does the same thing.
Already setup, just run it	Use upgrade mode 3 after you run the first or second upgrade mode, and when any of the following apply: • You are ready to continue with the upgrade. • The upgrade exited SQL*Plus during part of the DDL upgrade. • There were conversion errors.

After correcting any problems, use upgrade mode 3 to restart the upgrade without losing any override options.

d. Enter the database name.

This step does not occur in upgrade mode 3.

e. Enter the passwords for ASAP, EBOND, JOB, EDI, and SYS.

All passwords are verified. If a password fails, SQL*Plus exits.

This step does not occur in upgrade mode 3.

f. Choose one of the following storage options:

• If you want the tables that are dropped and recreated to be recreated with their current storage parameters, set the storage option to **2**. The upgrade takes into account the tablespace in which the tables are currently stored.

• If you choose not to use the tables' current storage parameters, select storage option **1**. The tables are recreated using the default values in the **ddlasap.sql** file.

The screen scrolls data as the upgrade script sets up the required framework of upgrade related tables, procedures, and data. The message MAIN UPGRADE IS ABOUT TO BEGIN displays in SQL*Plus, indicating the main upgrade.

> **✎ Note:**
>
> If for some reason, you must restart the upgrade after you reach this point, use upgrade mode 3.

The **_upgmss.sql** script is the master script for the upgrade process and calls the main process group scripts. Before the upgrade process begins, an on-screen

report appears, indicating the database is in restricted mode access and listing any users already connected. Only the DBA should be connected during the upgrade process. If other users are connected, you can start another SQL*Plus session to remove the user connections and return to this session to continue with the upgrade process.

If SQL*Plus exits, search the files in the Audits subdirectory for the string "ORA-". If you find any ORA messages, contact Oracle Global Customer Support and e-mail the **ddlerrs.txt** log in the Audits subdirectory.

If the upgrade is successful, the following message appears:

```
Upgrade Process Finished.
Please review the \audits\upgchk.txt report.
The report will show processes that passed and/or failed.
The \audits\*.log files should also be searched for 'ora-'
messages which will require further review by the DBA.
Don't forget to run the mdl_cur.sql script to produce an mdl_cur.txt report file
to verify table structures.
```

If the upgrade is not successful, the following message appears:

```
****** Upgrade PROBLEMS ******
Please review the \audits\upgchk.txt report.
The report will show processes that passed and/or failed.
The \audits\*.log files should also be searched for 'ora-'
messages which will require further review by the DBA.
After addressing any issues, restart the upgrade
and use OPTION MODE 3.
```

5. Review the **upgchk.txt** log in your Audits subdirectory to determine any processes that failed, then review the specific audit report to determine what caused the process to fail.

   Perform this task even if the upgrade was successful. The **upgchk.txt** log contains several views that provide information on the upgrade:

   - **Process Hierarchy:** Lists the upgrade hierarchy table, which enforces parent/child relationships. The upgrade framework uses this table when determining if parent or child processes performed successfully. The **process_nbr** field contains the unique identifier ID for the process that is referenced within the audit tables.

   - **Processes USER Marked as "OVERRIDE":** Lists processes that were overridden. If **upg_ovex.sql** is used to set the override option for any processes, the audits indicate that these processes passed even though they did not run.

   - **Grouping Type Processes That Passed:** Lists the major process groups within the upgrade that passed. If a group of processes has a controlling parent process, that parent process is listed along with duration statistics.

     If the filename _**upgmss.sql** does not appear in this list, the upgrade did not complete successfully.

   - **Non-Grouping Type Processes That Passed:** Lists the processes within the upgrade that passed. The filename of each successful process is listed, along with duration statistics.

   - **Processes That Did Not Complete:** If the _**upgmss.sql** filename was not present in the list of grouping processes that passed, this view lists all processes that ran and failed, or that did not run. Typically, when a process

fails, there are other processes that depend on its success and which do not run. Because of this, this view can list multiple processes that did not run because an earlier process failed.

If this view contains any processes, look at the *Suspect Processes That Did Not Complete* view.

- **Suspect Processes That Did Not Complete and May Have Cascaded the Other Processes to Fail:** Lists likely suspect processes. Use this view in conjunction with the Processes That Did Not Complete view to locate the processes that failed. This view is only a starting point and might not be completely accurate because of the complexity of the process dependencies in the upgrade framework.

  If this view contains any processes, contact Oracle Global Customer Support and e-mail the **upgchk.txt** log and all audits in the *Suspect Processes that Did Not Complete* view.

- **Before/After Record Counts for Processes**: Lists any tables along with record counts affected during conversions. The view groups the information by process name, listing each table affected by that process, along with the before and after record counts.

6. Search the files in the **Audits** subdirectory for ORA messages using the string "**ORA-**".

   The **Audits** subdirectory is located in the **SQL upgrade** directory. The following ORA messages are noncritical because they do not cause upgrade failure.

   - **Name is already used by an existing object**: This occurs when you try to assign a name that has already been assigned to a new object. These messages are written to **master_p.log**.

   - **Cannot drop constraint - nonexistent constraint**: This occurs when you try to drop a constraint that does not exist or has already been dropped. These messages are written to **ddlcmp.log.**

   - **Table or view does not exist**: This occurs when you try to drop a table or view that does not exist or has already been dropped. This message can be important in other contexts and can appear in any log file in the **Audits** subdirectory.

   - **Such a referential constraint already exists in the table**: This occurs when you try to add a foreign key constraint that already exists. The message can appear in any log file in the Audits subdirectory.

   - **Integrity constraint violated - child record found**: This occurs when base data that is in use is not deleted. These messages show up in the **static_r.log.**

   - **Success with compilation error**: This occurs when there is an error compiling an object. These messages are written to **o_recmpl.log.**

   If you find ORA messages that are not on the list, contact Oracle Global Customer Support.

7. Run the **mdl_cur.sql** script.

   The **mdl_cur.sql** script spools the **mdl_cur.txt** report to the Audits subdirectory. This view verifies the database structure by identifying missing tables or columns, extra tables or columns, and differences with column data types as compared to the data model.

8. Run the **mdl_cmp.sql** script.

   This script spools a report that indicates extra or missing indexes, primary keys, foreign keys, and sequences. This script gives the option to fix problems or only report the differences. When you run the script, you can compare the differences for individual sections or for all sections. The default is to compare all sections. For any missing information in **mdl_cmp.txt**, such as missing objects, run the **mdl_cmp.sql** script again in fix mode. Then run it again in report mode to verify that any problems were fixed.

9. (Optional) Run the SQL scripts in the **postcheck** folder.

   These scripts generate information on the data that was converted during the upgrade.

10. Exit SQL*Plus.

11. Install the current MSS database, using the scripts extracted from the **MSS.R6_3_0.b***xxx*_**DBInstall.zip** file.

   For complete instructions on installing the current MSS database, refer to the following sections, in "Upgrading Oracle Communications MetaSolv Solution" of this guide:

   • Upgrading Oracle Communications MetaSolv Solution

   • Updating Stored Procedures

   • Running Reports

You can review the following files for additional errors:

• **o_cfgrpt.txt**: Consists of objects currently being stored with storage settings below minimum standards or indicates if the index is not on the Indexes tablespace.

• This report is generated in the **Audits** subdirectory by the **o_config.sql** script and contains a list of tables and indexes having more than 100 extents allocated to them. These items are good candidates to be rebuilt (if indexes).

• **o_cfggen.sql**: Consists of a series of SQL statements that contain a list of stored objects with storage settings below minimum standards, or indicates if the index is not on the indexes tablespace. SQL code is used to correct the storage settings.

• **o_glocon.log**: Consists of a list of records in the foreign key exceptions section, where at least one constraint could not be enabled. All data issues must be corrected before you can enable the constraint. Run the **mdl_excp.sql** script to view a list of records containing constraint problems. Also, run the **mdl_cmp.sql** script to enable the foreign keys. If there are no records listed in this report, all constraints were enabled.

> **✎ Note:**
>
> If you do not find any ORA-messages in any of the audit files, the upgrade completed successfully.

Dropping the appdata Tablespace

If you are moving from a pre-6.0 version of MSS to MSS 6.3.*x*, you might have the **appdata** tablespace present in your database. If so, you must delete it. It was present in MSS 5.2.*X* and was deleted in the MSS 6.0 version.

To drop the tablespace

1. Start SQL*Plus.

2. Enter the following command at the prompt:

   ```
   drop tablespace appdata including contents;
   ```

3. Delete the data file from the operating system.

Database Post-Installation Tasks

You must complete the following tasks to ensure that the database operates properly:

- Load a set of graphics to the database

- Check the database using the Oracle Communications MetaSolv Solution feature called DB Health.

- Unlock the users that are locked during upgrade by running the following command:

  ```
  ALTER USER <username> ACCOUNT UNLOCK;
  ALTER USER <username> IDENTIFIED BY <password>;
  ```

- Change the role passwords.

  Only the database administrator can change passwords for the roles ADMIN_ROLE and WOTSTWTWWOO by running the following stored procedure:

  ```
  ===========pl/sql should be run by dba for changing role's password==========
  DECLARE
    C_NAME VARCHAR2(200);
    C_PASSWORD VARCHAR2(200);
  BEGIN
    C_NAME := 'role_name'; /*specify the role name, ADMIN_ROLE OR WOTSTWTWWOO*/
    C_PASSWORD := 'password'; /*specify the password*/
    SP_CREDSTORE_CHG_ROLE_PWD(C_NAME, C_PASSWORD);
  END;
  ```

  If you do not change the role passwords, then the following error message is displayed:

  ```
  ORA-01979: missing or invalid password for role WOTSTWTWWOO or ADMIN_ROLE
  ```

  See "Troubleshooting Database Issues" for more information.

Ensure that you have installed the appropriate files on the client workstation to successfully complete the database post-installation tasks. See "Performing Post-Installation Tasks" for information.

3

Preparing For the Application Server Installation

This chapter explains the tasks that you must do before installing the Oracle Communications MetaSolv Solution (MSS) application server.

About Required Software Installation

MSS requires Oracle database software and Oracle WebLogic application server software. This document does not explain how to install the software for either of these products. Setting Up The MSS Database describes how to install or upgrade your Oracle database. Table 3-1 shows where to find information for configuring Oracle WebLogic application server for MSS.

Table 3-1   Required Software Information

If you are setting up:	Find information on how to do it here:
An application server for MSS with Web Services.	In this guide: "Installing and Deploying MetaSolv Solution on a Single Server " or "Installing and Deploying MetaSolv Solution on a Clustered Server"

Oracle WebLogic Software Installation on an MSS Host Machine

Figure 3-1 shows the steps involved in installing Oracle WebLogic software on a machine that will host MSS. The figure describes step 3B in Figure 1-1.

See "Software Requirements" for information on required software versions.

Figure 3-1   Installing Oracle WebLogic Software on an Application Server Machine
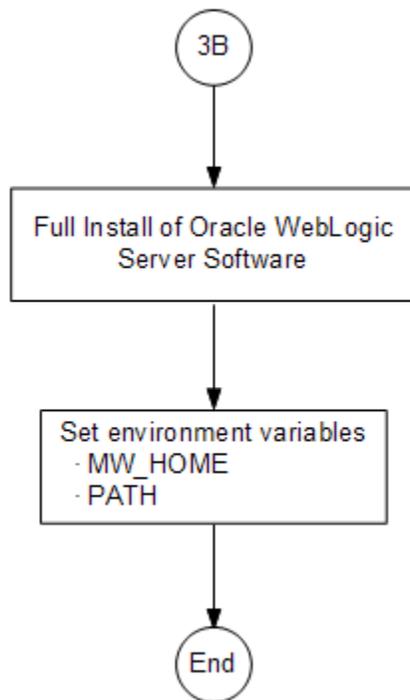
About the Oracle WebLogic Installation

This document does not explain how to install the Oracle WebLogic software, but it does provide basic information on how to set up and configure the Oracle WebLogic domain for MSS.

Where to Find Oracle WebLogic Server Software

You can find Oracle WebLogic software in the following location:

- If you purchased Oracle WebLogic software as part of or separately from MSS, you can find the WebLogic Server software in the Oracle Communications MetaSolv Solution software on the Oracle software delivery website.

Installation Notes

- If you are installing on a UNIX/Linux platform, you can run an X-Windows emulator like Hummingbird Exceed. The installer defaults to console mode if no X-Windows connection is made.

- Install Oracle WebLogic Server on every machine that has either the WebLogic administration server, a clustered server, or a single server hosting the MSS application.

    For information about installing Oracle WebLogic Server, see the Oracle WebLogic Server documentation.

Setting the MW_HOME Environment Variable

Once you have installed WebLogic Server on a machine, add the environment variable for MW_HOME that points to the WebLogic directory.

For example:

For UNIX/Linux:

```
MW_HOME=/Oracle/Middleware/Oracle_Home
```

For Windows:

```
MW_HOME=C:\Oracle\Middleware\Oracle_Home
```

This step is not optional and you must set the environment variable `MW_HOME` before the installation process of MSS.

Installing WebLogic Patches

After you install WebLogic Server, you must download any required patches from the My Oracle Support website and apply patches using the WebLogic Opatch tool.

For information about downloading and applying private patches, see *Knowledge Article 1302053.1 - Master Note: How to Locate and Download Patches for WebLogic Server Using My Oracle Support* and *Knowledge Article 1075833.1 - Master Note on WebLogic Server (WLS) Patches, Upgrade Installers, and Full Installers*.

Using the IBM AIX Operating System

MSS is certified to run on AIX 7.1. The Oracle JDK download page includes JDK 8 for Windows, HP, and Sun operating systems. JDK 8 for AIX is not provided by Oracle. If you have an AIX operating system, you must download the AIX JDK from the IBM website and install it in the following location:

/usr/java18

For information on the AIX JDK, see the following website:

http://www.ibm.com/us

About JacORB

JacORB is installed automatically during the MSS installation. Do *not* install JacORB manually.

How the Installer Works

You must download the installer with the following filename:

MSS.RreleaseNumber**.b**build_**AppServerInstaller.jar**

where *releaseNumber* is the MSS software release version and *build* is the build number. You find this on the Oracle software delivery website, then copy or FTP the

installer into a temporary directory on each machine on which you intend to install MSS.

Two options are available in the installer:

- **Full installation**: Select this option for new installations of any 6.3.*x* release. This option is also used when upgrading to 6.3.*x* from a pre-6.3 release.

- **Upgrade installation**: Select this option for subsequent MSS 6.3.*x* maintenance releases and patches.

The installer is delivered in a jar file. You only have to run the installer on each physical machine in a domain one time, regardless of the number of Oracle WebLogic application server instances and/or clusters running on the machine. The following actions are automated by the installer:

- **Parameter configuration**: Default parameters are entered for logging, threads, JDBC pool creation and sizing, reload, JMS/Bridge, memory GC, and SSL.

- **Deployment**: You can deploy to both clustered and non-clustered configurations from the installer.

The program validates the database connection and creates custom scripts for starting JacORB and WebLogic application server.

Directory Structure

MSS requires each server directory and its WebLogic domain directory to be placed in the *MSLV_Home* directory. This directory is a location on the server under which the MSS software will be installed.

In the example shown in Figure 3-2, the following structure exists:

- MetaSolv home (*MSLV_Home*) directory: **/opt/m63Single/single**

- Server directory: **/opt/m63Single/single/mslv01**

- Server domain directory: **/opt/m63Single/single/m63domain**

Figure 3-2 shows an example of a typical MSS directory structure.

Figure 3-2   Example of an MSS Directory Structure
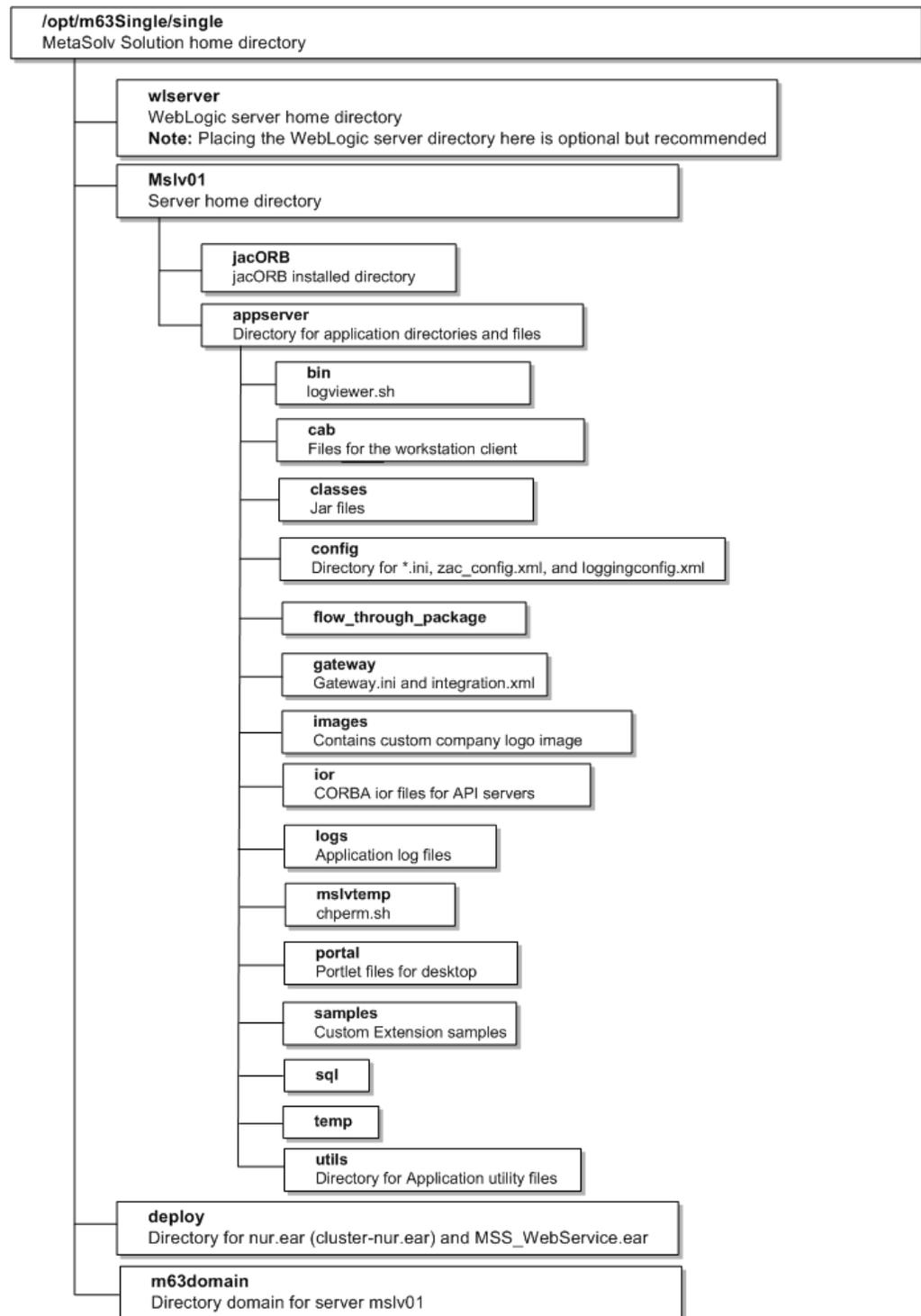
In the example shown in the figure, the following structure exists:

- MetaSolv home directory: **/opt/m63Single/single.**

- Server directory: **mslv01**. The directory is located in **/opt/m63Single/single**.

- Server domain directory: *m63domain*. The directory is located in **/opt/m63Single/single**.

Using Worksheets to Plan Your Installation

Before you begin to install MSS, it is prudent to plan the installation on paper. This is important if you have a number of machines on which to install. In this case, the assignment of names, port numbers, and other information is critical so that contention issues do not arise when you try to run the system for the first time.

The WebLogic application server domain that you plan to create dictates how you install MSS and what information you need to know beforehand. A sample worksheet is provided in Appendix C to help you plan out the information required at installation time. The worksheet indicates the information you need to create the Oracle WLS domain and provide examples of the expected values. Included in the worksheet is:

- Common installation information
- Single server environment information
- Clustered server environment information

Pre-requisites for the Latest MSS Release

The following are the pre-requisites for the latest MSS release. See "Software Requirements" for information on the required software versions.

- Upgrade to the current version of the MSS database.
- Install Oracle WebLogic software for the environment you need for MSS.
- Do not need to install the Oracle client on the server machine. The Oracle thin client for these versions is supplied through Oracle. The API startup detects the database information from the WebLogic server connection pool. This removes the need to store any of the database information in non-Oracle configuration files. It also prevents the API connections from being configured to connect to a different database.
- Resolve the DNS name of the database host machine. This means you must be able to ping the database server. If you cannot, add the IP address and host machine's name to the /etc/hosts file.
- Make sure the database users APP_MSLV, APP_API, and APP_INT exist. If they do not exist, ask your database administrator to create them before you proceed. These users should have been created during the database installation.
- Read the section entitled "Pre-installation Checklist".
- Make sure the user executing the installer has write permissions in the MetaSolv home directory and WebLogic home directory of the machine on which the installation is performed.
- After installing Oracle WebLogic on all target application server machines, verify that the `PATH` environment variable is set with the JDK directory defined as the first entry. See the following example:

```
PATH=/opt/jdkVersion/bin:$PATH; export PATH
```

where *Version* is the version portion of the JDK path. Run the command

```
java -version
```

to verify that you have the correct version of the Java in the `PATH`.

- Download the MSS release files from the Oracle software delivery website to an application server. Download the following files for the appropriate platform: Oracle WebLogic files (if you purchased them as part of MSS) and

  MSS.R_releaseNumber_**.b**_build__**AppServerInstaller.jar**

  where _releaseNumber_ is the MSS software release version and _build_ is the build number.

- Make sure the person installing has execute rights on the application server installation file. If you are using UNIX/Linux, use the `chmod` command to change permissions if this is necessary.

- If you are a UNIX/Linux user using an X-Windows emulator, set the `DISPLAY` environment variable to send the graphical display to your workstation by typing the following:

  `$DISPLAY=mymachinename:0.0;export DISPLAY` and pressing ENTER.

- Verify the _MW_Home_ environment variables have been set. The following is an example entry in a **.profile** file for UNIX/Linux users:

  ```
  MW_HOME=/opt/Oracle/Middleware/Oracle_Home; export MW_HOME
  ```

4

Installing and Deploying MetaSolv Solution on a Single Server

This chapter describes how to perform a full installation of the Oracle Communications MetaSolv Solution (MSS) release and explains how to set up the MSS application server for a single server installation. This chapter covers the Oracle WebLogic server domain configuration, including the installation and deployment of the MSS application server.

About Single Server Installation

A single server installation is one in which a single WebLogic server instance hosts the MSS application server process.

This section describes how to:

- Create a WebLogic domain for a single server.
- Install the MSS application server software.
- Deploy MSS to the single server.

Figure 4-1 shows the basic steps for installing MSS on a single server. The figure is an expansion of step 5 of the basic installation process shown in Figure 1-1.

Figure 4-1   Single Server Installation
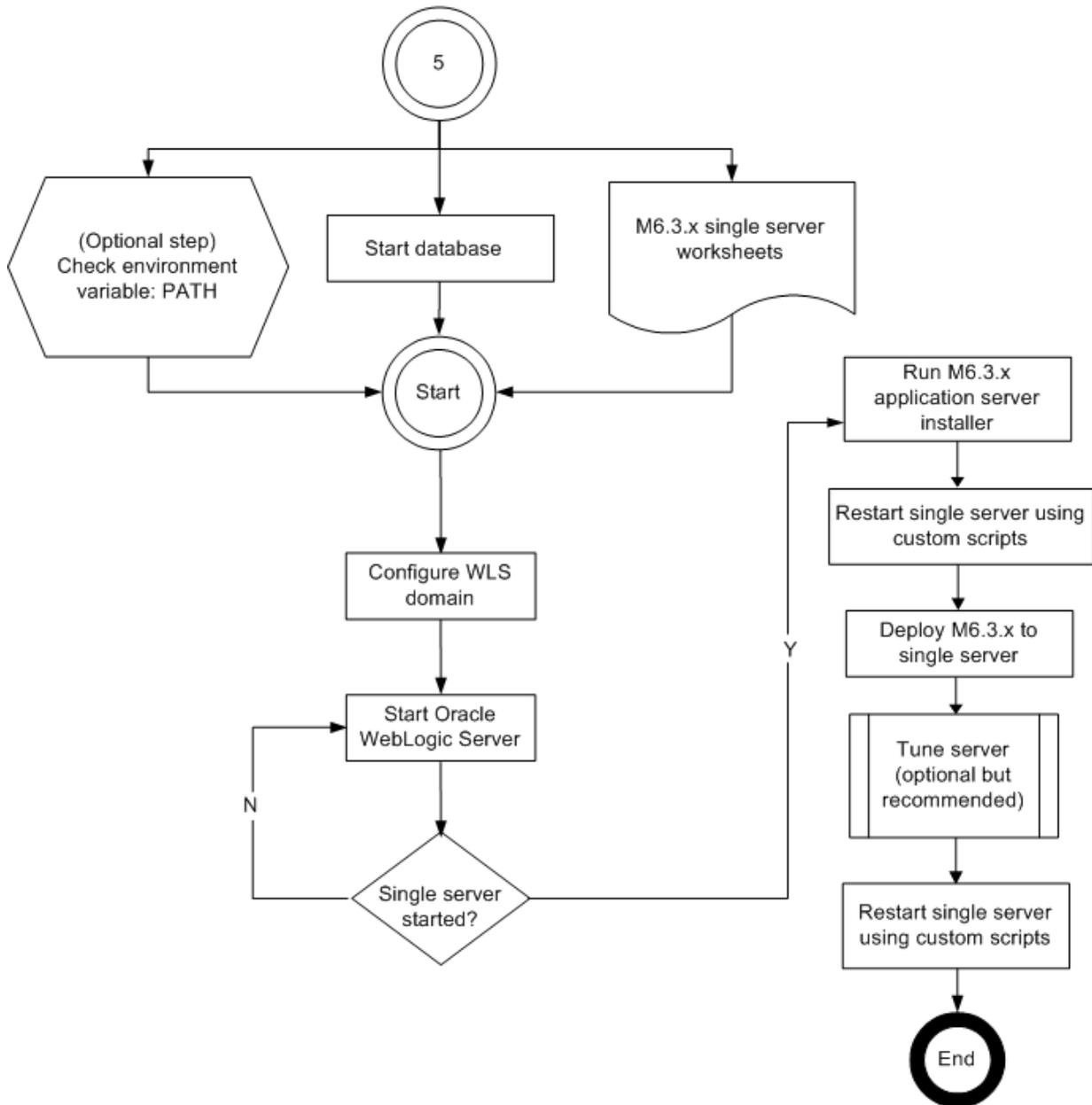
Before You Start

- Print and complete the following planning worksheets:

    – Application server common installation worksheet. See Table C-1.

    – Single server installation worksheet. See Table C-2.

    – Some steps in the procedures for the WebLogic domain configuration and the MSS installation refer to the worksheets. Each value that you are asked to enter has a worksheet reference number.

- Review "Pre-requisites for the Latest MSS Release" and make sure all tasks listed that apply to your installation are completed.

Creating a Single Server WebLogic Domain

To create a single server domain, perform the following:

1. From the Administration Server, start the Fusion Middleware Configuration Wizard by doing one of the following:

   - For UNIX/Linux platforms, this program (**config.sh**) is located in the following directory: *MW_HOME***/oracle_common/common/bin**.

   - For Windows platforms, this program (**config.cmd**) is located in the following directory: *MW_HOME***\oracle_common\common\bin**.

   The Configuration Type window appears.

2. Select **Create a new domain** and in the **Domain location** field, enter the full path for the domain or click **Browse** to navigate to the domain home directory (for example, /opt/m63Single/single/*m63domain*/), and then click **Next**.

   The Templates window appears.

3. Select the **Create Domain Using Product Templates** option and then the appropriate items from the provided list. You must select **WebLogic Advanced Web Services for JAX-WS Extension**, and the **WebLogic JAX-WS SOAP/JMS Extension** is optional depending on your requirements.

   - **WebLogic Advanced Web Services for JAX-WS Extension -** *Version* **[oracle_common]** - You must select this JAX-WS template for MSS Web Services as it is mandatory during the creation of an MSS domain.

   - **WebLogic JAX-WS SOAP/JMS Extension -** *Version* **[oracle_common]** - You select this template for SOAP over JMS Web Services or if you built custom web services that are SOAP over JMS.

   where *Version* is the Oracle WebLogic version.

   See "Software Requirements" for information on required WebLogic software version.

   See *Oracle Fusion Middleware Domain Template Reference* for more information on WebLogic templates.

4. Click **Next**.

   The Administrator Account window appears.

5. Enter a user name and password and verify the password by retyping, then click **Next**.

   Worksheet references and example values:

Field name	Worksheet reference number	Example value
User name	COMM-0020	weblogic
User password	COMM-0030	*password*

   You need to make a note of the user name and password. You need them for the administration console login.

   The Domain Mode and JDK window appears.

6. Do one of the following:

   - If you are installing for company operations, select the **Production Mode**.

   - If you are installing to do integration development or testing, select **Development Mode**.

7. Select the **Other JDK Location** option, browse to the location of another JDK, select the JDK version, and then click **Next**. See "Software Requirements" for the information on the required software versions.

   The **Other JDK Location** option is supported for both UNIX/Linux and Windows platforms.

   The Advanced Configuration window appears.

8. Select **Administration Server** and click **Next**.

   The Administration Server window appears.

9. Do the following:

   a. In the **Server Name** field, enter the Administration Server name.

      This single server serves as the MSS domain Administration Server.

   b. In the **Listen Address** field, select a DNS or an IP address.

      If you are creating an IPv6 domain, you must specify the IPv6 address in the **Listen Address** field.

      (Optional) If your firewall configuration does not support IPv6 addresses, you must enable HTTP tunneling in the WebLogic Server Administration Console. See "Enabling HTTP Tunneling" for more information.

   c. In the **Listen Port** field, accept the default.

   d. Select the **Enable SSL** check box if you want to enable SSL.

      It is not a requirement to either enable or disable SSL.

      If you decide to enable SSL, ensure that you configure SSL for WebLogic Server. See "Configuring SSL for WebLogic Server" for more information.

   e. In the **SSL Listen Port** field, enter a port that is not used by another domain.

      This field is enabled only if you selected the **Enable SSL** check box.

      Worksheet references and example values:

Field name	Worksheet reference number	Example value
Name	Single-0150	mslv01
Listen address	Single-0160	srvrchosa1
Listen port	Single-0170	7001
SSL Listen port **Note:** If using SSL, use this parameter.	Single-0180	7002

10. Click **Next**.

    The Configuration Summary window appears.

11. Review the summary to verify the contents of your domain and click **Create** to create the domain.

    The Configuration Progress screen appears, which displays the progress of the domain creation process.

12. After the progress indicator shows the percentage completion of the process as 100%, click **Next**.

    The Configuration Success screen appears.

13. Click **Finish**.

14. To verify the domain setup, start the server by completing the following steps:

    a. Run **startWebLogic.sh** (UNIX/Linux) or **startWebLogic.cmd** (Windows) in the domain directory.

       The domain directory is the name you specified during configuration.

       For example: /opt/m63Single/single/*m63domain*

    b. Type your administrator user name and password, when prompted, to start the server.

       The server takes a few moments to start. You will see information scroll on the screen. When the server has successfully started, you will see the words RUNNING mode at the prompt.

Configuring SSL for WebLogic Server

For information about public and private keys, about identity and trust keystores, and how to create and configure them in the WebLogic Administration Console, see the *Fusion Middleware Administering Security for Oracle WebLogic Server*.

To configure SSL for WebLogic Server:

1. Log in to the Oracle WebLogic Server Administration Console.

2. In the **Domain Structure** tree, expand **Environment**, and then click **Servers**.

   The Summary of Servers screen appears.

3. Click the **AdminServer** link.

   The Settings for AdminServer screen appears.

4. Click the **Configuration** tab, and then click the **Keystores** tab.

5. From the **Keystores** list, select **Custom Identity and Custom Trust**.

6. Do the following:

   • Under the Identity section, do the following:

     a. In the **Custom Identity Keystore** field, enter the full path for the identity keystore. For example, /opt/stores/identity.jks.

     b. In the **Custom Identity Keystore Type** field, enter the type of the keystore. Typically, this attribute is Java KeyStore (JKS); if you leave this field blank, it defaults to jks.

     c. In the **Custom Identity Keystore Passphrase** field, enter the password you will enter when reading or writing to the keystore.

     d. In the **Confirm Custom Identity Keystore Passphrase** field, enter the password again.

- Under the Trust section, do the following:

     a. In the **Custom Trust Keystore** field, enter the full path for the trust keystore. For example, /opt/stores/trust.jks

     b. In the **Custom Trust Keystore Type** field, enter the type of the keystore. Typically, this attribute is JKS; if you leave this field blank, it defaults to jks.

     c. In the **Custom Trust Keystore Passphrase** field, enter the password you will enter when reading or writing to the keystore.

     d. In the **Confirm Custom Trust Keystore Passphrase** field, enter the password again.

7. Click **Save**.

8. Click the **SSL** tab and do the following:

- Under the Identity section, do the following:

     a. In the **Private Key Alias** field, enter the private key for WebLogic Server from the keystore. For example, mycert.

     b. In the **Private Key Passphrase** field, enter the password you specified when loading the private key for WebLogic Server into the keystore.

     c. In the **Confirm Private Key Passphrase** field, enter the password again.

- Under the Trust section, under Advanced, from the **Hostname Verification** list, select **None**.

9. Click **Save**.

> **Note:**
>
> Before you install MetaSolv Solution in an IPv6 domain, ensure that your firewall configuration supports IPv6 addresses. If your firewall configuration does not support IPv6 addresses, you must enable HTTP tunneling in the WebLogic Server Administration Console. See "Enabling HTTP Tunneling" for more information.

10. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

11. Open the *MSLV_Home\m63domain***config\config.xml** file and add the following cipher suite entry for the SSL server:

```
<server>
    <name>SSLAdminServer</name>
    <ssl>
        <name>SSLAdminServer</name>
        <enabled>true</enabled>
        <ciphersuite>TLS_RSA_WITH_AES_128_CBC_SHA</ciphersuite>
        .
        .
        .
    </ssl>
```

12. (Optional) After updating the demo certificate to custom certificate, if the managed server that you are starting still points to the demo certificate, update the **startMSLVManaged.sh** or **startMSLVmanaged.cmd** file to include the following Java options:

```
set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dweblogic.security.SSL.trustedCAKeyStore=/opt/stores/trust.jks
set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dweblogic.security.SSL.ignoreHostNameVerification=true
```

If you observe similar issues on the proxy server, update the **startProxyServer.sh** or **startProxyServer.cmd** startup script file to include the same Java options mentioned in the preceding paragraph.

13. To call MSS Web services using the HTTPS port in an SSL environment (where the HTTP port is disabled), do the following:

    a. Log in to the Oracle WebLogic Server Administration Console.

    b. On the Home page, under Domain Configurations, click the **Domain** link.

    c. Click the **Configuration** tab, and then click the **JTA** subtab.

    d. Click **Advanced** to display advanced configuration options.

    e. From the **Web Service Transactions Transport Security Mode** list, select **SSL Required**.

    f. Click **Save**.

    g. Click **Activate Changes**.

       You can now call MSS Web services using the HTTPS port:

       ```
       https://hostname:https_port/MssWS/customer/CustomerAccount?WSDL
       ```

Installing the Self-Signed Certificate on the Client Machine

To install the self-signed certificate on the client machine:

1. Open Internet Explorer and enter the following URL:

   ```
   https://hostAddress:port/main/pblistener
   ```

   A security warning message appears.

2. Click **Continue to this website**.

3. Click the certificate errors in red.

4. Click **View Certificates**.

5. Click **Install Certificate**.

   The Certificate Import Wizard appears.

6. Select the **Place all certificates in the following store** option.

7. Click **Browse** beside the **Certificate Store:** field.

   The Select Certificate Store window appears.

8. Select **Trusted Root Certification Authorities** and click **OK**.

9. Complete the installation of the certificate.

10. Close all instances of Internet Explorer and start the MSS client.

Installing and Deploying MSS

This section explains how to install and deploy MSS.

Prerequisites

- The instructions for creating the domain configuration included starting the server after the configuration was complete. Leave the server running until you are instructed to shut it down.

- Ensure that the following environmental variables are set:

```
JAVA_HOME=/opt/jdkVersion
PATH=JAVA_HOME/jdkVersion/bin;$PATH
MW_HOME=/opt/Oracle/Middleware/Oracle_Home
```

where *Version* is the JDK software version. To install and deploy MSS, do the following:

1. From directory where the file was downloaded, enter the following command:

   ```
   java -jar MSS.RreleaseNumber.bbuild_AppServerInstaller.jar
   ```

   where *releaseNumber* is the MSS software release version and *build* is the build number. For example:

   ```
   java -jar MSS.R6_3.b400_AppServerInstaller.jar
   ```

   > **Note:**
   >
   > For 64-bit systems, use the following java_options parameter: **-d64**.

   The Select MetaSolv home directory window appears.

2. From the **Look In** list, click the down arrow and select a directory in which the installer files can be stored and used during the installation process, then click Select.

   A directory named **installer** is automatically created in the selected directory. Oracle recommends choosing your *MSLV_Home* directory for this task.

   The installer auto-launches the installation process by invoking **setup.sh** (UNIX/ Linux) or **setup.cmd** (Windows) in the *MSLV_Home***/installer** directory.

   Worksheet references and example values:

Field name	Worksheet reference number	Example value
File Name (*MSLV_Home*)	COMM-0090	/opt/m63Single/single

   The Oracle Communications MetaSolv Solution Installation window appears.

3. Click **Next**.

The Oracle Communications MetaSolv Solution Installation - Choose Install Type window appears.

4. Select **Full Installation on WebLogic Server with JAX-WS Domain** and click **Next**.

The Oracle Communications MetaSolv Solution Installation - Full Select Server window appears.

5. Do the following:

   a. In the **Admin Host** field, enter the host name or the IP address of the administration server.

   If you are creating an IPv6 domain, you must specify the IPv6 address in the **Admin Host** field.

   (Optional) If you are creating the cluster in an IPv6 domain in a dual-stack machine, ensure that you specify the IPv6 address and the system name in the **etc/hosts** file, as follows:

   ```
   IPv6address          ipv6machine@example.com        ipv6machine
   ```

   > **Note:**
   >
   > The MetaSolv Solution installer does not support the use of virtual IP address during installation. If you specify a virtual IP address during installation, the installer does not display the following:
   >
   > • The check box to select the server you want MSS installed on.
   >
   > • The following configuration tabs:
   >
   > Directory
   >
   > Oracle Database
   >
   > Oracle RAC
   >
   > Gateway
   >
   > Port
   >
   > Proxy
   >
   > If your configuration requires the use of virtual IP address, you must specify the physical IP address during installation. After the installation is complete, you can change the server's listen address to the virtual IP address, and then restart the WebLogic server. See "Changing an IP Address" for more information.

   b. In the **Port#** field, enter the port number of the administration server.

   c. In the **User ID** field, enter the user name for the administration server.

   d. In the **Pass** field, enter the password for the administration server.

   Worksheet references and example values:

Field name	Worksheet reference number	Example value
Admin Host	Admin-0250	srvrchscal

Field name	Worksheet reference number	Example value
Port#	Admin-0260, Admin-0270	7001 (HTTP port), 7002 (HTTPS port)
User ID	COMM-0020	weblogic
Pass	COMM-0030	*password*

e. (Optional) If you want to install and deploy MSS using the SSL port, leave the **Connect to WebLogic using SSL** check box selected (which the installer selects by default).

See the Oracle WebLogic Server documentation for information about configuring keystores.

f. In the **Key Store Location** field, enter the path for the keystore or click **Browse** to navigate to the keystore location. The keystore should be referred to in the **trust.jks** file.

6. Click **GO**.

The installer queries the Admin Host machine and returns with values you entered during the configuration of the WebLogic domain. This process can take a few moments.

If the domain does not have a JAX-WS template applied, then the following message is displayed:

```
Please update the domain with the required JAX-WS Extension template and restart
the installation.
```

Please exit the installer and upgrade the domain by applying the **WebLogic Advanced Web Services for JAX-WS Extension** template and optionally the **WebLogic JAX-WS SOAP/JMS Extension** template. Retry the installation again after selecting the appropriate template(s):

• WebLogic Advanced Web Services for JAX-WS Extension Template (Required)

• WebLogic JAX-WS SOAP/JMS Extension Template (Optional)

The Oracle Communications MetaSolv Solution Installation window appears with the domain and any servers in the domain appearing in the left pane.

7. In the tree view on the left, select the check box next to the single server you want MSS installed on.

Tabs appear in the right pane for information to be entered for the selected server.

Figure 4-2   View to Select the Server for Single Server Installation
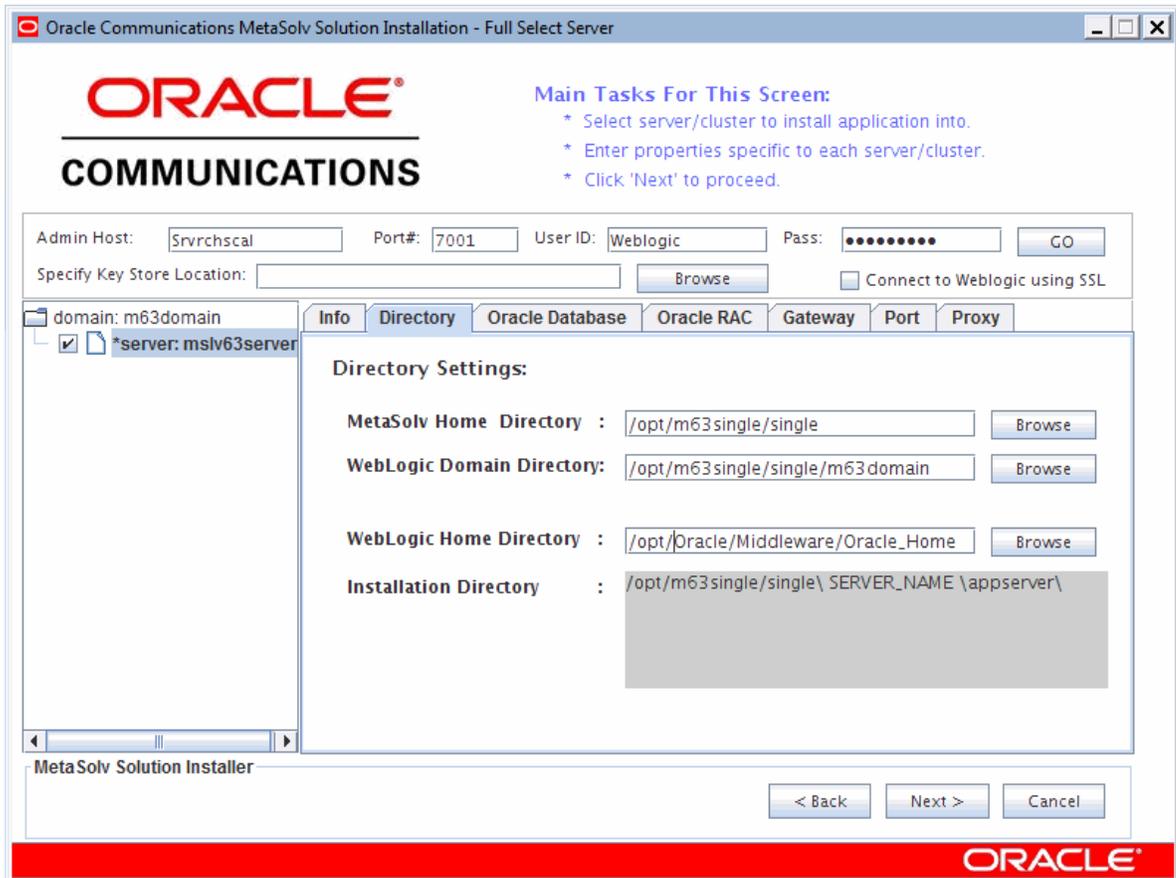
8. Complete domain information by selecting and completing the following tabs:

    a. Click the **Directory** tab and enter the path and name of the MetaSolv home directory, WebLogic domain directory, and WebLogic Home directory or click **Browse** to search for the directories.

    Worksheet references and example values:

Field name	Worksheet reference number	Example value
MetaSolv Home Directory	COMM-0090	/opt/m63Single/single
WebLogic Domain Directory	COMM-0110	/opt/m63Single/single/*m63domain*

    b. Depending on your database configuration, do one of the following (Option 1 or Option 2):

    Option 1:

    Click the **Oracle Database** tab and do one of the following:

    In the **Oracle Server Name**, **Oracle Port#**, and **Oracle Service Name** fields, enter the relevant values, and select the **Pluggable DB** check box if you are running the MSS database instance as a pluggable database (PDB).

    OR

In the **JDBC URL** field, enter your own free-form JDBC connect string.

Example of a JDBC URL string:

```
jdbc:oracle:thin:@srvrchscal2:1521:BEN6
```

Example of a JDBC URL string for a pluggable database:

```
jdbc:oracle:thin:@srvrchscal2:1521/BEN6
```

Worksheet references and examples values:

Field name	Worksheet reference number	Example value
Oracle Database Server Name	COMM-0130	srvrchscal2
Oracle Database Port	COMM-0140	1521
Oracle Database Service Name	COMM- 0150	BEN6
APP_MSLV Password	COMM-0040	mss6mslv
APP_API Password	COMM-0050	mss6api
APP_INT Password	COMM-0055	mss6int

Option 2:

Click the **Oracle RAC** tab. The **Remote Listener** check box is selected by default. Deselect this check box if remote listener is turned off in the Oracle RAC database. In the **Number of RAC Nodes** field, specify the number of RAC nodes and click **GO**.

Do one of the following (Option A or Option B):

Option A:

Enter the relevant values in the following fields: **Oracle DBService Name**, **Oracle Server1**, **Oracle Port#1**, **Oracle Instance name1**, **Oracle Server2**, **Oracle Port#2**, **Oracle Instance name2.....Oracle Server**n, **Oracle Port**#n, **Oracle Instance name**n, where n is the number of nodes specified in the **Number of RAC Nodes** field, and select the **Pluggable DB** check box if you are running the MSS database instance as a pluggable database (PDB).

Option B:

Specify the JDBC URLs in the following fields:

JDBC URL#1

(Remote listener turned off)

```
jdbc:oracle:thin:@v-ip1:port1/dbservice1
```

(Remote listener turned on)

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-
ip1)(PORT=port1))(CONNECT_DATA= (SERVICE_NAME=dbservice1)
(INSTANCE_NAME=instance1)))
```

(Remote listener turned on for a pluggable database)

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-
ip1)(PORT=port1))(CONNECT_DATA= (SERVICE_NAME=pdbservice1)
(INSTANCE_NAME=instance1)))
```

JDBC URL#2

(Remote listener turned off)

```
jdbc:oracle:thin:@v-ip2:port2/dbservice2
```

(Remote listener turned on)

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-ip2)
(PORT=port2))(CONNECT_DATA= (SERVICE_NAME=dbservice2)
(INSTANCE_NAME=instance2)))
```

(Remote listener turned on for a pluggable database)

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-ip2)
(PORT=port2))(CONNECT_DATA= (SERVICE_NAME=pdbservice2)
(INSTANCE_NAME=instance2)))
```

JDBC URL#*n*

(Remote listener turned off)

```
jdbc:oracle:thin:@v-ipn:portn/dbservicen
```

(Remote listener turned on)

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-ipn)
(PORT=portn))(CONNECT_DATA= (SERVICE_NAME=dbservicen)
(INSTANCE_NAME=instancen)))
```

(Remote listener turned on for a pluggable database)

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-ipn)
(PORT=portn))(CONNECT_DATA= (SERVICE_NAME=pdbservicen)
(INSTANCE_NAME=instancen)))
```

Where:

n is the number of nodes specified in the **Number of RAC Nodes** field.

v-ip is the IP address of the node.

port is the port address of the node.

dbservice is the database service name.

pdbservice is the pluggable database service name.

instance is the instance name.

> **Note:**
>
> You must specify values in either the **Oracle Database** tab or the **Oracle RAC** tab. If you specify values in both the **Oracle Database** and the **Oracle RAC** tabs, you get an error message.

If you specify the incorrect number of nodes in the **Number of RAC Nodes** field and click **GO** on the **Oracle RAC** tab, do the steps in "Correcting the Specified Number of RAC Nodes".

Worksheet references and example values for a two-node RAC:

Field name	Worksheet reference number	Example value
Oracle Database Service Name	COMM- 0150	BEN6
Oracle Database Server Name1	COMM-0160	srvrchscal1
Oracle Database Port#1	COMM-0165	1521
Oracle Instance Name1	COMM-0170	drac1
Oracle Database Server Name2	COMM-0175	srvrchscal2
Oracle Database Port#2	COMM-0180	1521
Oracle Instance Name2	COMM-0185	drac2
APP_MSLV Password	COMM-0040	mss6mslv
APP_API Password	COMM-0050	mss6api
APP_INT Password	COMM-0055	mss6int

c. Click the **Gateway** tab, check the default selections for event servers that are to be activated, and make any necessary changes.

If you are unsure, leave the default settings. You can manually edit these settings through the **gateway.ini** file. The check boxes that appear on the tab are for APIs. When you select a check box, modifications are made to the **gateway.ini** file used to configure MSS APIs. See *MetaSolv Solution System Administrator's Guide* for more information on the **gateway.ini** file.

d. Click the **Port** tab and enter values in the **Log Port** and **CORBA Port** fields

Worksheet references and example values:

> ✎ **Note:**
>
> Default port assignments appear and may be replaced with the available port values.

Field name	Worksheet reference number	Example value
Log Port	Single-0190	4501
CORBA Port	Single-0200	2507
Debug Port	Single-0205	8453

e. Click the **Proxy** tab and enter the URL of the proxy server.

Worksheet reference and example value:

Field name	Worksheet reference number	Example value
Proxy Server URL	Single-0210	http://srvrchosa1:7070, https://srvrchosa1:7071 (when using the SSL port)

   f. Click the **Info** tab to see a summary of the selected server's properties.

9. When all tabs have correct information for the single server, click **Next**.

The installation summary appears.

10. After checking the information in the summary for accuracy, click **Install**. When the files are installed, the location of the startup file created for the server is displayed.

> **Note:**
>
> Do not exit the installer.

11. Note the location of the startup file for the application server.

12. (Optional) Do this step only if you create the domain using SSL. Open the *MSLV_Home\mslv01***\jacORB\orb.properties** file (where *MSLV_Home* is the directory in which the MSS software is installed and *mslv01* is the server home directory) and provide the appropriate values for the following properties:

```
jacorb.security.keystore=/opt1/stores/identity.jks
jacorb.security.keystore_password=identity_pwd
jacorb.security.default_user=mycert
jacorb.security.default_password=def_pwd
```

Required/Optional	Field name	Worksheet reference number	Example value
Required (Only if SSL is enabled)	jacorb.security.keystore	Single-2015	/opt1/stores/identity.jks
Required (Only if SSL is enabled)	jacorb.security.keystore_password	Single-2020	*password*
Required (Only if SSL is enabled)	jacorb.security.default_user	Single-2025	mycert
Required (Only if SSL is enabled)	jacorb.security.default_password	Single-2030	*password*

13. (Optional) Do this step only if you create the domain using SSL on the AIX platform. Open the *MSLV_Home\mslv01***\jacORB\orb.properties** file (where *MSLV_Home* is the directory in which the MSS software is installed and *mslv01* is the server home directory) and provide the appropriate values for the following properties:

```
jacorb.security.jsse.server.key_manager_algorithm=IbmX509
jacorb.security.jsse.server.trust_manager_algorithm=IbmX509
jacorb.security.jsse.client.key_manager_algorithm=IbmX509
jacorb.security.jsse.client.trust_manager_algorithm=IbmX509
```

14. Shut down the server, and restart it using the custom script installed by the installer and listed on the window.

To start the servers, navigate to the *MSLV_Home\m63domain* directory (where *m63domain* is the domain directory for the server) directory and entering the following command at a command prompt:

- For UNIX/Linux:

  ```
  startmslv01.sh
  ```

- For Windows:

  ```
  startmslv01.cmd
  ```

To shut down the server, navigate to the *m63domain* directory. At the command prompt, enter the command:

- For UNIX or Linux:

  ```
  stopmslv01.sh
  ```

- For Windows:

  ```
  stopmslv01.cmd
  ```

15. Start the WebLogic Server Administration Console by typing the following information into the **Address** field of Internet Explorer:

    ```
    http://host_admin:port_number/console
    ```

    You can monitor the deployment from the console. To check the servers, click **Servers** in the left pane of the Console, and the right pane will show the status of all servers.

16. After the startup commands have been run and the application server has been started, maximize the installer window and click **Deploy Application**.

    The Oracle Communications MetaSolv Solution Installation window appears listing the server you can select for deployment.

    This process can take a few moments. If the server is not started, a status appears on the window indicating the installer is waiting for the server to be in running mode. When the server is in running mode, you can begin the deployment.

17. Select a server in the Target Servers list box, and click **Deploy**.

    The deployment process begins. You can follow the progress of the deployment by viewing the text that appears in the right pane of the installation window.

    When the deployment is complete, the Deployment Completed window appears.

18. Click **OK**.

19. Click **Exit**.

    The Exit? window appears.

20. Click **OK** to exit.

Correcting the Specified Number of RAC Nodes

To correct the specified number of RAC nodes:

1. On the **Oracle RAC** tab, click **GO** beside the **Password** field.

2. Select the check box for the server.

3. Specify correct values in all the fields on the **Info**, **Directory**, **Oracle Database**, **Oracle RAC**, **Gateway**, **Port**, and **Proxy** tabs.

Verifying the Installation

Verification is done from the WebLogic Server Administration Console on a client workstation.

To verify the installation, do the following:

1. From a client workstation, close all open applications and start a web browser.

2. Enter the following information into the **Address** field:

   `http://host_admin:port number/console`

3. Log in to the Administration Console using your user name and password.

   The WebLogic Server Console window appears.

4. In the left pane, click *DOMAIN_NAME*, then click **Deployments**.

   The list of available applications appears in the pane on the right of the screen.

5. Verify that the following applications appear in the list:

   > **Note:**
   >
   > Click **Next** in the Deployments window to advance to the next page of applications.

   • nur
   • MSS_WebService

6. From the Domain Structure tree, expand **Services**, and then click **Data Sources** in the left pane.

   The list of available data sources and connection pools appears in the pane on the right of the screen.

7. Compare the values, shown in Table 4-1, to your installation screen to make sure you have configured WebLogic correctly for your installation.

   Table 4-1   Data Sources and Connection Pools

Data Sources	Connection Pools
mslvDataSource	MSLVPool
mslvDbTraceDataSource	MSLVDbTracePool
mslvNoneTxDataSource	MSLVNonTxPool
mslvProcDataSource	MSLVProcPool
mslvPSDataSource	MSLVpsPool
mslvWSDataSource	MSLVwsPool

8. In the left pane, click the *DOMAIN_NAME*, then click **Services**, then click **Messaging**, then click **JMS Modules**.

The list of available JMS modules appears in the pane on the right of the screen.

9. In the right pane, click **mssJMSModule**.

The list of available resources appears in the pane on the right of the screen.

10. Verify that the following JMS connection factory is present in the list of resources:

   • MSS.QueueConnectionFactory

11. Verify that mss.external.event.queue is included in the list of resources.

12. From the web browser, enter the following information into the **Address** field:

   ```
   http://host_admin:port number/main
   ```

   The MetaSolv Solution AppServer Runtime Information page appears.

13. Install the client application manually and start the MSS client.

   The MetaSolv Solution login window is displayed.

5

Installing and Deploying MetaSolv Solution on a Clustered Server

This chapter describes how to perform a full installation of the Oracle Communications MetaSolv Solution (MSS) 6.3.*x* release, if you are a new customer or upgrading from a pre-6.3 release, and explains how to set up the MSS application server for clustered server installations. The chapter covers the Oracle WebLogic server domain configuration and the installation and deployment of the MSS application server.

About Clustered Server Installation

A clustered server installation (also called an administration server with cluster-managed servers installation) is one in which one or more WebLogic Server instances are managed by a separate administration server. In this arrangement, clustering the managed servers in WebLogic allows the servers to work together as one unit, rather than several independent processing units. This is the configuration Oracle recommends because it provides protection in the event a server fails.

This section describes how to:

- Create a WebLogic domain for clustered servers
- Install MSS
- Deploy MSS to the cluster

Figure 5-1 shows the detailed process for a clustered server installation.

Figure 5-1   Installing a Cluster-Managed Server
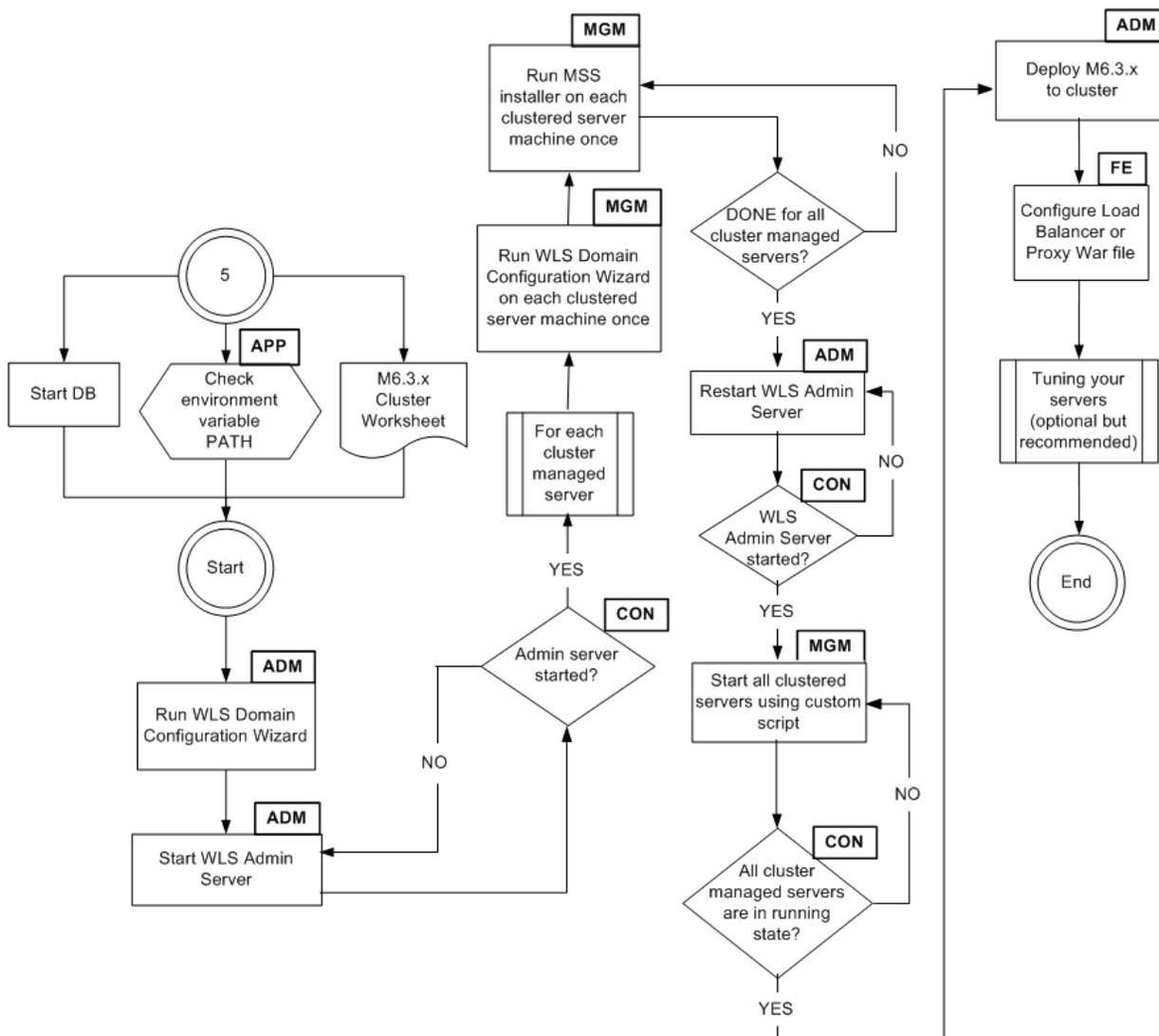
The following acronyms indicate the machine used in a step in the installation and deployment process:

ADM – WLS administration server machine   **CON** – WLS administration console
APP – All application server machine   **MGM** – All cluster-managed server machines

FE – Front end host machine, such as load balancer or proxy

Figure 5-2 shows an example configuration. This installation includes two clustered managed servers (mslv01 and mslv02), an administration server, and a hardware load balancer or Proxy server used for load balancing. To see complete information on the data for the installation, refer to the worksheet examples.

Figure 5-2   Example Cluster-Managed Server Configuration
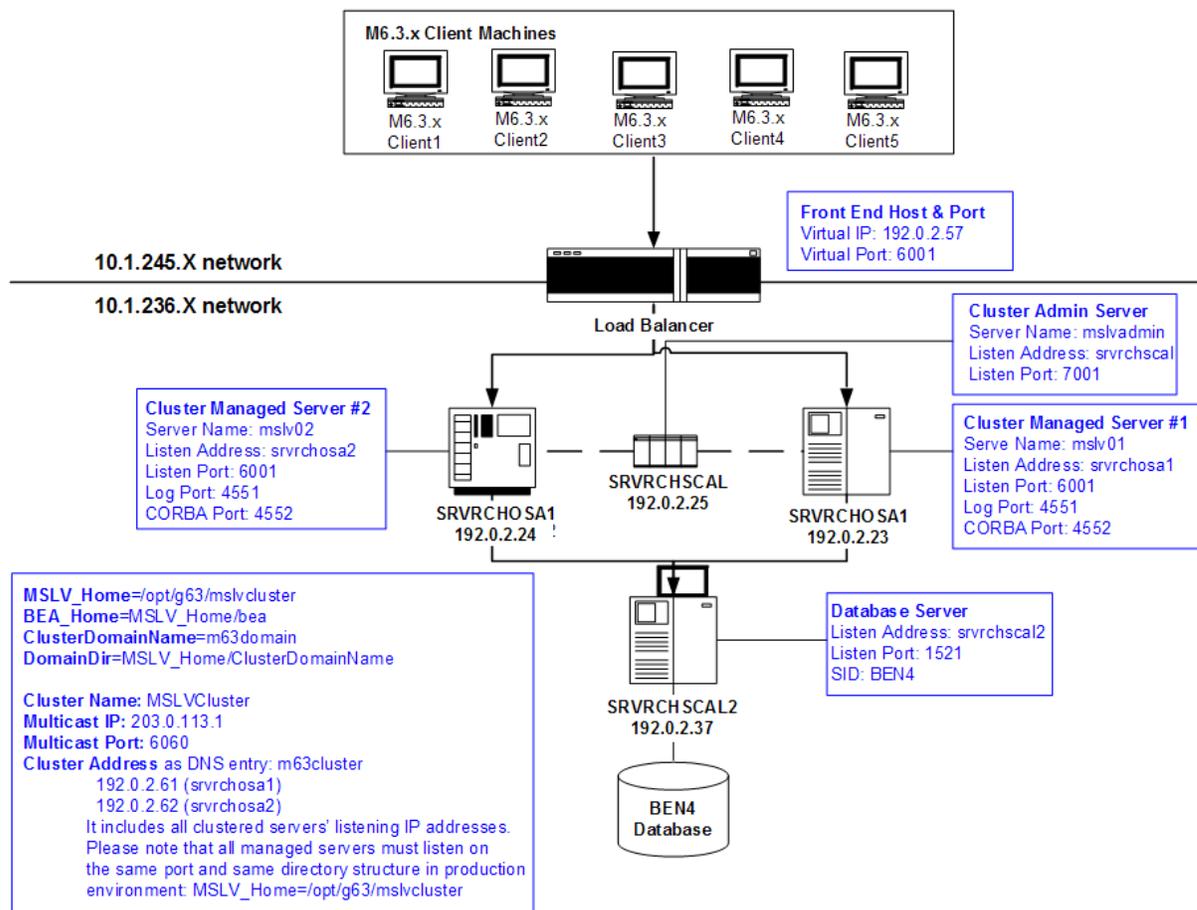
Before You Start

- Print and complete the following planning worksheets:

    – Application server common installation worksheet. See Table C-1.

    – Admin server installation worksheet. See Table C-3.

    – Clustered server general installation worksheet. See Table C-4.

    – Clustered server installation worksheet. See Table C-5.

      Complete a worksheet for each managed server in the cluster. In the example configuration used for the installation, two worksheets must be filled out, one for mslv01 and the other for mslv02.

    – WebLogic proxy server installation worksheet. See "Proxy Server Setup" for a complete description of the proxy server installation.

      Some steps in the procedures for the WebLogic domain configuration and the MSS installation refer to the worksheet.

- Review "Pre-requisites for the Latest MSS Release" and make sure all tasks listed there that apply to your installation are completed.

- You may need assistance from your system administrator or network engineering team to perform the following tasks:

  – Set up a DNS entry to include all clustered servers' listening IP addresses for cluster address during cluster domain configuration in production environment.

  – In production environment, all clustered servers must listen on the same port. If there are multiple clustered servers running on the same machine in the same cluster, the machine must have multiple network interface cards (NICs).

  – Set up a load balancer

  – Acquire the multicast IP address and port for the cluster

  – Define and verify a range of ports for each machine hosting cluster-managed servers and administration servers.

- See "Load Balancer Configuration Example" if you are using a load balancer in your clustered server installation.

Creating the Clustered Server WebLogic Domain

To create the domain, perform the following:

1. From the Administration Server, start the WebLogic Configuration Wizard by doing one of the following:

   - For UNIX/Linux platforms, run the program **config.sh** located in the directory: *MW_Home/***oracle_common/common/bin**.

   - For Windows platforms, run the program **config.cmd** located in the directory: *MW_Home***oracle_common\common\bin**.

   The Configuration Type window appears.

2. Select **Create a new domain** and in the **Domain location** field, enter the full path for the domain or click **Browse** to navigate to the domain home directory (for example, /opt/m63Cluster/cluster/*m63domain/*).

   Oracle recommends that you specify the values for domain name and domain location as shown below.

   Worksheet references and example values:

Field name	Worksheet reference number	Example value
Domain name	COMM-0010	m63domain
Domain location	COMM-0110	/opt/m63Cluster/cluster

3. Click **Next**.

   The Templates window appears.

4. Click **Next**.

   The Administrator Account window appears.

5. Enter a user name and password and verify the password by retyping, then click **Next**.

   Worksheet references and example values:

Field name	Worksheet reference number	Example value
User name	COMM-0020	weblogic
User password	COMM-0030	*password*

The Domain Mode and JDK window appears.

6. Do one of the following:

   • If you are installing for company operations, select the **Production Mode**.

   • If you are installing to do integration development or testing, select **Development Mode**.

7. Select the **Other JDK Location** option, browse to the location of another JDK, select the JDK version, and then click **Next**. See "Software Requirements" for information on required software versions.

   The **Other JDK Location** option is supported for both UNIX/Linux and Windows platforms.

   The Advanced Configuration window appears.

8. Select **Administration Server, Topology** and click **Next**.

   The Administration Server window appears.

9. Do the following:

   a. In the **Server Name** field, enter the Administration Server name.

      This single server serves as the MSS domain Administration Server.

   b. In the **Listen Address** field, select a DNS or an IP address.

      If you are creating an IPv6 domain, you must specify the IPv6 address in the **Listen Address** field.

   c. In the **Listen Port** field, accept the default.

   d. Select the **Enable SSL** check box if you want to enable SSL.

      It is not a requirement to either enable or disable SSL.

      If you decide to enable SSL, ensure that you configure SSL for WebLogic Server. See "Configuring SSL for WebLogic Server" for more information.

   e. In the **SSL Listen Port** field, enter a port that is not used by another domain.

      This field is enabled only if you selected the **Enable SSL** check box.

   f. In the **Server Groups** list, accept the provided default value.

      Worksheet references and example values:

Field name	Worksheet reference number	Example value
Name	Admin-0240	mslvadmin
Listen address	Admin-0250	srvrchsca1
Listen port	Admin-0260, Admin-0270	7001 (HTTP port), 7002 (HTTPS port)

10. Click **Next**.

The Managed Servers window appears.

11. Do the following:

    a. Click **Add** to add a managed server to the cluster.

    b. In the **Server Name** field, enter a name for the managed server.

    c. In the **Listen Address** field, enter the host, or IP address of the machine where the managed server is running.

    If you are creating an IPv6 domain, you must specify the IPv6 address in the **Listen Address** field.

> **Note:**
>
> Use listener addresses that are equal to a resolvable DNS host or IP address. Do not use **localhost** or **127.0.0.1**. Those addresses interfere with clustered servers.

    d. In the **Listen Port** field, enter the number of the port where the managed server will listen for incoming messages.

    e. Select **Enable SSL** as required.

    f. In the **SSL Listen Port** field, enter the appropriate value only if SSL is selected.

> **Note:**
>
> You can also add a proxy server at this point, if the WebLogic proxy is used.
>
> For example:
>
> • Name: **M63Proxy**;
>
> • Listen address: **servrchosal**;
>
> • Listen port: **7001**.

Field name	Worksheet reference number	Example value
Name	Cluster-0520	mslv01, mslv02
Listen address	Cluster-0550	srvrchosa1, srvrchosa2
Listen port	Cluster-0570, Cluster-0580	6001, 6001 (HTTP port); 6002, 6002 (HTTPS port) (2-node cluster)

    g. (Optional) Click **Add** to add more managed servers or proxy servers as required on your MSS deployment.

    h. Click **Next**.

    The Clusters screen appears.

12. Do the following:

a. Click **Add** to start configuring the cluster.

b. In the **Cluster Name** field, enter the name for the cluster.

c. In the **Cluster Address** field, provide the cluster address information.

   The cluster address contains each managed server along with the managed server's port separated by a comma. Separate the managed server and the port number by a colon.

   (Optional) If you are creating the cluster in an IPv6 domain, you must specify the IPv6 addresses in the **Cluster Address** field, as follows:

   ```
   [IPv6_address1]:port1, [IPv6_address2]:port2
   ```

   For example:

   ```
   [2606:b400:2010:484b:f13b:4672:38b7:5af9]:9083, [2606:b400:2010:484b:f13b:
   4672:38b7:5af9]:9084
   ```

d. In the **Frontend Host** field, enter the IP address of the frontend host for the cluster.

   (Optional) If you are creating the cluster in an IPv6 domain, you must specify the IPv6 address in the **Frontend Host** field.

   For example:

   ```
   [2606:b400:2010:484b:f13b:4672:38b7:5af9]
   ```

e. In the **Frontend HTTP Port** field, enter the port number of the frontend host for the cluster.

Field name	Worksheet reference number	Example value
Name	Cluster-0410	MSLVCluster
Frontend Host	Cluster-0430	203.0.113.1
Frontend HTTP Port	Cluster-0440	6060
Cluster address	Cluster-0420	Test/development environment: srvrchosa1:6001 (HTTP port), srvrchosa1:6002 (HTTPS port) srvrchosa2:6001 (HTTP port), srvrchosa2:6002 (HTTPS port) (2-node cluster). Production environment requires a DNS entry: m63cluster: 192.0.2.23 (srvrchosa1), 192.0.2.37 (srvrchosa2)

f. Click **Next**.

   The Server Template screen appears.

13. Click **Next** on Server Templates screen.

    The Dynamic Servers screen appears.

14. Click **Next** on Dynamic Servers screen.

The Assign Servers to Clusters screen appears.

15. Assign the servers to the cluster by moving the managed servers in the left pane to the required cluster in the right pane. Ensure that the proxy server remains in the **Servers** list.

16. Click **Next**.

    The HTTP Proxy Applications window appears.

17. (Optional) Select the **Create HTTP Proxy** check box to create an HTTP proxy application for each cluster, and from the **Proxy Server** list, select the managed server on which the proxy application must be deployed.

18. Click **Next**.

19. Click the **Machine** tab, and do the following:

    a. Click **Add** to create the first machine.

    b. In the **Name** field, enter a name for the machine.

    c. In the **Node Manager Listen Address** field, enter the host, or IP address of the node manager.

       (Optional) If you are creating the cluster in an IPv6 domain, you must specify the IPv6 address in the **Node Manager Listen Address** field.

    d. In the **Node Manager Listen Port**, enter the port number for the node manager.

    e. (Optional) Create further machines as required on your MSS deployment.

    f. Click **Next**.

       The Assign Servers to Machines screen appears.

20. Assign the servers to the machines by moving the servers in the left pane to the required machine in the right pane.

21. Click **Next**.

    The Virtual Targets screen appears.

22. Click **Next** on Virtual Targets Screen.

    The Partitions screen appears.

23. Click **Next** on Partitions Screen.

    The Configuration Summary screen appears.

24. Review the summary to verify the contents of your domain and click **Create** to create the domain.

    The Configuration Progress screen appears, which displays the progress of the domain creation process.

    After the domain is created successfully, the Configuration Success screen appears.

25. Click **Finish**.

26. From the Administration Server, start the WebLogic Configuration Wizard again by doing one of the following:

    • For UNIX/Linux platforms, run the program **config.sh** located in the directory: *MW_Home*/**oracle_common/common/bin**.

- For Windows platforms, run the program **config.cmd** located in the directory: *MW_Home***oracle_common\\common\\bin**.

   The Configuration Type window appears.

27. Select **Upgrade an existing domain**. In the **Domain location** field, enter the full path for the domain or click **Browse** to navigate to the created domain, for example in the **/opt/m63Cluster/cluster/***m63domain* directory.

28. Click **Next**.

   The Templates window appears.

29. Select the **Update Domain Using Product Templates** option and then the appropriate items from the provided list. You must select **WebLogic Advanced Web Services for JAX-WS Extension**, and the **WebLogic JAX-WS SOAP/JMS Extension** is optional depending on your requirements.

   - **WebLogic Advanced Web Services for JAX-WS Extension -** *Version* **[oracle_common]** - You must select this JAX-WS template for MSS Web Services as it is mandatory during the creation of an MSS domain.

   - **WebLogic JAX-WS SOAP/JMS Extension -** *Version* **[oracle_common]** - You select this template for SOAP over JMS Web Services or if you built custom web services that are SOAP over JMS.

   where *Version* is the Oracle WebLogic version.

   See "Software Requirements" for information on required WebLogic software version.

   See *Oracle Fusion Middleware Domain Template Reference* for more information on WebLogic templates.

30. Click **Next**.

   The Advanced Configuration window appears.

31. Keep the options the same as the default values, and click **Next**.

   The Configuration Summary window appears.

32. Click **Update**.

   The Configuration Progress window appears.

33. When the upgrade process reaches 100% completion, click **Next**.

   The End of Configuration window appears.

34. Click **Finish**.

   Then continue through the steps in the section "Verifying the Clustered WebLogic Domain Setup".

See Oracle Fusion Middleware documentation for more information on creating a clustered WebLogic Server domain.

Verifying the Clustered WebLogic Domain Setup

To verify the domain, perform the following:

1. To verify the domain setup, start the server by completing the following steps:

   a. Run **startWebLogic.sh** (UNIX/Linux) or **startWebLogic.cmd** (Windows) in the domain directory.

The domain directory is the name you specified during configuration.

For example: **/opt/m63Cluster/cluster/***m63domain*

  b. Enter your administrator user name and password, when prompted.

The server takes a few moments to start. You will see information scroll on the screen. When the server has successfully started, you will see the words RUNNING mode at the prompt.

2. (Optional) If you are creating the cluster in an IPv6 domain, you must modify the **web.xml** file of the proxy web application, as follows:

```
<servlet-name>HttpClusterServlet</servlet-name>
  <servlet-class>weblogic.servlet.proxy.HttpClusterServlet</servlet-class>
    <init-param>
     <param-name>WebLogicCluster</param-name>
     <param-value> [IPv6_address1]:port1|[IPv6_address2]:port2</param-value>
    </init-param>
```

Configuring SSL for WebLogic Server

For information about public and private keys, about identity and trust keystores, and how to create and configure them in the WebLogic Administration Console, see the following website:

http://docs.oracle.com/cd/E24329_01/web.1211/e24422/identity_trust.htm

For information about how the WebLogic server locates trust keystores, see the "How WebLogic Server Locates Trust" section at the following website:

http://docs.oracle.com/cd/E24329_01/web.1211/e24422/
identity_trust.htm#SECMG382

To configure SSL for WebLogic Server:

1. Log in to the Oracle WebLogic Server Administration Console.

2. In the **Domain Structure** tree, expand **Environment**, and then click **Servers**.

The Summary of Servers screen appears.

3. Click the **AdminServer** link.

The Settings for AdminServer screen appears.

4. Click the **Configuration** tab, and then click the **Keystores** tab.

5. From the **Keystores** list, select **Custom Identity and Custom Trust**.

6. Do the following:

  • Under the Identity section, do the following:

    a. In the **Custom Identity Keystore** field, enter the full path for the identity keystore. For example, /opt/stores/identity.jks.

    b. In the **Custom Identity Keystore Type** field, enter the type of the keystore. Typically, this attribute is Java KeyStore (JKS); if you leave this field blank, it defaults to jks.

    c. In the **Custom Identity Keystore Passphrase** field, enter the password you will enter when reading or writing to the keystore.

        d.   In the **Confirm Custom Identity Keystore Passphrase** field, enter the password again.

    •   Under the Trust section, do the following:

        a.   In the **Custom Trust Keystore** field, enter the full path for the trust keystore. For example, /opt/stores/trust.jks

        b.   In the **Custom Trust Keystore Type** field, enter the type of the keystore. Typically, this attribute is JKS; if you leave this field blank, it defaults to jks.

        c.   In the **Custom Trust Keystore Passphrase** field, enter the password you will enter when reading or writing to the keystore.

        d.   In the **Confirm Custom Trust Keystore Passphrase** field, enter the password again.

7.   Click **Save**.

8.   Click the **SSL** tab and do the following:

    •   Under the Identity section, do the following:

        a.   In the **Private Key Alias** field, enter the private key for WebLogic Server from the keystore. For example, mycert.

        b.   In the **Private Key Passphrase** field, enter the password you specified when loading the private key for WebLogic Server into the keystore.

        c.   In the **Confirm Private Key Passphrase** field, enter the password again.

    •   Under the Trust section, under Advanced, from the **Hostname Verification** list, select **None**.

9.   Click **Save**.

> **Note:**
>
> Before you install MetaSolv Solution in an IPv6 domain, ensure that your firewall configuration supports IPv6 addresses. If your firewall configuration does not support IPv6 addresses, you must enable HTTP tunneling for the Administration Server, proxy server, and all the managed servers in the WebLogic Server Administration Console. See "Enabling HTTP Tunneling" for more information.

10.   In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

11.   Open the *MSLV_Home\m63domain***\config\config.xml** file and add the following cipher suite entry for the SSL server:

```
<server>
    <name>SSLAdminServer</name>
    <ssl>
        <name>SSLAdminServer</name>
        <enabled>true</enabled>
        <ciphersuite>TLS_RSA_WITH_AES_128_CBC_SHA</ciphersuite>
        .
        .
        .
    </ssl>
```

12. Repeat steps 1 through 11 for the proxy and for each of the managed servers.

13. (Optional) This step is applicable only if you are using HTTP Cluster Servlet as the proxy server. If the domain is created for a cluster that has SSL enabled, add the following two init-parameters in the **WEB-INF\web.xml** file of the proxy application.

```
<!--The following two init-parameter tags are required if the proxy server is
set up using SSL in a clustered environment-->
<init-param>
  <param-name>SecureProxy</param-name>
  <param-value>ON</param-value>
</init-param>
<init-param>
    <param-name>DebugConfigInfo</param-name>
    <param-value>ON</param-value>
</init-param>
```

14. (Optional) If you have created the cluster in an IPv6 domain, add the following init-parameters in the **WEB-INF\web.xml** file of the proxy application.

```
<init-param>
    <param-name>WebLogicCluster</param-name>
    <param-value> [IPv6_address1]:port1|[IPv6_adrress2]:port2</param-value>
</init-param>
```

15. (Optional) If you have created the SSL cluster with proxy, change the HTTP port to HTTPS port in the **WEB-INF\web.xml** file of the proxy application.

```
<init-param>
    <param-name>WebLogicCluster</param-name>
    <param-value> [IP Address]:HTTPS_port1|[IP Address]:HTTPS_port2</param-value>
</init-param>
```

16. To call MSS Web services using the HTTPS port in an SSL environment (where the HTTP port is disabled), do the following:

    a. Log in to the Oracle WebLogic Server Administration Console.

    b. On the Home page, under Domain Configurations, click the **Domain** link.

    c. Click the **Configuration** tab, and then click the **JTA** subtab.

    d. Click **Advanced** to display advanced configuration options.

    e. From the **Web Service Transactions Transport Security Mode** list, select **SSL Required**.

    f. Click **Save**.

    g. Click **Activate Changes**.

       You can now call MSS Web services using the HTTPS port:

       ```
       https://hostname:https_port/MssWS/customer/CustomerAccount?WSDL
       ```

Installing the Self-Signed Certificate on the Client Machine

To install the self-signed certificate on the client machine:

1. Open Internet Explorer and enter the following URL:

   ```
   https://hostAddress:port/main/pblistener
   ```

   A security warning message appears.

2. Click **Continue to this website**.

3. Click the certificate errors in red.

4. Click **View Certificates**.

5. Click **Install Certificate**.

   The Certificate Import Wizard appears.

6. Select the **Place all certificates in the following store** option.

7. Click **Browse** beside the **Certificate Store:** field.

   The Select Certificate Store window appears.

8. Select **Trusted Root Certification Authorities** and click **OK**.

9. Complete the installation of the certificate.

10. Close all instances of Internet Explorer and start the MSS client.

Installing and Deploying MSS

You must run the installer and install MSS on each machine that will host a clustered server.

Prerequisites

- The instructions for creating the domain configuration included starting the server after the configuration was complete. Leave the server running until you are instructed to shut it down.

- Ensure that the following environmental variables are set:

```
JAVA_HOME=/opt/jdkVersion
PATH==JAVA_HOME/jdkVersion/bin;$PATH
MW_HOME=/opt/Oracle/Middleware/Oracle_Home
```

  where *Version* is the JDK version portion of the directory.

To install and deploy MSS, do the following:

1. From *MSLV_Home,* enter the following command:

   `java -jar MSS.RreleaseNumber.bbuild_AppServerInstaller.jar`

   where *releaseNumber* is the MSS software release version and *build* is the build number. For example:

   `java -jar MSS.R6_3.b400_AppServerInstaller.jar`

   > **✎ Note:**
   >
   > For 64-bit systems, use the following java_options parameter: **-d64**.

   The Select MetaSolv home directory window appears.

2. From the **Look In** list, select a directory in which to store the installer files then click **Select**.

   A directory named **installer** is automatically created in the selected directory. Oracle recommends choosing your *MSLV_Home* directory for this task.

The installer auto-launches the installation process by invoking **setup.sh** (UNIX/ Linux) or **setup.cmd** (Windows) in the *MSLV_Home/***installer** directory.

Worksheet reference and example value:

Field name	Worksheet reference number	Example value
File Name (*MSLV_Home*)	COMM-0090	/opt/m63Cluster/cluster

The Oracle Communications MetaSolv Solution Installation window appears.

3. Click **Next**.

    The Oracle Communications MetaSolv Solution Installation - Choose Install Type window appears.

4. Select **Full Installation on WebLogic Server with JAX-WS Domain** and click **Next**.

    The Oracle Communications MetaSolv Solution Installation - Full Select Server window appears.

5. Do the following:

    a. In the **Admin Host** field, enter the host name or the IP address of the administration server.

        If you are using an SSL cluster, enter the host name in the **Admin Host** field.

        If you are creating an IPv6 domain, you must specify the IPv6 address in the **Admin Host** field.

        (Optional) If you are creating the cluster in an IPv6 domain in a dual-stack machine, ensure that you specify the IPv6 address and the system name in the **etc/hosts** file, as follows:

        ```
        IPv6address          ipv6machine@example.com      ipv6machine
        ```

> **Note:**
>
> The MetaSolv Solution installer does not support the use of virtual IP address during installation. If you specify a virtual IP address during installation, the installer does not display the following:
>
> - The check box to select the server you want MSS installed on.
> - The following configuration tabs:
>
>   Directory
>
>   Oracle Database
>
>   Oracle RAC
>
>   Gateway
>
>   Port
>
>   Proxy
>
> If your configuration requires the use of virtual IP address, you must specify the physical IP address during installation. After the installation is complete, you can change each managed server's listen address and port to the virtual IP address, and then restart the WebLogic server. See "Changing an IP Address" for more information.

b. In the **Port#** field, enter the port number of the administration server.

c. In the **User ID** field, enter the user name for the administration server.

d. In the **Pass** field, enter the password for the administration server.

Worksheet references and example values:

Field name	Worksheet reference number	Example value
Admin Host	Admin-0250	srvrchscal
Port#	Admin-0260, Admin-0270	7001 (HTTP port), 7002 (HTTPS port)
User ID	COMM-0020	weblogic
Pass	COMM-0030	*password*

e. (Optional) If you want to install and deploy MSS using the SSL port, leave the **Connect to WebLogic using SSL** check box selected (which the installer selects by default).

See the Oracle WebLogic Server documentation for information about configuring keystores.

f. In the **Key Store Location** field, enter the path for the keystore or click **Browse** to navigate to the keystore location. The keystore should be referred to in the **trust.jks** file.

6. Click **GO**.

The installer queries the Admin Host machine and returns with values you entered during the configuration of the WebLogic domain. This process can take a few moments.

If the domain does not have a JAX-WS template applied, then the following message is displayed:

```
Please update the domain with the required JAX-WS Extension template and restart
the installation.
```

Please exit the installer and upgrade the domain by applying the **WebLogic Advanced Web Services for JAX-WS Extension** template and optionally the **WebLogic JAX-WS SOAP/JMS Extension** template. Retry the installation again after selecting the appropriate template(s):

- WebLogic Advanced Web Services for JAX-WS Extension Template (Required)
- WebLogic JAX-WS SOAP/JMS Extension Template (Optional)

The Oracle Communications MetaSolv Solution Installation window appears with the domain and any servers in the domain appearing in the left pane.

7. In the tree view on the left, select the check box next to the server you want MSS installed on.

   Tabs appear in the right pane for information to be entered for the selected cluster.

Figure 5-3   View to Select the Server for Cluster Installation
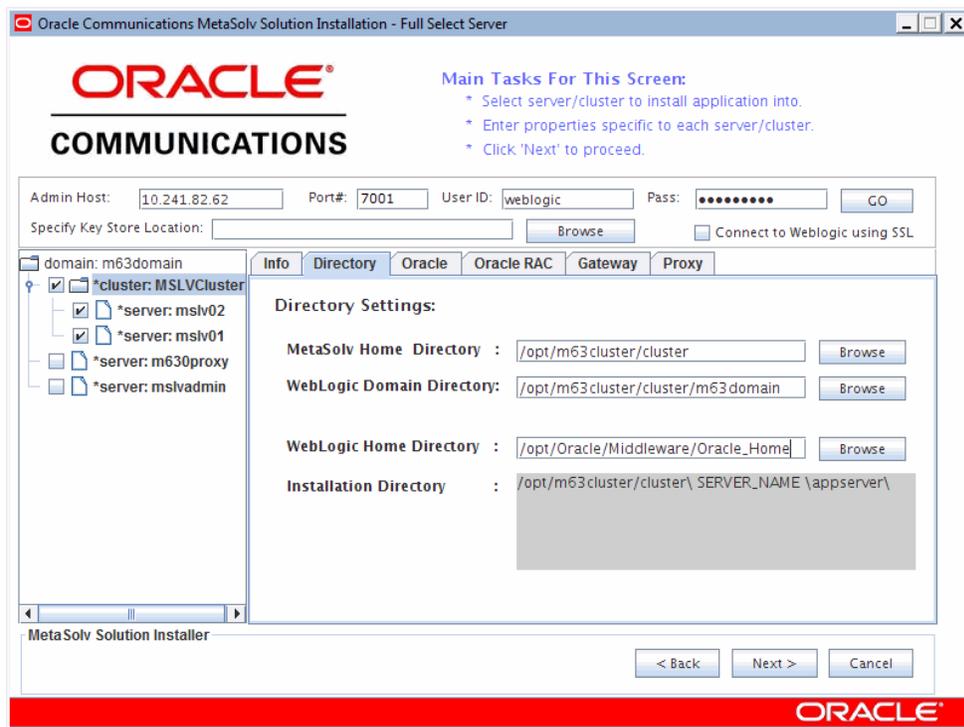
8. Complete domain information by selecting and completing the following tabs:

   a. Click the **Directory** tab and type the path and name of the MetaSolv home directory, WebLogic Domain directory, and WebLogic Home directory or click **Browse** to search for the directories.

      Worksheet references and example values:

Field name	Worksheet reference number	Example value
MetaSolv Home Directory	COMM-0090	/opt/m63Cluster/cluster
WebLogic Domain Directory	COMM-0010	/opt/m63Cluster/cluster/*m63domain*

b. Depending on your database configuration, do one of the following (Option 1 or Option 2):

Option 1:

Click the **Oracle Database** tab and do one of the following:

In the **Oracle Server Name**, **Oracle Port#**, and **Oracle Service Name** fields, enter the relevant values, and select the **Pluggable DB** check box if you are running the MSS database instance as a pluggable database (PDB).

OR

In the **JDBC URL** field, enter your own free-form JDBC connect string.

Example of a JDBC URL string:

```
jdbc:oracle:thin:@srvrchscal2:1521:BEN6
```

Example of a JDBC URL string for a pluggable database:

```
jdbc:oracle:thin:@srvrchscal2:1521/BEN6
```

Worksheet references and example values:

Field name	Worksheet reference number	Example value
Oracle Database Server Name	COMM-0130	srvrchscal2
Oracle Database Port	COMM-0140	1521
Oracle Database Service Name	COMM- 0150	BEN6
APP_MSLV Password	COMM-0040	mss6mslv
APP_API Password	COMM-0050	*password*
APP_INT Password	COMM-0055	*password*

Option 2:

Click the **Oracle RAC** tab. The **Remote Listener** check box is selected by default. Deselect this check box if remote listener is turned off in the Oracle RAC database. In the **Number of RAC Nodes** field, specify the number of RAC nodes and click **GO**.

Do one of the following (Option A or Option B):

Option A:

Enter the relevant values in the following fields: **Oracle DBService Name**, **Oracle Server1**, **Oracle Port#1**, **Oracle Instance name1**, **Oracle Server2**, **Oracle Port#2**, **Oracle Instance name2.....Oracle Server***n*, **Oracle Port***#n*, **Oracle Instance name***n*, where *n* is the number of nodes specified in the

Number of RAC Nodes field, and select the **Pluggable DB** check box if you are running the MSS database instance as a pluggable database (PDB).

Option B:

- Specify the JDBC URLs in the following fields:

  JDBC URL#1

  (Remote listener turned off)

  ```
  jdbc:oracle:thin:@v-ip1:port1/dbservice1
  ```

  (Remote listener turned on)

  ```
  jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-ip1)
  (PORT=port1))(CONNECT_DATA= (SERVICE_NAME=dbservice1)
  (INSTANCE_NAME=instance1)))
  ```

  (Remote listener turned on for a pluggable database)

  ```
  jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-
  ip1)(PORT=port1))(CONNECT_DATA= (SERVICE_NAME=pdbservice1)
  (INSTANCE_NAME=instance1)))
  ```

  JDBC URL#2

  (Remote listener turned off)

  ```
  jdbc:oracle:thin:@v-ip2:port2/dbservice2
  ```

  (Remote listener turned on)

  ```
  jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-ip2)
  (PORT=port2))(CONNECT_DATA= (SERVICE_NAME=dbservice2)
  (INSTANCE_NAME=instance2)))
  ```

  (Remote listener turned on for a pluggable database)

  ```
  jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-
  ip2)(PORT=port2))(CONNECT_DATA= (SERVICE_NAME=pdbservice2)
  (INSTANCE_NAME=instance2)))
  ```

  JDBC URL#n

  (Remote listener turned off)

  ```
  jdbc:oracle:thin:@v-ipn:portn/dbservicen
  ```

  (Remote listener turned on)

  ```
  jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-ipn)
  (PORT=portn))(CONNECT_DATA= (SERVICE_NAME=dbservicen)
  (INSTANCE_NAME=instancen)))
  ```

  (Remote listener turned on for a pluggable database)

  ```
  jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=TCP)(HOST=v-
  ipn)(PORT=portn))(CONNECT_DATA= (SERVICE_NAME=pdbservicen)
  (INSTANCE_NAME=instancen)))
  ```

  Where:

  n is the number of nodes specified in the **Number of RAC Nodes** field.

ORACLE®

v-ip is the IP address of the node.

port is the port address of the node.

dbservice is the database service name.

instance is the instance name.

> **Note:**
>
> You must specify values in either the **Oracle Database** tab or the **Oracle RAC** tab. If you specify values in both the **Oracle Database** and the **Oracle RAC** tabs, you get an error message.
>
> If you specify the incorrect number of nodes in the **Number of RAC Nodes** field and click **GO** on the **Oracle RAC** tab, do the steps in "Correcting the Specified Number of RAC Nodes".

Worksheet references and example values for a two-node RAC:

Field name	Worksheet reference number	Example value
Oracle Database Service Name	COMM- 0150	BEN6
Oracle Database Server Name1	COMM-0160	srvrchscal1
Oracle Database Port#1	COMM-0165	1521
Oracle Instance Name1	COMM-0170	drac1
Oracle Database Server Name2	COMM-0175	srvrchscal2
Oracle Database Port#2	COMM-0180	1521
Oracle Instance Name2	COMM-0185	drac2
APP_MSLV Password	COMM-0040	mss6mslv
APP_API Password	COMM-0050	*password*
APP_INT Password	COMM-0055	*password*

c. Click the **Gateway** tab, check the default selections for event servers that are to be activated, and make any necessary changes.

If you are unsure, leave the default settings. You can manually edit these settings through the **gateway.ini** file. The check boxes that appear on the tab are for APIs. When you select a check box, modifications are made to the **gateway.ini** file used to configure MSS APIs. See *MetaSolv Solution System Administrator's Guide* for more information on the **gateway.ini** file.

d. Click the **Proxy** tab if you use a proxy server or an external load balancer and provide the URL of the proxy server in the **Proxy Server URL** field.

If the installation type is SSL, specify the host name in the **Proxy Server URL** field.

For example:

```
https://example.com/9095
```

Worksheet references and example values:

Field name	Worksheet reference number	Example value
Proxy Server URL	Cluster-0450	http://srvplosa1:7001

e. Click the **Info** tab to see a summary of the selected server's properties.

9. When all tabs have correct information for the single server, click **Next**.

   The Installation Summary window appears.

10. After checking the information in the summary for accuracy, click **Install**.

   The installer installs the appropriate MSS files to the server. When the files are installed, the location of the startup file created for the server is displayed.

   > **Note:**
   >
   > Do not exit the installer.

11. Note the location of the startup file for the application server.

    If the installation type is SSL then perform step 12 for each managed

12. (Optional) Do this step only if you create the domain using SSL. Open the *MSLV_Home\mslv01***jacORB\orb.properties** file (where *MSLV_Home* is the directory in which the MSS software is installed and *mslv01* is the server home directory) and provide the appropriate values for the following properties:

    ```
    jacorb.security.keystore=/opt1/stores/identity.jks
    jacorb.security.keystore_password=<password of the identity keystore>
    jacorb.security.default_user=<default user>
    jacorb.security.default_password=<default password>
    ```

    Repeat this step for each managed server.

13. (Optional) Do this step only if you create the domain using SSL on the AIX platform. Open the *MSLV_Home\mslv01***jacORB\orb.properties** file (where *MSLV_Home* is the directory in which the MSS software is installed and *mslv01* is the server home directory) and provide the appropriate values for the following properties:

    ```
    jacorb.security.jsse.server.key_manager_algorithm=IbmX509
    jacorb.security.jsse.server.trust_manager_algorithm=IbmX509
    jacorb.security.jsse.client.key_manager_algorithm=IbmX509
    jacorb.security.jsse.client.trust_manager_algorithm=IbmX509
    ```

    Repeat this step for each managed server.

14. Shut down the server by navigating to the *MSLV_Home\m63domain* directory (where *m63domain* is the domain directory for the server) and entering the following command at a command prompt:

    • For UNIX or Linux:

      ```
      stopmslv01.sh
      ```

    • For Windows:

      ```
      stopmslv01.cmd
      ```

15. Restart the server by entering the command:

- For UNIX or Linux:

  ```
  startmslv01.sh
  ```

- For Windows:

  ```
  startmslv01.cmd
  ```

16. (Optional) If you are in Development mode, you should also start the Debug Proxy server using the following command:

- For Windows:

  ```
  startDebugProxy.cmd
  ```

- For UNIX/Linux:

  ```
  startDebugProxy.sh
  ```

17. Start the WebLogic Server Administration Console by entering the following in a web browser:

```
http://host_admin:port/console
```

where:

host_admin is the name or IP address of the Administration Server.

port is the port number of the Administration Server.

You can monitor the deployment from the console. To check the servers, click **Servers** in the left pane of the Console, and the right pane will show the status of all servers.

18. After the startup commands have been run and the application server has been started, maximize the installer window and click **Deploy Application**.

The Oracle Communications MetaSolv Solution Installation window appears listing the server you can select for deployment.

This process can take a few moments. If the server is not started, a status appears on the window indicating the installer is waiting for the server to be in running mode. When the server is in running mode, you can begin the deployment.

19. From the Target Servers list, select a server and click **Deploy**.

The deployment process begins. You can follow the progress of the deployment by viewing the text that appears in the right pane of the installation window.

When the deployment is complete, the Deployment Completed window appears.

20. Click **OK**.

21. Click **Exit**.

The Exit? window appears.

22. Click **OK**.

23. When all clustered servers have been deployed, shut down all servers, and restart them from the locations given using the start command listed on the window.

Start the administration server first, then bring up the remaining servers using the commands listed in the window. For example, using the servers from the procedures, the first server to be started would be mslvadmin, then mslv01, and then mslv02.

To shut down the admin, manage, and proxy servers, use the stop server scripts in the *m63domain* directory.

For example:

```
stopmslv01.sh
stopmslv02.cmd
stopProxyAndAdmin.sh
stopProxyAndAdmin.cmd
```

24. (Optional) Configure the load balancer.

See "Load Balancer Configuration Example" for more information.

25. (Optional) Configure the proxy server set up.

See "Proxy Server Setup" for more information.

26. (Optional) Do performance tuning on the servers.

See "Tuning Servers For Performance" for more information.

Verifying the Deployment and Configuration

To verify deployment:

1. From a client workstation, start Microsoft Internet Explorer.

2. Enter the following information into the **Address** field:

```
http://host_admin:port number/main
```

The MetaSolv Solution AppServer Runtime Information page appears, indicating that the deployment was successful.

To verify the configuration:

1. Start the WebLogic Server Administration Console by typing the following information into the **Address** field of Internet Explorer and pressing ENTER:

```
http://host_admin:port/console
```

2. Type your user name and password, then click **Sign in**.

3. Compare the values shown in Table 5-1 to your installation screen to make sure you have configured WebLogic correctly for your installation.

Table 5-1   Data Sources and Connection Pools

Data Sources	Connection Pools
mslvDataSource	MSLVPool
mslvDbTraceDataSource	MSLVDbTracePool
mslvNoneTxDataSource	MSLVNonTxPool
mslvProcDataSource	MSLVProcPool
mslvPSDataSource	MSLVpsPool
mslvWSDataSource	MSLVwsPool

JMS Connection Factories and Distributed Destinations

To view the JMS connection factories and distributed destinations:

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Services**, then expand **Messaging**, and then click **JMS Modules**.

   The Summary of JMS Modules page appears.

3. Click **mssJMSModule**.

   The Settings for mssJMSModule page appears. The resources for the mssJMSModule are listed under the Summary of Resources section.

   Figure 5-4 shows the list of connection factories and distributed destinations.

Figure 5-4   Summary of Resources Section

Connection Factories

•   MSS.QueueConnectionFactory

Distributed Destinations

> **Note:**
>
> The following queues in the list of Distributed Destinations have a separate queue configured for each clustered server for load balancing.

•   mss.external.event.queue

JMS Servers

To view JMS Servers:

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Services**, then expand **Messaging**, and then click **JMS Servers**.

   The Summary of JMS Servers page appears.

The installer creates queues under each JMS server.

Figure 5-5 shows JMS servers for the installation example.

Figure 5-5   JMS Servers Web Page

JMS Servers (Filtered - More Columns Exist)

Click the *Lock & Edit* button in the Change Center to activate all the buttons on this page.

Name ⌃	Persistent Store	Target	Current Target	Health
mssJMSServer_auto_1	mssJMSStore_auto_1	DIT2_ManagedServer_1 (migratable)	DIT2_ManagedServer_1	✔ OK
mssJMSServer_auto_2	mssJMSStore_auto_2	DIT2_ManagedServer_2 (migratable)	DIT2_ManagedServer_2	✔ OK
pluginJMSServer_auto_1	pluginStore_auto_1	DIT2_ManagedServer_1 (migratable)	DIT2_ManagedServer_1	✔ OK
pluginJMSServer_auto_2	pluginStore_auto_2	DIT2_ManagedServer_2 (migratable)	DIT2_ManagedServer_2	✔ OK
WseeJaxwsJmsServer_auto_1	WseeJaxwsFileStore_auto_1	DIT2_ManagedServer_1 (migratable)	DIT2_ManagedServer_1	✔ OK
WseeJaxwsJmsServer_auto_2	WseeJaxwsFileStore_auto_2	DIT2_ManagedServer_2 (migratable)	DIT2_ManagedServer_2	✔ OK
WseeJaxwsJmsServer_auto_3		M63DIT2Proxy	M63DIT2Proxy	✔ OK

Showing 1 to 7 of 7 Previous | Next

Multiple Single Server Instances on the Same Machine

Complete the following steps for each single server being set up on a machine.

> **Note:**
>
> Create each single server under a different logon user ID.

To set up one single server instance on a machine:

1. Create an *MSLV_Home* directory for the single server.

2. Install the Oracle WebLogic Server under the *MSLV_Home* directory.

3. Create the WebLogic domain for a single server. See "Creating a Single Server WebLogic Domain" for more information.

   > **Note:**
   >
   > You need to perform the Load Database action only once for each database, regardless of the number of servers on the machine.

4. Log in to the WebLogic Server Administration Console.

5. In the Domain Structure tree, expand **Services**, and then click **Persistent Stores**.

   The Summary of Persistent Stores page appears.

6. Click **cgJMSStore**.

   The Settings for cgJMSStore page appears.

7. In the **Prefix Name** field, modify the prefix name.

   This value should be unique for each server.

8. Click **Save**.

9. Restart the WebLogic server.

6

Upgrading Oracle Communications MetaSolv Solution

This chapter explains how to upgrade Oracle Communications MetaSolv Solution (MSS) to a newer version. The topics in the chapter cover downloading and installing a maintenance release or patch to the following MSS components:

- Database
- Application server
- Client workstation

> **Note:**
>
> This chapter focuses on upgrading to a future maintenance release or patch of MSS 6.3.*x*, using the Upgrade option of the MSS Installer.
>
> If MSS 6.3.*x* has not been previously installed, refer to "Installing and Deploying MetaSolv Solution on a Single Server " or "Installing and Deploying MetaSolv Solution on a Clustered Server" to install MSS 6.3.*x* and then return to this chapter to perform subsequent maintenance release or patch installations.
>
> If MSS 6.3.*x* has been previously installed, you can install the maintenance release or patch using the *Full Installation* option of the MSS Installer. Refer to "Installing and Deploying MSS" in "Installing and Deploying MetaSolv Solution on a Single Server " or "Installing and Deploying MSS" in "Installing and Deploying MetaSolv Solution on a Clustered Server" to install the maintenance release or patch using this option.

MSS Application Server Upgrade Process

The high-level application server upgrade process is described below:

- Undeploy MSS 6.3-related applications.
- Install MSS 6.3.*x*.
- Install/deploy MSS 6.3.*x*-related applications.
- Update/restore configuration files.

Downloading the Maintenance Release or Patch Software

Software for MSS patches is downloaded from the My Oracle Support website. For information on downloading product software, see "Downloading the Installation Files".

Download the file for the appropriate patch you are installing. The following bullet shows how the download link for the file appears on the Oracle software delivery website.

- **MSS.R***releaseNumber*.**b***build*_**AppServerInstaller**: This file contains an installer for application server machines where *releaseNumber* is the MSS software release version and *build* is the build number. The files it installs on the application server include both the application server software and the client software, which is distributed from the application server. An example filename is in the following format:

  ```
  MSS.R6_3.b400_AppServerInstaller.jar
  ```

Installing a Maintenance Release or Patch on the Database

Your database must be at least at the 6.3 release level to install a 6.3.*x* maintenance release or patch. See "Setting Up The MSS Database" for steps on how to upgrade the database to MSS 6.3.*x.* Then, follow the steps in this chapter to apply a subsequent maintenance release or patch.

To learn about database changes included in a given release, see *MetaSolv Solution Database Change Referenc*e. This document can be downloaded from the Oracle software delivery website.

Figure 6-1 shows the upgrade path for the database.

Figure 6-1   MSS Database Upgrade Path
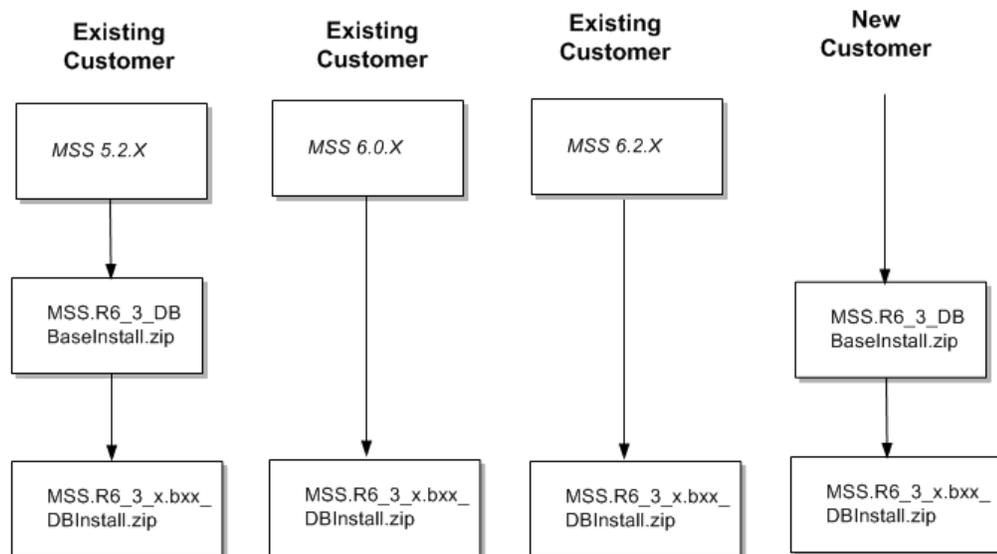
> **Note:**
>
> Before upgrading your database to MSS 6.3.x, ensure that you grant the SELECT ON privileges to ASAP user ID by running the following GRANT statement using a user ID other than ASAP (for example, SYS) that has database administrator privileges:
>
> ```
> GRANT SELECT ON sys.user$ TO asap WITH GRANT OPTION;
> ```

Extracting the MSS Database Scripts

Extracting the contents of the **MSS.R6_3_0.b**xx**_DBInstall.zip** file copies SQL scripts, procs, and reports to a directory you choose on a client machine or on the database server. Figure 6-2 shows the directory structure that results from the extract, based on the paths specified in the ZIP file.

Figure 6-2   Structure of Database Upgrade File
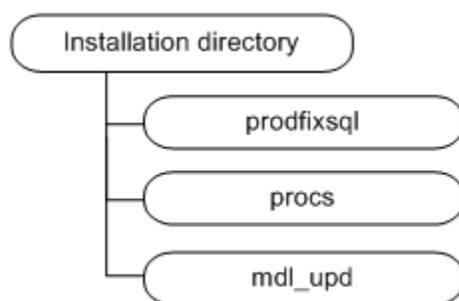
The MSS database scripts reside in the **MSS.R6_3_0.b**xx**_DBInstall.zip** file (where *xx* is the build number). This zip file contains database scripts used to upgrade an existing MSS 6.0.2 or higher database to MSS 6.3.*x*.

To extract the MSS database scripts to the database server machine:

1. Locate and select the **MSS.R6_3_0.b**xx**_DBInstall.zip** file.

2. Right-click the file, select **Open With**, then select **WinZip Executable**.

3. From the main menu bar, select **Actions** and then select **Select All**.

4. From the main menu bar, select **Actions** and then select **Extract**.

5. Browse to the directory to which you want to extract the database scripts. Oracle recommends extracting the scripts to a directory on your database server.

To successfully install a maintenance release or patch on the database, you must run the two following master SQL files:

*   **pfixSQL_Master** located in the **prodfixsql** directory

*   **master** located in the **procs** directory.

All 6.3.*x* maintenance releases carry cumulative changes from previous maintenance releases. That means you only have to run the **pfixSQL_Master** and **master** SQL files

for the maintenance release you are installing to get all changes since the 6.0.2 GA release.

Updating the Database by Running SQL Scripts

The **prodfixsql** directory has a number of SQL scripts that update your database.

To update the database:

1. Change your **Start in:** directory to the location where you want the audit logs to appear and connect (from that location) to SQL*Plus using the ASAP user ID.

2. At the prompt, enter:

   `@driveletter:installation_directory/prodfixsql/pfixSQL_Master.sql`

   The SQL scripts run against the database and make the appropriate changes for the maintenance release or patch. When the prompt reappears, the contents of the **prodfixsql** directory where the SQL files were stored have been applied.

   > **✎ Note:**
   >
   > Before running the SQL scripts, refer to Technical Bulletin ID # 435879.1 to determine how it affects your upgrade. To locate this bulletin, go to the My Oracle Support website:
   >
   > https://support.oracle.com
   >
   > and click the **Knowledge** tab.

3. Verify that the contents of the **prodfixsql** directory have been applied to your database correctly, review the log file for each **prodfixsql** file that was applied.

   The log files reside in the **Start in:** directory. Search the files in the directory for **ORA-**.

4. Open the **dm_rprt.txt** file and look for processes that have passed, failed, or not run.

   If you find processes that failed or did not run, contact Oracle Global Customer Support.

Updating Stored Procedures

Use SQL*Plus to apply the contents of the *install_directory***procs** directory to the database. These steps update the stored procedures for your database.

To update stored procedures:

1. Set the current directory to:

   `drive_letter:\install_directory\procs`

2. Connect to SQL*Plus using the ASAP user ID.

3. At the prompt, enter:

   ```
   spool master.log
   @master
   ```

The stored procedures have been applied when the **<SQL>** prompt reappears.

4. Enter:

```
spool offrun
```

Running Reports

The **mdl_upd** directory contains SQL files that include any modifications to the database structure in a service pack. To apply these updates to the reports, copy the contents of this directory into either the **db/inst_60** or **db/upg_60** directory. After applying the files in the **prodfixsql** directory, you can validate the database structure by running the **mdl_upd_cur.sql** or **mdl_upd_cmp.sql** file, or both. These processes provide the reports **mdl_upd_cur.txt** and **mdl_upd_cmp.txt** identical to the **mdl_cur.sql** and **mdl_cmp.sql** files. See *MetaSolv Solution System Administrator's Guide* for more information on reports.

> ✎ **Note:**
>
> This task is not required. If you choose not to apply updates to the reports before you run them, extra database objects can appear in the reports.

Upgrading the MSS Application Server

The installer JAR file for the application server portion of MSS is the same for both maintenance release and patch installations. Download the installer for the appropriate platform and the appropriate upgrade type (maintenance release or patch) from the Oracle software delivery website.

See "Downloading the Maintenance Release or Patch Software" for more information on the JAR file name.

Installation Options for the Application Server

Oracle recommends the following for the application server installation of the MSS 6.3.*x* maintenance release and patches:

- **First time installing or upgrading the MSS 6.3.*x* release stream**: Select the MSS 6.3.*x* **Full Installation** option in the application installer. Significant changes were made in the WebLogic Server configuration for these maintenance releases, and using the full installation guarantees that all changes are installed on your machine. Refer to "Installing and Deploying MetaSolv Solution on a Single Server" or "Installing and Deploying MetaSolv Solution on a Clustered Server" to install MSS 6.3.*x*.

  The files in the following directories (under the *MSLV_Home/server_name***l appserver** directory) are updated if you select the **Full Installation** option and it will be necessary to backup the following files and directories:

  – bin

  – cab

  – classes

- – config

  - – flow_through_package

  - – portal

  - – samples

  - – samples/customExtensions

  - – utils

- • **Patches and Subsequent Maintenance Releases:** select the MSS 6.3.x **Upgrade** option when you install a patch or subsequent maintenance release. Review the **ReadMe** file and manually apply any required configuration changes.

  The following application server configuration files are updated if you select the **Upgrade** option and it will be necessary to backup these files:

  - – jmaster.ini

  - – lerg.ini

  - – loggingconfig.xml

  - – npasplit.ini

  - – tbs.ini

  - – tbs_util.ini

  The following files are not updated if you select the **Upgrade** option:

  - – Application server start up files:

    - * **startMSLVmanaged.sh** or **startMSLVmanaged.cmd**

    - * **startMSLVsingle.sh** or **startMSLVsingle.cmd**

    - * **start**_servername_**.sh** or **start**_servername_**.cmd**

  - – Gateway configuration files

    - * **gateway.ini**

    - * **integration.xml**

  - – WebLogic Server configuration parameters

  - – JacORB configuration parameters

Single Server Upgrade Basic Steps

To upgrade the single server:

1. Prepare for the upgrade. This includes downloading files and collecting information.

2. Install /Deploy MSS 6.3.*x.*

3. Complete post-upgrade tasks.

    a. (Optional) Tune the server.

    b. (Optional) Make changes to the configuration files.

Single Server Upgrade

Follow the procedures in this section to upgrade the server.

> **Note:**
>
> Before upgrading your application server to MSS 6.3.*x*, refer to Technical Bulletin ID # 435745.1, to determine how it affects your upgrade. Failure to do so results in the server failing to start after installing the application. To locate this bulletin, go to the My Oracle Support website:
>
> https://support.oracle.com
>
> and click the **Knowledge** tab.

> **Note:**
>
> You will need to manually modify the **loggingconfig.xml** and the **integration.xml** files or you will receive an error on your appserver console. Additionally, if using custom extensions, you will need to manually modify the **gateway.ini** file. For information on custom extensions, see *MetaSolv Solution Custom Extensions Developer's Reference*.

Preparing for the Upgrade

The highlighted sections of Figure 6-3 show the steps for preparing for the upgrade.

Figure 6-3   Preparing for the Upgrade
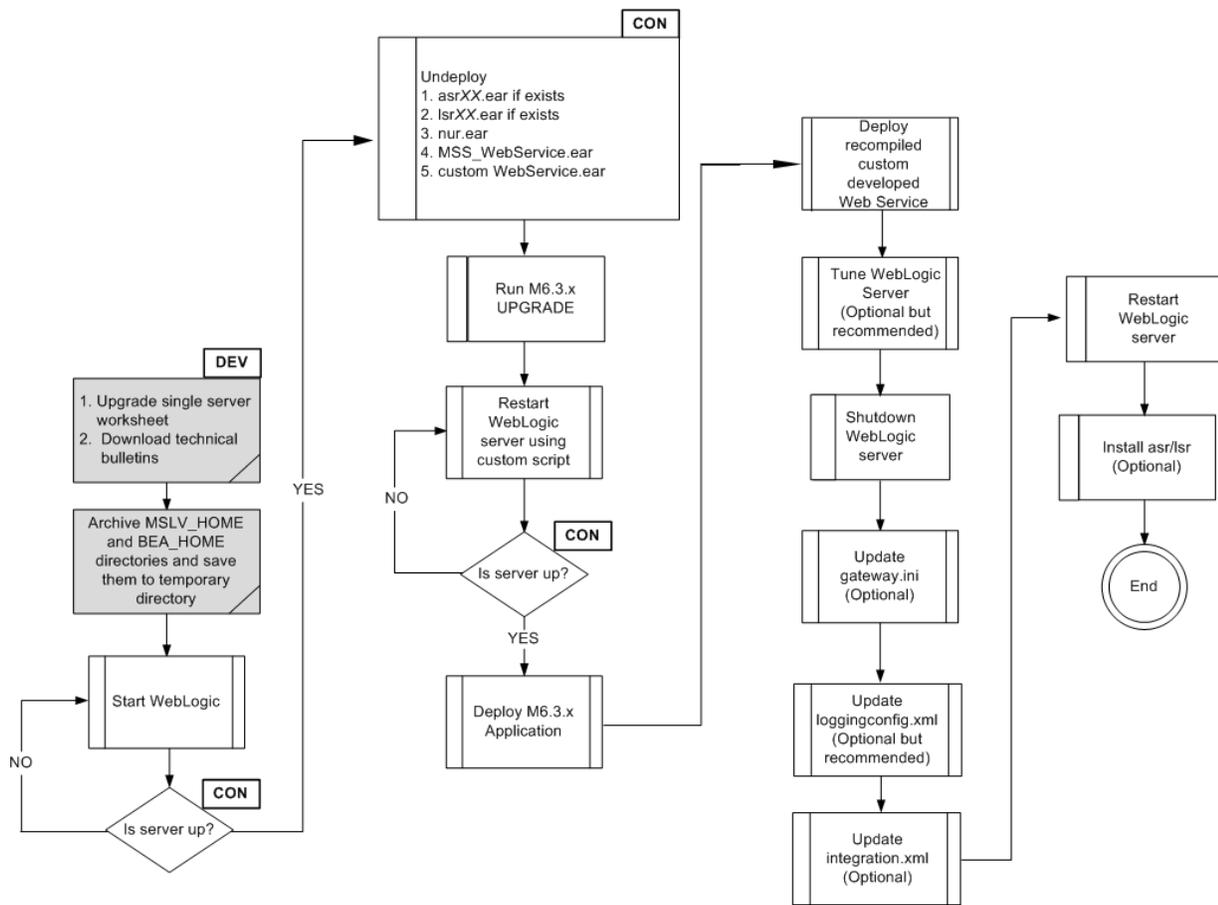
To prepare for the upgrade**:**

1. Download the MSS upgrade (either a maintenance release or a patch) from the Oracle software delivery website.

2. FTP the MSS upgrade file to the target server machine.

3. Complete the appropriate single server worksheets in Appendix C.

4. Archive the *MSLV_Home* and *MW_Home* directories and save the archive file to a temporary directory.

Undeploy Previously Installed Applications

The highlighted sections of Figure 6-4 show the steps for undeploying previously installed applications.

Figure 6-4   Undeploying Applications
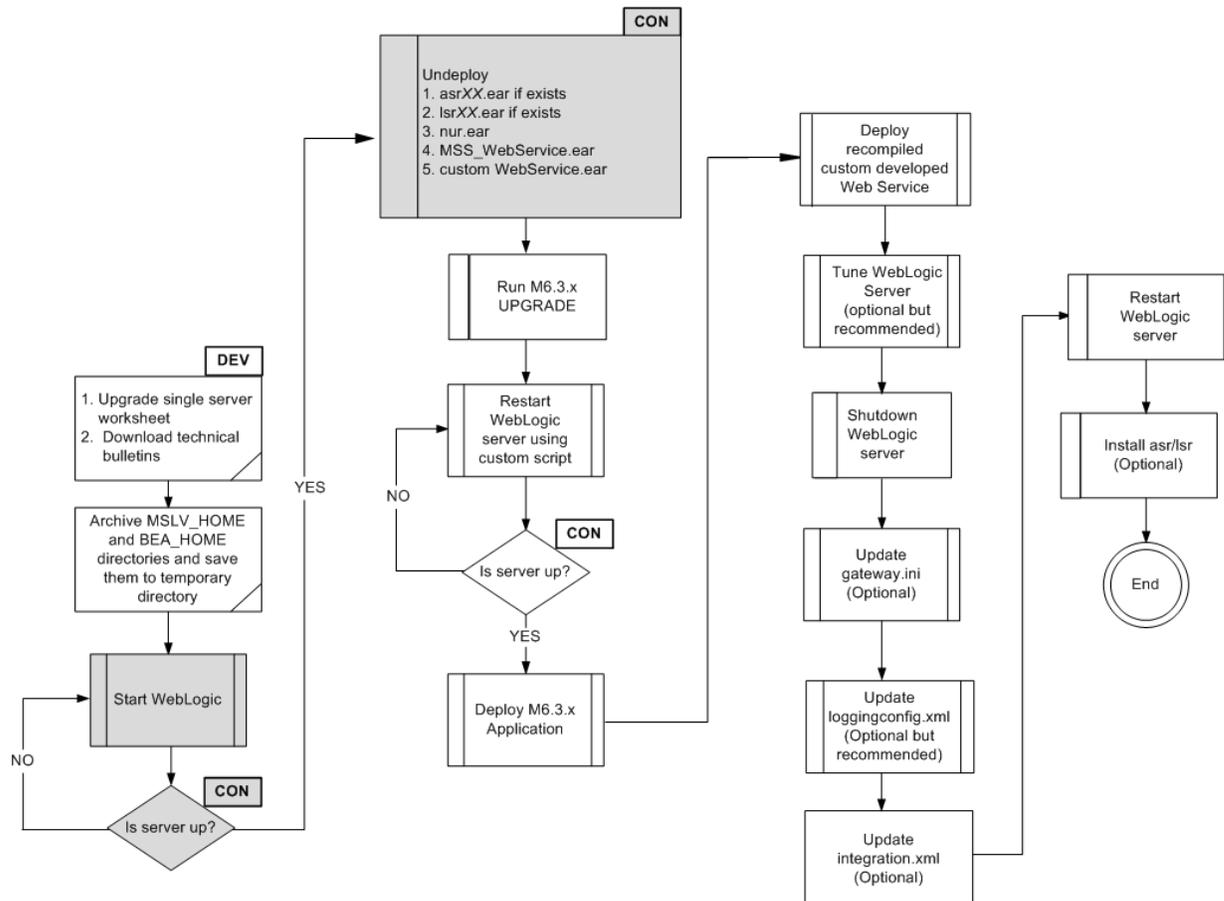
To undeploy previously installed applications:

1. Start the WebLogic server and log in to the WebLogic Server Administration Console.

2. To undeploy the application, do the following:

    a. From the Domain Structure tree, click **Deployments**.

    b. In the Change Center pane, click **Lock & Edit**.

    c. From the Summary of Deployments pane, go to the Control tab and click the check box for **nur.ear**.

    d. Click **Stop** and select **Force Stop Now**.

    e. Click **Delete**.

    f. Click **Yes** to delete the deployment.

    g. In the Change Center pane, click **Activate Changes**.

3. Repeat step 2 for each application that is to be deleted, refer to the following list:

    •   asr*XX*.ear (if deployed)

    •   lsr*XX*.ear (if deployed)

    •   custom Web Service EAR

- • MSS_WebService.ear

Installing the Upgrade

The highlighted sections of Figure 6-5 show the steps for installing the upgrade.

Figure 6-5   Installing the Upgrade
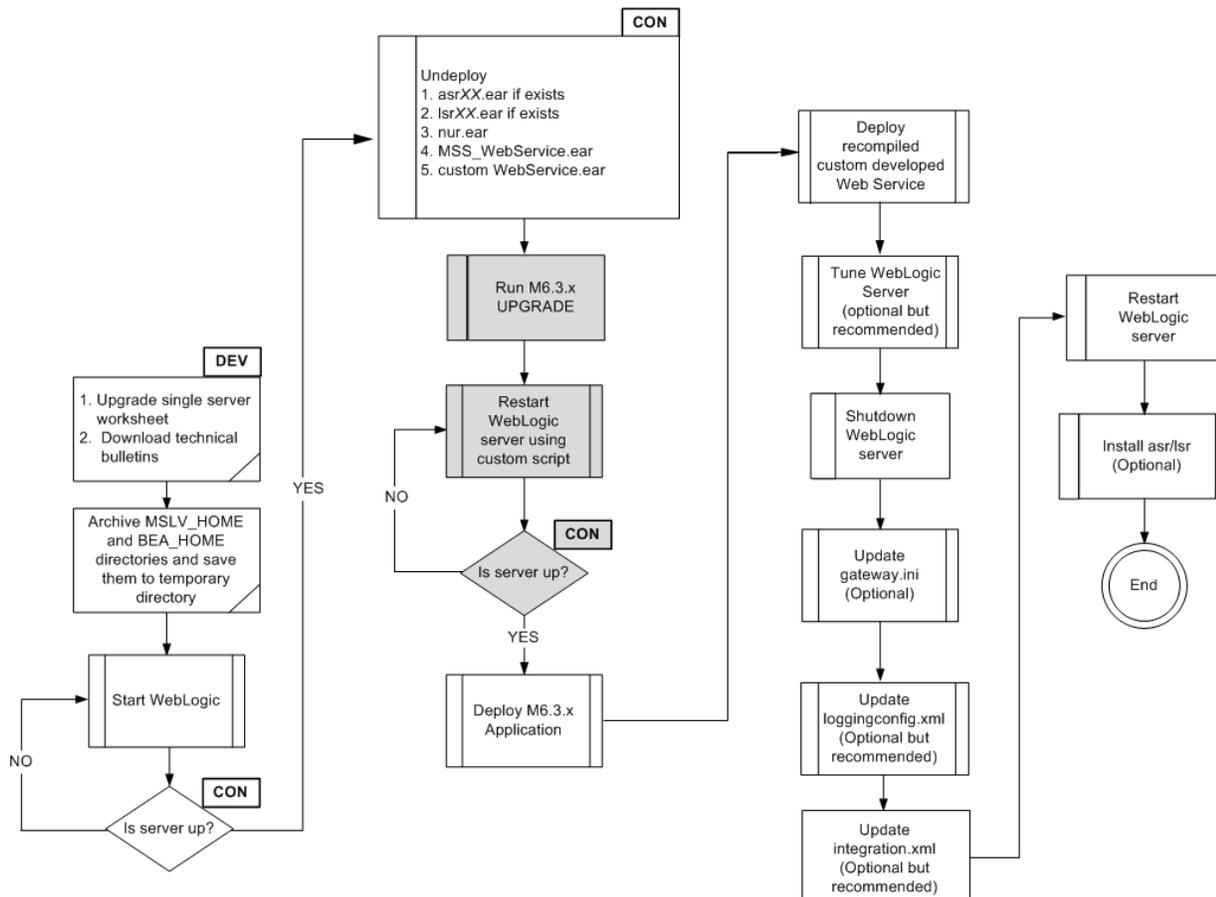
To install the upgrade, do the following:

1. From the directory where the maintenance release or patch file was downloaded, enter the following command:

   `java -jar MSS.R`*releaseNumber*`.b`*build*`_AppServerInstaller.jar`

   where *releaseNumber* is the MSS software release version and *build* is the build number. For example:

   `java -jar MSS.R6_3.b400_AppServerInstaller.jar`

   > **✎ Note:**
   >
   > For 64-bit systems, use the following java_options parameter: **-d64**.

The Select MetaSolv home directory window appears.

2. From the **Look In** list, click the down arrow and select a directory in which the installer files can be stored and used during the installation process, then click **Select**.

A directory named **installer** is automatically created in the selected directory. Oracle recommends choosing your *MSLV_Home* directory for this task.

The installer auto-launches the installation process by invoking **setup.sh** (UNIX/ Linux) or **setup.cmd** (Windows) in the *MSLV_Home/***installer** directory.

Worksheet references and example values:

Field name	Worksheet reference number	Example value
File Name (MSLV_Home)	COMM-0090	/opt/m63Single/single

The Oracle Communications MetaSolv Solution Installation window appears.

3. Click **Next**.

The Oracle Communications MetaSolv Solution Installation - Choose Install Type window appears.

4. Select **Upgrade** and click **Next**.

The Oracle Communications MetaSolv Solution Installation - Upgrade Select Server window appears.

5. In the **MetaSolv Home** field, enter the path and name of the MetaSolv home directory or click **Browse** to navigate to the directory.

All the remaining fields (except the **Pass** field) are auto-populated with the values you specified during full installation.

6. In the **Pass** field, enter the password for the administration server.

Worksheet references and example values:

Field name	Worksheet reference number	Example value
Admin Host	Admin-0250	srvrchscal
Port#	Admin-0260, Admin-0270	7001 (HTTP port), 7002 (HTTPS port)
User ID	COMM-0020	weblogic
Pass	COMM-0030	*password*

7. Click **Go**.

The installer queries the Admin Host machine and returns with values you entered during the configuration of the WebLogic domain. This process can take a few moments.

If the domain does not have a JAX-WS template applied, then the following message is displayed:

```
Please update the domain with the required JAX-WS Extension template and restart
the installation.
```

Please exit the installer and upgrade the domain by applying the **WebLogic Advanced Web Services for JAX-WS Extension** template and optionally the **WebLogic JAX-WS SOAP/JMS Extension** template. Retry the installation again after selecting the appropriate template(s):

- WebLogic Advanced Web Services for JAX-WS Extension Template (Required)

- WebLogic JAX-WS SOAP/JMS Extension Template (Optional)

The Oracle Communications MetaSolv Solution Installation window appears with the domain and any servers in the domain appearing in the left pane.

8. Select the server in the left pane.

9. Click **Install**.

   The Installation Summary window appears.

10. After the installation completes, the Installation Complete window appears.

    The installer installs the appropriate MSS files to the server. When the files are installed, the location of the startup file created for the server is displayed.

    > **Note:**
    >
    > Do not exit the installer.

11. Note the location of the startup file for the application server, then minimize the installer window.

12. Shut down the server, and restart it using the custom script installed by the installer and listed on the window.

    To start the servers, navigate to the *m63domain* directory. At the command prompt, enter the command:

    For UNIX/Linux:

    ```
    startmslv01.sh
    ```

    For Windows:

    ```
    startmslv01.cmd
    ```

    To shut down the servers, navigate to the *m63domain* directory. At the command prompt, enter the command:

    For Unix/Linux:

    ```
    stopmslv01.sh
    ```

    For Windows:

    ```
    stopmslv01.cmd
    ```

> **Note:**
>
> To start or stop the administration server and managed servers (in a cluster environment) using the SSL port, you must add an **s** after **http** in the ADMIN_URL argument in the startup/stop server scripts for the administration server and for each managed server. For example:
>
> ```
> https://host_name:admin_sslport
> ```

13. Start the WebLogic Server Administration Console by typing the following information into the **Address** field of Internet Explorer:

```
http://host_admin:port number/console
```

You can monitor the deployment from the console. To check the servers, click **Servers** in the left pane of the Console, and the right pane will show the status of all servers.

Deploying the Application

The highlighted sections of Figure 6-6 show the steps for deploying the upgrade.

Figure 6-6   Deploying the Application

To deploy the upgrade, do the following:

1. After the startup commands have been run and the application server has been started, maximize the installer window and click **Deploy Application**.

   The Oracle Communications MetaSolv Solution Installation window appears listing the server you can select for deployment.

   This process can take a few moments. If the server is not started, a status appears on the window indicating the installer is waiting for the server to be in running mode. When the server is in running mode, you can begin the deployment.

2. Select a server in the Target Servers list box, and click **Deploy**.

   The deployment process begins. You can follow the progress of the deployment by viewing the text that appears in the right pane of the installation window.

   When the deployment is complete, the Deployment Completed window appears.

3. Click **OK**.

4. Click **Exit**.

   The Exit? window appears.

5. Click **OK** to exit.

6. Continue with the steps in "Completing Post-Upgrade Tasks".

Completing Post-Upgrade Tasks

The highlighted sections of Figure 6-7 show the steps for completing post-upgrade tasks.

Figure 6-7   Completing Post-Upgrade Tasks
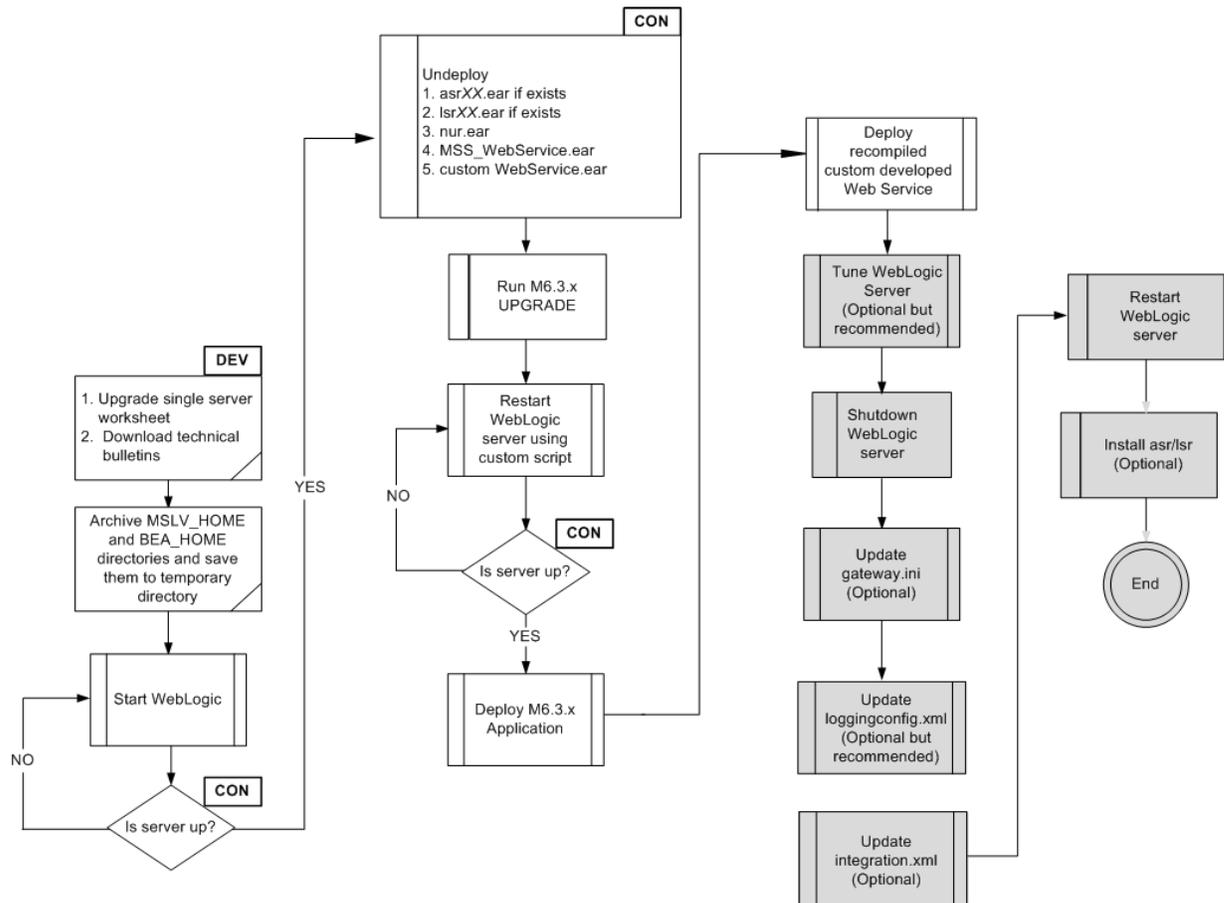
To complete the post-upgrade tasks, do the following:

1. Tune the Oracle WebLogic server.

   See "Tuning Servers For Performance" for information on tuning.

2. Shut down the Oracle WebLogic Server and update the following files:

   • **gateway.ini file.**

   • **integration.xml file.**

   • **loggingconfig.xml**

   See "Configuration Files" for more information.

3. Start the Oracle WebLogic Server.

4. Run **TBSGraphicsLoad.exe** from a client workstation to load specific graphics to the database. See "Loading New and Updated Graphics to the Database" for more information.

5. Re-install LSR or ASR, if required.

Clustered Server Upgrade Basic Steps

To upgrade the clustered server:

1. Prepare for the upgrade, which includes downloading files and collecting information.

2. Install and deploy MSS 6.3.*x*.

3. Complete the post-upgrade tasks.

Clustered Server Upgrade

Follow the procedures in this section to upgrade the clustered servers.

Preparing for the Upgrade

The highlighted sections of Figure 6-8 show the steps for preparing for the upgrade.

Figure 6-8   Preparing for the Upgrade
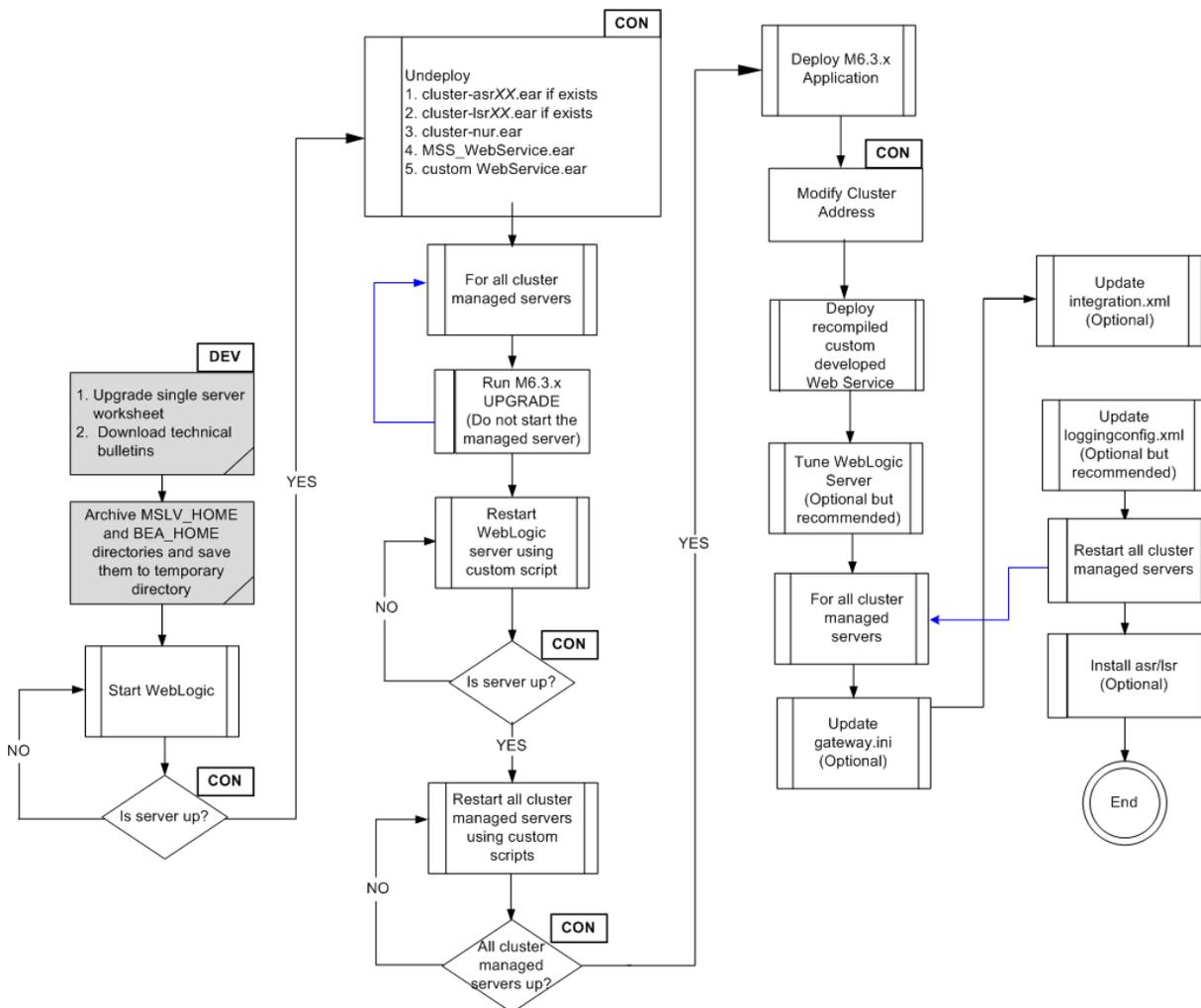
To prepare for the upgrade:

1. Download the MSS upgrade (either a maintenance release or a patch) from the Oracle software delivery website.

2. FTP the MSS upgrade file to the target server machine.

3. Complete the appropriate single server worksheets in Appendix C.

4. Archive the *MSLV_Home* and *MW_Home* directories, on the administration server and all clustered servers, and save the archive files to a temporary directory.

Undeploy Previously Installed Applications

The highlighted sections of Figure 6-9 show the steps for undeploying previously installed applications.

Figure 6-9   Undeploying Applications
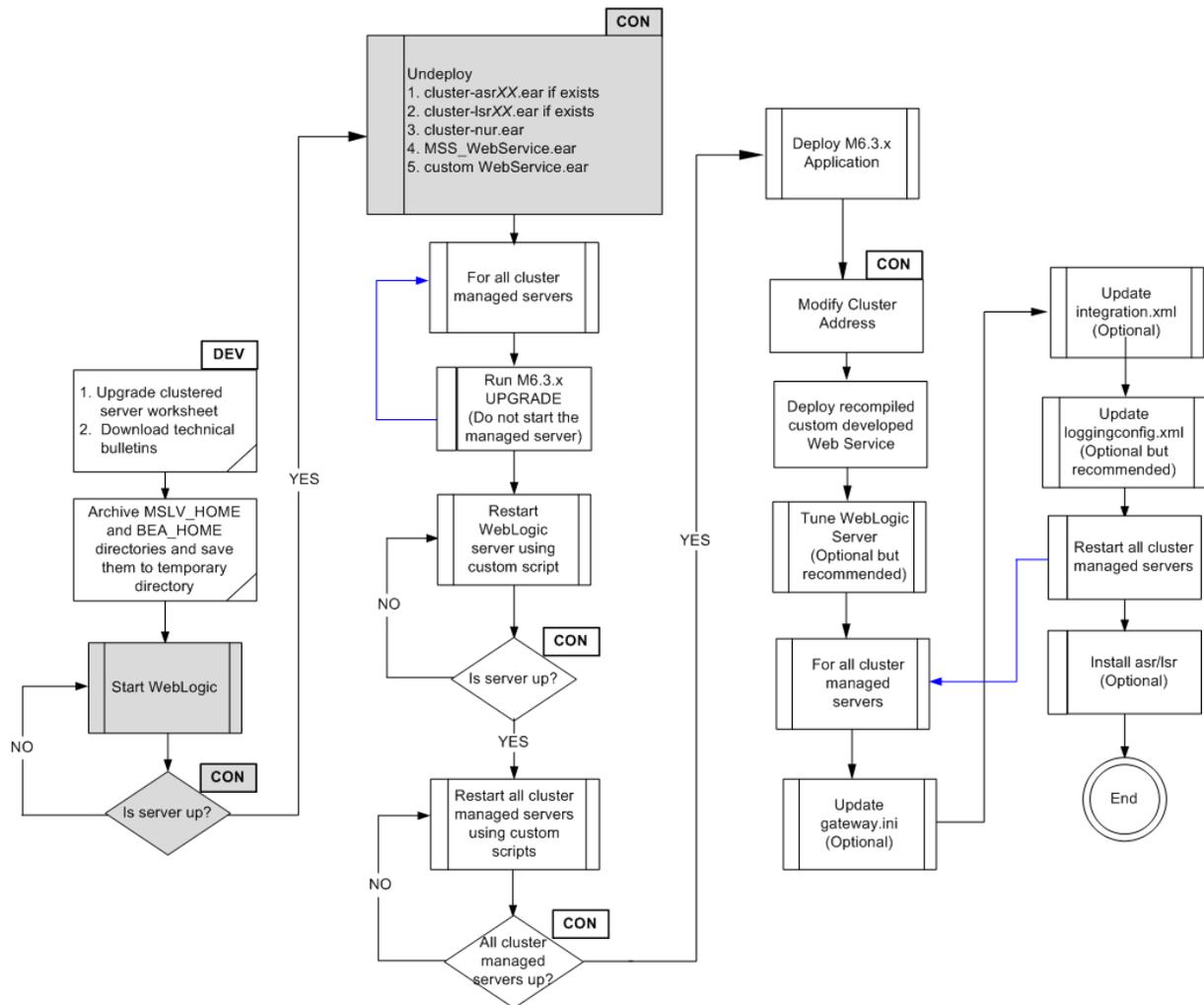
To undeploy previously installed applications:

1. Start the WebLogic server and log in to the WebLogic Server Administration Console.

2. Verify that all the clustered servers are running.

   a. From the Domain Structure tree, expand **Environment** and click **Servers**.

3. To undeploy the application, do the following:

   a. From the Domain Structure tree, click **Deployments**.

   b. In the Change Center pane, click **Lock & Edit**.

   c. From the Summary of Deployments pane, go to the Control tab and click the check box for **nur.ear** (or **cluster-nur.ear**).

   d. Click **Stop** and select **Force Stop Now**.

   e. Click **Delete**.

   f. Click **Yes** to delete the deployment.

   g. In the Change Center pane, click **Activate Changes**.

4. Repeat step 3 for each application that is to be deleted, refer to the following list:

   • asr*XX*.ear (if deployed)

   • lsr*XX*.ear (if deployed)

   • Custom Web Service EAR

   • MSS_WebService.ear

Installing the Upgrade

The highlighted sections of Figure 6-10 show the steps for installing the upgrade.

Figure 6-10   Installing the Upgrade
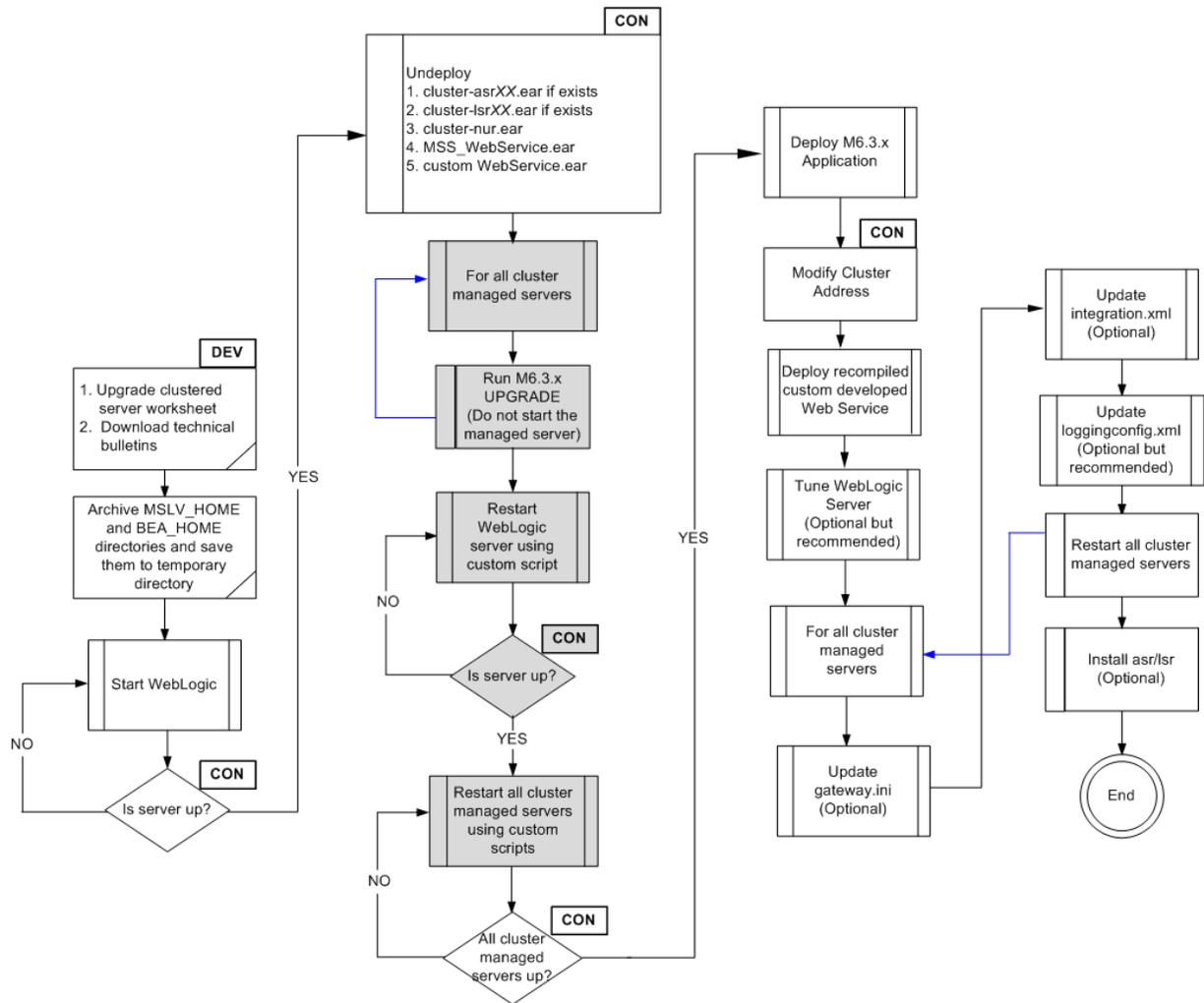
To install the upgrade, do the following:

1. For each clustered server, from the directory where the maintenance release or patch file was downloaded, enter the following command:

   `java -jar MSS.R`*releaseNumber*`.b`*build*`_AppServerInstaller.jar`

   where *releaseNumber* is the MSS software release version and *build* is the build number. For example:

   `java -jar MSS.R6_3.b400_AppServerInstaller.jar`

   > ✎ **Note:**
   >
   > For 64-bit systems, use the following java_options parameter: **-d64**.

   The Select MetaSolv home directory window appears.

2. From the **Look In** list, click the down arrow and select a directory in which the installer files can be stored and used during the installation process, then click **Select**.

A directory named **installer** is automatically created in the selected directory. Oracle recommends choosing your *MSLV_Home* directory for this task.

The installer automatically starts the installation process by invoking **setup.sh** (UNIX/Linux) or **setup.cmd** (Windows) in the *MSLV_Home/***installer** directory.

Worksheet reference and example value:

Field name	Worksheet reference number	Example value
File Name (MSLV_Home)	COMM-0090	/opt/m63Single/single

The Oracle Communications MetaSolv Solution Installation window appears.

3. Click **Next**.

The Oracle Communications MetaSolv Solution Installation - Choose Install Type window appears.

4. Select **Upgrade** and click **Next**.

The Oracle Communications MetaSolv Solution Installation - Upgrade Select Server window appears.

5. In the **MetaSolv Home** field, enter the path and name of the MetaSolv home directory or click **Browse** to navigate to the directory.

All the remaining fields (except the **Pass** field) are auto-populated with the values you specified during full installation.

6. In the **Pass** field, enter the password for the administration server.

Worksheet references and example values:

Field name	Worksheet reference number	Example value
Admin Host	Admin-0250	srvrchscal
Port#	Admin-0260, Admin-0270	7001 (HTTP port), 7002 (HTTPS port)
User ID	COMM-0020	weblogic
Pass	COMM-0030	*password*

7. Click **Go**.

The installer queries the Admin Host machine and returns with values you entered during the configuration of the WebLogic domain. This process can take a few moments.

If the domain does not have a JAX-WS template applied, then the following message is displayed:

```
Please update the domain with the required JAX-WS Extension template and restart
the installation.
```

Please exit the installer and upgrade the domain by applying the **WebLogic Advanced Web Services for JAX-WS Extension** template and optionally the

WebLogic JAX-WS SOAP/JMS Extension template. Retry the installation again after selecting the appropriate template(s):

- WebLogic Advanced Web Services for JAX-WS Extension Template (Required)
- WebLogic JAX-WS SOAP/JMS Extension Template (Optional)

The Oracle Communications MetaSolv Solution Installation window appears with the domain and any servers in the domain appearing in the left pane.

8. Select the server in the left pane.

9. Click **Install**.

   The Installation Summary window appears.

10. After the installation completes, the Installation Complete window appears.

    The installer installs the appropriate MSS files to the server. When the files are installed, the location of the startup file created for the server is displayed.

> **Note:**
>
> Do not exit the installer.

11. Note the location of the startup file for the application server, then minimize the installer window.

12. Repeat steps 1 through 11 for all clustered server machines.

13. Shut down the administration server, and restart it using the custom script installed by the installer and listed on the window.

    To start the servers, navigate to the *m63domain* directory. At the command prompt, enter the command:

    - For UNIX/Linux:

      ```
      startmslv01.sh
      ```

    - For Windows

      ```
      startmslv01.cmd
      ```

    To shut down the servers, navigate to the *m63domain* directory. At the command prompt, enter the command:

    - For UNIX/Linux:

      ```
      stopmslv01.sh
      ```

    - For Windows

      ```
      stopmslv01.cmd
      ```

> **Note:**
>
> To start or stop the administration server and managed servers (in a cluster environment) using the SSL port, you must add an **s** after **http** in the ADMIN_URL argument in the startup/stop server scripts for the administration server and for each managed server. For example:
>
> ```
> https://host_name:admin_sslport
> ```

14. Start the WebLogic Server Administration Console by typing the following information into the **Address** field of Internet Explorer:

```
http://host_admin:port number/console
```

You can monitor the deployment from the console. To check the servers, click **Servers** in the left pane of the Console, and the right pane will show the status of all servers.

15. Restart all the clustered servers using the custom scripts installed by the installer and listed on the window.

16. Verify that all the clustered servers are running.

   a. From the Domain Structure tree, expand **Environment** and click **Servers**.

Deploying the Application

The highlighted sections of Figure 6-11 show the steps for deploying the upgrade.

Figure 6-11   Deploying the Application

To deploy the upgrade, do the following:

1. After the startup commands have been run and the application server has been started, maximize the installer window and click **Deploy Application**.

   The Oracle Communications MetaSolv Solution Installation window appears listing the server you can select for deployment.

   This process can take a few moments. If the server is not started, a status appears on the window indicating the installer is waiting for the server to be in running mode. When the server is in running mode, you can begin the deployment.

2. Select a server in the Target Servers list box, and click **Deploy**.

   The deployment process begins. You can follow the progress of the deployment by viewing the text that appears in the right pane of the installation window.

   When the deployment is complete, the Deployment Completed window appears.

3. Click **OK**.

4. Click **Exit**.

The Exit? window appears.

5. Click **OK** to exit.

6. From the WebLogic Server Administration Console, modify the cluster address by performing the following:

    a. From the Domain Structure tree, expand **Environment** and click **Clusters**.

    b. Click the cluster name.

       The **Configuration** tab and the **General** tab are selected by default.

    c. Change the SSL port for the cluster address to a DNS entry containing all clustered servers' listening IP addresses. All clustered servers in the production environment should listen on the same port. If not, navigate to **Servers**, select each clustered server, click the **Configuration** tab followed by the **General** tab, and change the **Listen Port**. Modify the **JNDI** URL in the **gateway.ini** file for each clustered server.

7. Continue with the steps in "Completing Post-Upgrade Tasks".

Completing Post-Upgrade Tasks

The highlighted sections of Figure 6-12 show the steps for completing post-upgrade tasks.

Figure 6-12   Completing Post-Upgrade Tasks
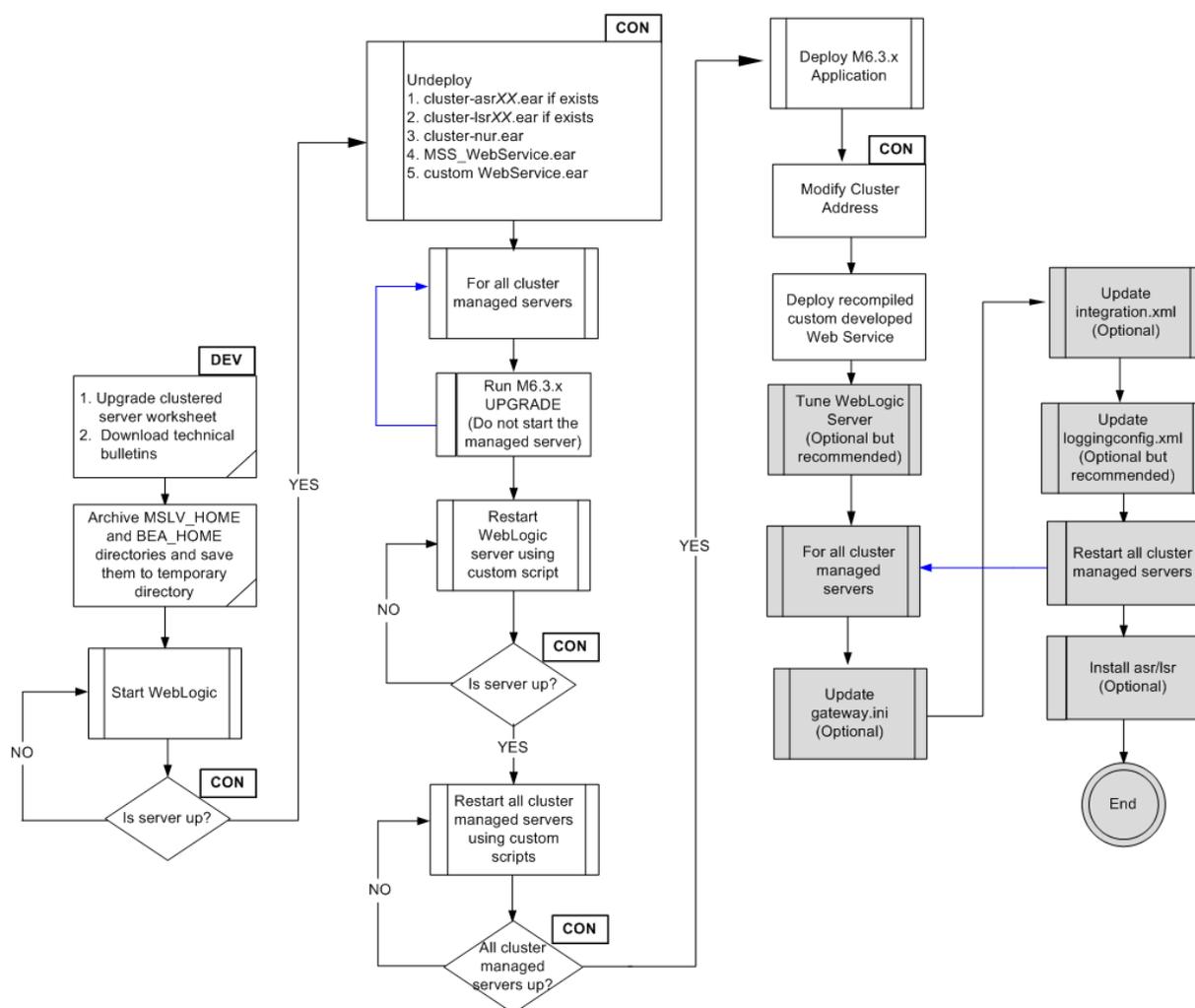
To complete the post-upgrade tasks, do the following**:**

1. Tune the Oracle WebLogic server.

2. See "Tuning Servers For Performance" for information on tuning.

3. Start the WebLogic Server Administration Console and in the left pane under your domain, click **Clusters**, and then click the cluster.

4. Change the cluster address to the DNS host name.

> ✎ **Note:**
>
> Do *not* use the comma-separated list of single address host names or IP addresses in a production environment. These can be used in a development or test environment

5. Shut down the Oracle WebLogic Server and update the following files:

- **gateway.ini file.**

- **integration.xml file.**

- **loggingconfig.xml**

See "Configuration Files" for more information.

6. Restart all cluster managed servers.

7. Run **TBSGraphicsLoad.exe** from a client workstation to load specific graphics to the database. See "Loading New and Updated Graphics to the Database" for more information.

8. Re-install LSR or ASR, if required.

Updating Client Workstations

If you are manually installing and updating client workstations, a maintenance release or patch update to the workstation needs to be done manually the first time a user logs on to MSS after the maintenance release or patch has been installed on the application server.

7

Installing The Client Workstation

This chapter explains how to install the client application onto your workstation. You need the client installed to complete post installation tasks for the database and application server installations.

This chapter also provides information on distributing the client application to users across a network.

Installation Methods

You can distribute the client application to workstations in the following ways:

- By using a third-party software product such as Microsoft SMS.
- By copying the compressed client CAB files stored on the application server to a location where you can expand them for users to copy to client workstations or use directly.

Editing Internet Explorer 11 Registry Settings

By default, Internet Explorer (IE) 11 uses WINDOWLESS SELECT control and hence you can view all the values in a drop-down list but not select them. To select a value from the drop-down list, add the WINDOWLESS Select Control value to the IE 11 registry settings.

To edit the registry settings:

1. Open **cmd.exe**.

2. Enter the following:

    ```
     "REG ADD "HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl
    \FEATURE_USE_WINDOWEDSELECTCONTROL" /V tbs.exe /T REG_DWORD /F /D 1"
    ```

    Upon successful completion, The operation completed successfully message appears.

Installing the Client Application Manually

The following procedure explains how to install the core MSS application. It does not include any utility applications.

To install the client application manually:

1. Create a directory in the location where the client installation will be placed.

2. Copy the following files from the listed application server directories to the client installation location.

    - **/appserver/cab**

- – All CAB files
- – expand_mss.cmd
- • **/appserver/config**
  - – jmaster.ini
  - – lerg.ini
  - – npasplit.ini
  - – tbs.ini
  - – tbs_util.ini
- • **/appserver/gateway**
  - – gateway.ini

> **Note:**
>
> If you are copying the files using the FTP site, use the following modes for different file types:
>
> * CAB files: Binary mode
> * CMD, XML, and INI files: ASCII mode

3. Run **expand_mss.cmd** using the Run option on the Windows Start menu.

Starting the MSS Client

Start the client using one of the following procedures:

- • On the MSS Start page, click **MetaSolv Solution**.
- • From the Start menu select **Programs**, select **MetaSolv**, select **MetaSolv Solution v.6.3.**

  If you installed manually, you must add the menu option to the Start menu in Windows to start MetaSolv Solution.
- • Double-click the executable file (**tbs.exe**) located in the MSS installation directory on the workstation.
- • Users can create a desktop shortcut to start the application after installation. The following example shows how the http:// address for a customized ZAC page with links might look when distributed to users.

  `http://host_server_name:port_number/HTML page?app=mss`

  or in cluster or load balancer environment:

  `http://load_balancer_virtual_IP_address:port_number/HTML page?app=mss`

Tools and Utilities

This section describes special considerations for MSS tool and utility applications. See *MetaSolv Solution System Administrator's Guide* for information on using these applications.

NPA NXX Split Utility

Before you can run this application, you must:

- Modify the INI file
- Create Oracle tables by applying the latest MSS maintenance release

The following sections explain how to complete these tasks.

Modifying the NPASplit.ini File

Before running the utility, you must customize the **npasplit.ini** file. The file is set up identically to the **tbs_util.ini** file in the client installation directory folder, so the logon database name and Oracle SID can be copied from that file.

To modify the **npasplit.ini** file:

1. Locate the file in the client installation directory and open it in a text editor.

2. Change the *Example1* text in the Profiles section to the name the users will pick from the **Database** drop-down box in the initial logon window.

   Any changes must match the title of the Profile listed in brackets that appears later in the file (for example: **[Profile Example1]**). Additional profiles can also be added in the same manner.

3. Change the value in the **ServerName** field to the Oracle SID shortcut in the **TNSNames.ora** file.

   The easiest method of finding this information is in the **tbs_util.ini** file (for example:

   ```
   ServerName=@EXAMPLE1
   ```

4. Save the **npasplit.ini** file with these changes.

Creating NPA NXX Split Utility Oracle Tables

The utility uses Oracle tables that are not found in the MSS database. To ensure that you have the appropriate Oracle tables for the NPA Split Utility, apply the latest MSS maintenance release. These tables must be created prior to the execution of a split.

To create the tables, do the following:

1. Download the **npasplit.cab** and **expand_mss.cmd** files from the *MetaSolv_Home/server_name***/appserver/cab** directory, on the WebLogic Administration server, to a directory on the client workstation.

2. On the client workstation, run the **expand_mss.cmd** file to expand the **npasplit.cab** file.

3. Connect to SQL*Plus and run the following script:

   - **Install.sql**

> **Note:**
>
> There is also an **Uninstall.sql** file available to undo the changes, if necessary.

MetaSolv Solution Utilities

Copy the appropriate files download to your workstation and the logon window appears.

If you are installing manually, copy the appropriate files into the client installation directory for MSS. See Table 7-1 for information on which files are needed for MSS Utilities.

If you want to run the Purge utility from a client workstation, you must install the Oracle 10.2.0.4+ client on the workstation to establish a connection to the database.

> **Note:**
>
> Ensure that you have added the DB instance entry in the **TNSNames.ora** file on the workstation.

Background Processor

Oracle recommends installing this application on a separate machine. This application has two executables:

*   Job Manager - is installed on a client workstation to view and manage jobs being processed
*   Job Master - is installed on a separate machine to do processing

See *MetaSolv Solution System Administrator's Guide* for complete information on the Background Processor.

This application requires the Oracle client.

See Table 7-1 for information on which files are needed for this application.

Location and Routing Gateway

Copy the appropriate files into the client installation directory for MSS. See Table 7-1 for information on which files are needed for this application.

Installing a Utility to a Separate Installation Directory

Oracle recommends installing MSS applications in the same directory on the workstation. The exception to this rule is the Background Processor, which should be installed in its own directory on a separate machine.

You can install an application in a directory other than the MSS installation directory if you choose. If you use this method, you must make sure the INI file for the application you are copying is in the same installation directory as the application. If you install manually, make sure that you edit the INI file for the utility you install to point to the appropriate application server.

Table 7-1 lists the CAB, INI, and XML files required for each application.

Table 7-1   MetaSolv Solution Application Files

Application	CAB file(s) required	INI files required	Install to
MSS core application	app.cab dll.cab pbvm.cab mapping.cab	tbs.ini	Client installation directory
Job Manager (Background Processor)	jobmgr.cab pbvm.cab dll.cab	jmaster.ini	Machine dedicated to running this application
Job Master (Background Processor)	app.cab jobmstr.cab pbvm.cab dll.cab	jmaster.ini	Machine dedicated to running this application
Location and Routing Gateway	lerg.cab pbvm.cab dll.cab	lerg.ini	Client installation directory
MetaSolv Solution Utilities	utility.cab pbvm.cab dll.cab	tbs_util.ini	Client installation directory
NPA NXX Utility	npasplit.cab pbvm.cab dll.cab	npasplit.ini	Client installation directory

8

Performing Post-Installation Tasks

This chapter explains tasks that you must perform once the database, the application servers, and the first client installation have been completed.

See *MetaSolv Solution System Administrator's Guide* for more information on ongoing administration and maintenance tasks.

Verifying the Database

To verify the database, you must have Oracle Communications MetaSolv Solution (MSS) Utilities installed.

Run the Database (DB) Health Utility to make sure that all database objects required by MetaSolv Solution are valid, make response times quicker, and eliminate problems in processing information. While DB Health is required only after an installation, maintenance release or patch, you may use it at any time.

You can use the DB Health Utility to repair database errors.

> **✏ Note:**
>
> The DB Health Utility cannot correct errors in invalid objects, the DBA must correct these errors. The DB Health Utility will attempt to grant privileges, create public synonyms and enable disabled objects.

The DB Health Utility can also generate a DB Status Report, which provides statistics vital to the health of the database.

See the discussion on using the DB Health Utility in the *MetaSolv Solution System Administrator's Guide* for detailed instructions.

Loading New and Updated Graphics to the Database

A utility named TBS Load Graphic Images loads new and updated graphics to the MSS database. You must run this utility one time, from any client workstation that has MSS Utilities installed, to update the database.

To load graphics to the database:

1. Open the MetaSolv Solution directory on a client workstation and double-click **TBSGraphicLoad.exe**.

2. The TBS Load Graphics Images utility appears minimized on the status bar. Click the icon on the status bar to display the utility. The TBS Load Graphics Images window appears.

3. Enter your user ID and password.

4. Enter the name of the database to which graphics are being loaded.

5. Click **Start**.

Once you run this file, subsequent attempts to run it have no effect on the database.

Loading Preferences to the Database

To ensure that all preferences have a value in the database after a first time installation, you must open the Preferences window. This causes any preferences that are not currently in the database to be added with the MSS default value.

To load preferences to the database:

1. On the MetaSolv Solution Navigation Bar, click **Application Setup**, then click **Preferences**.

   The Preferences window appears.

2. Click **Close**.

   Any preferences in this window not already defined in the database are included with default values.

   If a preference is added through an upgrade or a patch, you must open the Preferences window, locate the preference, and configure it with the appropriate value for the feature to which it applies.

Compiling Invalid Objects for Oracle Database

Run the DBHealth utility, from a client machine, to ensure that there are no invalid objects in the Oracle Database.

1. Navigate to the *MSLV_Home* directory and double-click **tbs_util.exe**.

   This starts MetaSolv Solution Utilities.

2. When the logon window appears, log on as **ASAP**.

3. In MetaSolv Solution Utilities, click **DBHealth** on the toolbar, then click the **Compile Invalid Objects** tab and click **Execute**.

   This recompiles any invalid procedures. If invalid procedures remain, click **Execute** again.

4. Select any of the tabs in the following list that have a value greater than zero and click the **Execute** button.

   • Grant Privileges

   • Create Public Synonyms

   • Enable Disabled Objects

   > ✎ **Note:**
   >
   > It is not necessary to recompile the Analyze Statistics tab at this time.

5. Exit DBHealth.

User Authentication

User authentication is the process that allows a user to log on and use MSS. For user authentication, MSS uses an external security provider to validate the user ID and password. MSS can support a variety of security providers. MSS system administrators must decide which security provider to use to validate users. The options available include authentication by:

- Oracle Database
- Oracle WebLogic Server
- A third-party software solution

Oracle Database Authentication

Oracle software provides the default user authentication.When Oracle database is used for user authentication, the user ID and password are validated using a standard SQL connect. The database performs the lookup to determine if the user ID is valid and returns the result to MSS. If the lookup is successful, the user is allowed to enter the system. If the lookup is not successful, the user receives an error message.

No changes are required to the default installation of MSS or Oracle WebLogic Server to use Oracle database authentication.

Oracle WebLogic Authentication

Oracle WebLogic Server provides an internal LDAP server and the ability to connect to other external providers such as Microsoft's Active Directory or another LDAP server. This authentication method has the advantage of being able to provide a common user ID and password for MSS as well as other applications.

The Oracle WebLogic Server authentication option requires an authentication provider. The default choice is the internal Oracle LDAP database. However, Oracle WebLogic Server also supports Microsoft Active Directory, Open LDAP providers, IPlanet, and Novell. Refer to the Oracle WebLogic Server security documentation for a description of capabilities for each of these providers. See the Oracle WebLogic Server documentation for more information.

To enable Oracle WebLogic Server authentication, configuration changes must be made to the base MSS installation. MSS uses the JEE JAAS authentication standard to connect to Oracle WebLogic. The changes that are outlined here enable the Java VM to load the correct classes. After you complete the changes, restart the server for the changes to take effect.

To enable Oracle WebLogic Server authentication:

1. Locate the JRE Security folder included in the *JAVA_Home* directory.

   Default paths:

   For UNIX/Linux: *JAVA_Home/***jre/lib/security**

   For Windows: *JAVA_Home***jre\lib\security**

> **✎ Note:**
>
> Ensure that the *JAVA_Home*/**jre/lib/security** folder has write permissions.

2. Using any text editor, edit the text file called **mss_jaas.config** in the **Security** directory.

   This file creates a pointer to the class that accesses Oracle WebLogic Server for security functions. The file needs to have the exact contents defined below and it must appear with the text between the braces on one line.

   ```
   MSS {
   weblogic.security.auth.login.UsernamePasswordLoginModule required
   debug=false;
   };
   ```

3. Edit the **java.security** file to enable the external security call. Uncomment the following line:

   ```
   login.config.url.1=file:${java.home}/lib/security/mss_jaas.config.
   ```

4. Configure the Oracle WebLogic Server security realm.

   During this step, you must choose the Oracle WebLogic Server authentication mechanism. You have the choice of several providers distributed with the Oracle WebLogic Server software, or you can define a custom application and integrate it into the Oracle WebLogic Server installation. Refer to the Oracle WebLogic Server documentation for steps on how to accomplish this configuration.

5. Restart the server.

After the restart is completed, the MSS logon will use the Oracle WebLogic Server security configuration defined in step 4. There are several considerations for using this type of security:

- Creating a user is a two-step process.

  First, users must be added to the external security system so that authentication can be performed during the logon procedure. Refer to the Oracle WebLogic Server documentation on how to add users to the system.

  Next, users must be added to the MSS security tables. This step enables the permission functionality so that portions of the application, even individual screens, can be secured internally if necessary. See *MetaSolv Solution System Administrator's Guide* for more information.

- Oracle WebLogic Server security system users cannot be created from the MSS security window. This window only creates MSS users; it does not enable user logon.

- User IDs are limited to eight characters.

- Passwords are limited to 30 characters.

- The applications that connect to the database directly and do not use the application server cannot use this authentication method. These applications, which must continue to use the Oracle database authentication method, include the Location and Routing Gateway, MetaSolv Solution Utilities, and the NPA Split Utility.

- Group functionality is different in MSS and the external provider software, and groups are not kept in sync by the software. This task must be completed manually.

Third-party Authentication

The final alternative for user authentication is to use a third-party authentication software package. This option lets you use an enterprise security package and bypass the Oracle WebLogic Server for authentication. One reason for bypassing the Oracle WebLogic Server is that it does not directly support a security provider and you may not prefer to extend Oracle WebLogic Server to add an additional security package.

MSS allows this option because it has enabled JAAS. This is the same architecture used to enable Oracle WebLogic Server authentication. The only requirement to enable a third-party authentication provider is that the provider must have a JAAS logon module (that conforms to the Java 8 specification), or you must develop one. If the provider has a JAAS logon module, skip to the configuration section.

Developing a JAAS Logon Module

This section provides an overview of the steps required to develop a JAAS logon module. It is not a comprehensive guide. You will need to review Oracle's information about JAAS that can be accessed from java.sun.com, and you will have to review your security provider's documentation on how to provide for authentication.

The only class that needs to be developed is a logon module class. This class gets called from MSS on logon. The class must implement the LoginModule. Inside the class you develop several methods. The key method is the logon method. This method gets called on each logon. Inside this method you get the userid and password from the callback object, verify the information, and return a success or failure message. The following is a code fragment from the logon method of a sample JAAS logon module. It simply gets the userid and password and compares it to a static string of TESTUSER/TESTPASS. If it matches, it returns true.

```
NameCallback name = new NameCallback("name");
PasswordCallback pwd = new PasswordCallback("Password",false);
Callback[] calls = new Callback[2];
calls[0] = name;
calls[1] = pwd;
try {
callbackHandler.handle(calls);
} catch (Exception e) {
System.out.print(e);
}
boolean isSuccess = false;
String userId, password;
userId = name.getName();
password = String.valueOf(pwd.getPassword());

// verify the username/password

if (userId.equals("TESTUSER"))
 isSuccess = true;
if (isSuccess  &&
 password.equals("TESTPASS"))
{
// authentication succeeded!!!
isSuccess = true;
```

```
} else
   isSuccess = false;

      return isSuccess;
```

Configuring a JAAS Logon Module

If you are using a third-party JAAS logon module or a logon module you developed, you must configure the application server to use that module.

To configure a JAAS logon module:

1. Edit the **startMSLVServer** script file located in the domain directory.

    To do this, copy one of the POST_CLASSPATH lines and add your jar file to the line.

    > **Note:**
    >
    > This file gets overlaid with each service pack. Therefore, this change needs to be re-applied to the **startMSLVServer** script after each service pack.

2. Navigate to the *JAVA_Home* directory and locate the **jre/security** directory.

    Default paths:

    For UNIX/Linux: *JAVA_Home***/jre/lib/security**

    For Windows: *JAVA_Home***\jre\lib\security**

3. Using any text editor, edit the text file called **mss_jaas.config** in the security folder.

    This file creates a pointer to the class that accesses the third-party security software. The file needs to have the package name of the third-party security class, and it must appear with the text between the braces on one line. Here is an example:

    ```
    MSS {
    Sample.module.SampleJAASLoginModule required debug=false;
    };
    ```

4. Edit the **java.security** file, located in the **jre/lib/security** folder, using any text editor and uncomment the following line:

    ```
    login.config.url.1=file:${java.home}/lib/security/mss_jaas.config.
    ```

    This allows the Java runtime to find **mss_jaas.config**.

5. Configure the third-party security software.

    Refer to the security software documentation for steps on how to accomplish this configuration.

6. Restart the server.

After the restart is completed, the MSS logon authentication uses the third-party security software. See the following considerations for using a third-party solution:

*   Creating the user is a two-step process.

First, users must be added to the external security system so that authentication can be performed during the logon procedure. Refer to your third-party security system documentation on how to add users to the system.

Next, users must be added to the MSS security tables. This step enables permission functionality so that portions of the application, even individual screens, can be secured internally if necessary. See *MetaSolv Solution System Administrator's Guide* for more information.

- Third-party security system users cannot be created from the MSS security window. This window creates only MSS users; it does not enable user logon.

- User IDs are limited to eight characters.

- Passwords are limited to 30 characters.

- The applications that connect to the database directly and do not use the application server cannot use this authentication method. These applications, which must continue to use the Oracle authentication method, include: the Location and Routing Gateway, MetaSolv Solution Utilities, and the NPA Split Utility.

- Group functionality is different in MSS and the external provider software, and groups are not kept in sync by the software. This task must be completed manually.

Encrypting Network Traffic

MSS uses HTTPS to encrypt network traffic between the client and the application server; however, by default, MSS uses HTTP for client-to-server communication. To enable HTTPS for network encryption, you must change the standard installation.

The following steps apply only to applications that use the application server for its services. The applications that connect directly to the database can not use HTTPS.

To encrypt network traffic:

1. Obtain an SSL certificate.

   Typically you get this from a provider like Verisign. The provider requires a CSR to be generated from the application server. To generate the CSR, navigate to the URL:

   ```
   https://host_name:ssl_port/certificate
   ```

   where:

   - *host_name* is the name of the Administration Server machine

   - *ssl_port* is the Administration Server SSL port number

   See the Oracle WebLogic Server documentation for more information about the certificate application.

2. Configure the application server to enable HTTPS.

   Use the management console to complete the configuration. Refer to the Oracle WebLogic Server documentation and documentation from the certificate provider for details on how to complete this step. After the configuration is complete, restart the server.

3. Test the configuration by navigating to the MSS start page.

The URL for the page is:

```
https://host_name:ssl_port/main
```

where:

- *host_name* is the name of the Administration Server machine
- *ssl_port* is the Administration Server SSL port number

The page should render without any warning dialog boxes from Internet Explorer. These warnings prevent the application from working with HTTPS.

4. To start or stop the administration server and managed servers (in a cluster environment) using the SSL port, you must add an **s** after **http** in the ADMIN_URL argument in the startup/stop server scripts for the administration server and for each managed server. For example:

```
https://host_name:admin_sslport
```

5. Change the **gateway.ini** file for the application and distribute the changes to each client using any distribution method.

Under the JNDI heading, edit the URL parameter by changing:

- HTTP to HTTPS
- The port number to the SSL port number you configured

6. Configure the browser on the client workstation to allow mixed content to be displayed.

   a. Start Microsoft Internet Explorer.

   b. On the Tools menu, click **Internet Options**.

   The Internet Options window appears.

   c. On the Security tab, click **Custom Level**.

   d. For the **Display mixed content** option, click **Enable.**

   If this option is disabled, the application does not work. If you set the option to **Prompt**, the user will be prompted with each page.

Gateway Events Setup

If you use the integration server for processing the gateway events, ensure that you configure the **gateway.ini** file as follows:

1. Navigate to the *MSLV_Home***/appserver/gateway** directory and edit the **gateway.ini** file.

2. Uncomment the INTEGRATIONSERVER entry in the [ThreadProcs] section.

3. Continue with the steps given in the "Gateway Events through Integration Server" section in the *MSS System Administrator's Guide*.

Internationalization Web Service Character Set

If you use Web Services with extended character codes, you must specify the Web service character set in the startup properties using the following directives.

- Add a directive in the WebLogic Server domain environment configuration file to force proper encoding for Web services. For example:

  – setDomainEnv.cmd (Windows)

  ```
  @REM Added to force webservices to use utf-8 encoding
  set EXTRA_JAVA_PROPERTIES=%EXTRA_JAVA_PROPERTIES% -
  Dweblogic.webservice.i18n.charset=utf-8
  ```

  – setDomainEnv.sh (UNIX/Linux)

  ```
  # To force webservices to use UTF-8 encoding
  EXTRA_JAVA_PROPERTIES=${EXTRA_JAVA_PROPERTIES} -
  Dweblogic.webservice.i18n.charset=utf-8
  export EXTRA_JAVA_PROPERTIES
  ```

- Add a directive in the WebLogic Server domain startup file to force proper encoding for Web services. For example:

  – startWebLogic.cmd (Windows)

  ```
  @REM Added to force webservices to use utf-8 encoding
  set SAVE_JAVA_OPTIONS=%SAVE_JAVA_OPTIONS% -
  Dweblogic.webservice.i18n.charset=utf-8
  ```

  – startWebLogic.sh (UNIX/Linux)

  ```
  # To force webservices to use UTF-8 encoding
  SAVE_JAVA_OPTIONS="${SAVE_JAVA_OPTIONS} -
  Dweblogic.webservice.i18n.charset=utf-8"
  export SAVE_JAVA_OPTIONS
  ```

Adding Your Company Logo to the MSS My Desktop and Forms

You can add your company logo to the MSS interface as shown in Figure 8-1.

Figure 8-1   Location of Customized Company Logo in the MSS Interface
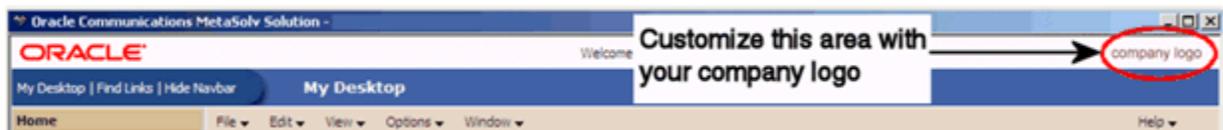
The logo has the following requirements:

- Size: Width = 100 pixels Height = 25 pixels
- File name: **imgCompanyLogo.jpg**

To add your logo to My Desktop:

1. Locate a directory named **images** in the *MSLV_Home/DOMAIN_NAME/***logo** directory.

2. Copy the company logo file with the required name (**imgCompanyLogo.jpg**) into the directory.

The image stored in this directory under the file name given appears in the Company Logo field on the My Desktop page and on the Start page for MSS users.

The following option is available if you installed MSS as a full installation. If you used the upgrade option, rather than a full installation, this option is not available.

To add your logo to MSS forms:

1. On the navigation bar, select **Application Setup**, and then **Preferences**.

   The Preferences window appears.

Figure 8-2   Preferences Window
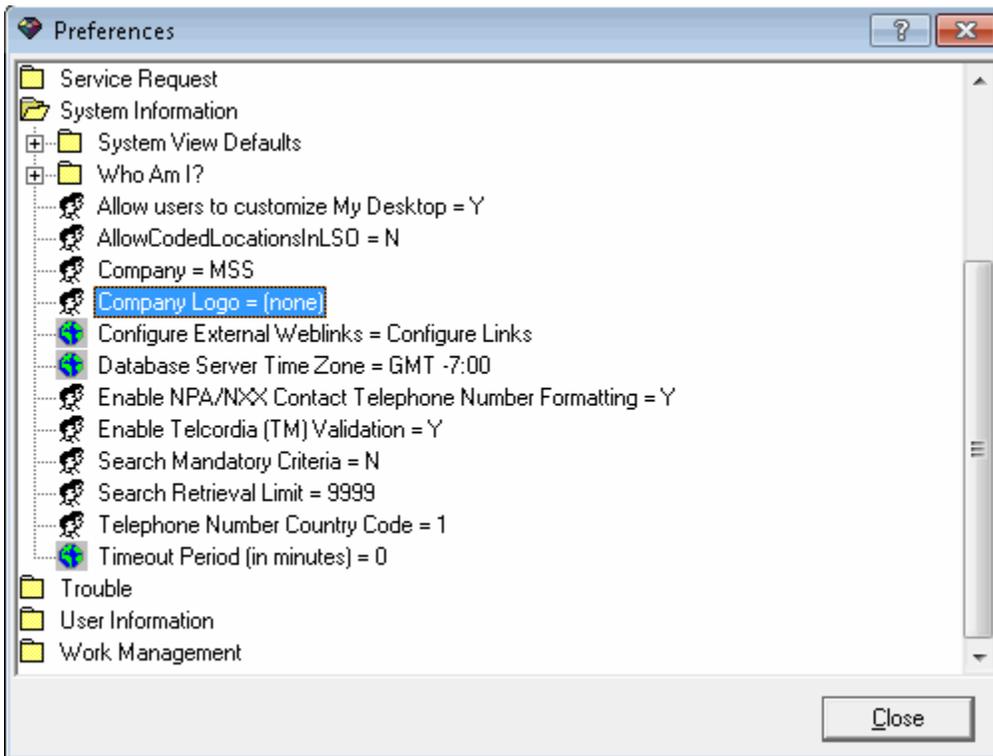
2. Expand the System Information folder.

3. Double-click Company Logo and type the path for the bitmap logo into the **Company Logo** field of the window that appears.

   The default is **None**. If you leave the default, your company logo does not appear on forms such as orders or DLRs.

4. Click **OK**.

5. Click **Close** to close the Preferences window.

What to Do Next to Secure MSS

You must implement MSS security for individual users and groups of users. You can secure portions of the user interface to specific users to prevent unintended changes. This is especially useful if users only work in a portion of the application like ordering

or connection design. See *MetaSolv Solution System Administrator's Guide* for complete information on setting up security for MSS.

9

Configuring JDBC Active GridLink Data Sources

This chapter describes how to configure the Oracle Communications MetaSolv Solution (MSS) JDBC Active GridLink (AGL) data sources to work in an Oracle Real Application Cluster (RAC) environment for MSS.

About Oracle RAC

Oracle RAC consists of two or more Oracle database instances that run on two or more clustered machines and access a shared storage device using cluster technology. The host machines for the database instances must be linked by a high-speed interconnection to form the cluster and enable communications among the nodes in the cluster.

> ✎ **Note:**
>
> For more information on configuring Oracle RAC, your clustering software, your operating system, and storage solution, see the documentation from the respective vendors.

For information using Oracle RAC with Oracle WebLogic servers, refer to the *Oracle Fusion Middleware Administering JDBC Data Sources for Oracle Weblogic Server* documentation.

Creating the JDBC Active GridLink Data Sources

A single Active GridLink (AGL) data source provides connectivity between WebLogic Server and an Oracle Database service, which may include one or more Oracle RAC clusters. An Oracle Database service represents a workload with common attributes that enables administrators to manage the workload as a single entity. You scale the number of AGL data sources as the number of services increases in the database, independent of the number of nodes in the Oracle RAC clusters.

> ✎ **Note:**
>
> MSS supports only the failover algorithm (with remote listener enabled).

You can create JDBC Active GridLink data sources by doing one of the following:

- Manually Creating the JDBC Active GridLink Data Sources

- Creating JDBC Active Data Sources by Updating the Configuration Files

JDBC Data Source Properties

JDBC data source properties include options on the data source identify and the handling of data for the database connection. Before creating data sources, you need to be familiar with this topic. For detailed information on JDBC data sources and their properties, see *Fusion Middleware Administering JDBC Data Sources for Oracle WebLogic Server* on the Oracle Help Center website at:

http://docs.oracle.com/en/middleware/middleware.html

Manually Creating the JDBC Active GridLink Data Sources

You must create the JDBC Active GridLink data sources manually. By default, the MSS installer creates the multi data sources when the Oracle RAC database is selected. A multi data source provides an ordered list of data sources to use to satisfy connection requests.

To create the JDBC Active GridLink data sources, perform the following tasks in the WebLogic Administration Console:

- Deleting the existing multi data sources. See "Deleting Multi Data Sources" for more information.
- Creating the following JDBC Active GridLink data sources:
  - mslvDataSource
  - mslvDbTraceDataSource
  - mslvNoneTxDataSource
  - mslvProcDataSource
  - mslvPSDataSource
  - mslvWSDataSource

  See "Creating Active GridLink Data Sources" for more information.
- Creating the following persistent stores:
  - mssJMSStore (and point it to mslvPSDatasource)
  - pluginstore (and point it to mslvPSDatasource)

  See "Creating Persistent Stores" for more information.
- Creating the following JMS servers:
  - mmsJMSServer (and point it to mssJMSStore)
  - pluginJMSServer (and point it to pluginstore)

  See "Creating JMS Servers" for more information.
- Creating the following JMS modules:
  - mssJMSModule
  - pluginModule

    After you create mssJMSModule and pluginModule, you must create JMS module resources (such as queues and connection factories) and create the

subdeployments for those resources. A subdeployment is a process for grouping JMS module resources and targeting them to a server instance or cluster.

See "Creating JMS Modules" for more information.

Deleting Multi Data Sources

To remove a multi data source, perform the following:

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Services**, and then click **Data Sources**.

   The Summary of JDBC Data Sources page appears.

3. Click the **Configuration** tab.

4. Select the check box beside each data source that you want to delete and click **Delete**.

Creating Active GridLink Data Sources

To create an Active GridLink data source:

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Services**, and then click **Data Sources**.

   The Summary of JDBC Data Sources page appears.

3. Click **New** and select **GridLink Data Source**.

   The JDBC GridLink Data Source Properties page appears.

4. In the **Name** field, enter **mslvDataSource**.

5. In the **JNDI** name field, enter the JNDI path to where this data source is bound. By default, the JNDI name is the name of the data source. For example, MSLVPool.

6. From the **Database Driver** list, select any one of the following database drivers, depending on the Active GridLink data source that you are creating:

   • When creating mslvDataSource and mslvWSDataSource, select **Oracle's Driver (Thin XA) for GridLink Connections Versions:Any**.

   • When creating mslvDbTraceDataSource, mslvNoneTxDataSource, mslvProcDataSource, and mslvPSDataSource, select **Oracle's Driver (Thin) for GridLink Connections; Versions:Any**.

7. Click **Next**.

   The Transaction Options page appears.

   For XA drivers, the system automatically selects the **Two-Phase Commit** protocol for global transaction processing.

   The **Supports Global Transactions** check box is selected by default.

8. (For non-XA drivers) If you selected the **Supports Global Transactions** check box, you must also select any one of the following transaction protocols for this data source:

   • Logging Last Resource

   • Emulate Two-Phase Commit

- One-Phase Commit

9. Click **Next**.

The GridLink data source connection Properties Options page appears.

10. Do one of the following:

- Select **Enter individual listener information** and click **Next**.

  The Connection Properties page appears.

  a. In the **Service Name** field, enter the name of the service.

  b. In the **Host and Port** field, enter the host and port; separate the host and the port of each listener with a colon.

  c. In the **Database User Name** field, enter the database user name.

  Table 9-1 lists the GridLink data sources, including the JNDI name, driver class name, and user name that you must specify to create each data source.

Table 9-1   GridLink Data Sources

GridLink Data Source	JNDI Name	Driver Class Name	User Name
mslvDataSource	MSLVPool	oracle.jdbc.xa.client.OracleXADataSource	APP_MSLV
mslvDbTraceDataSource	MSLVDbTracePool	oracle.jdbc.OracleDriver	APP_MSLV
mslvNoneTxDataSource	MSLVNoneTxPool	oracle.jdbc.OracleDriver	APP_MSLV
mslvProcDataSource	MSLVProcPool	oracle.jdbc.OracleDriver	APP_API
mslvPSDataSource	MSLVpsPool	oracle.jdbc.OracleDriver	APP_MSLV
mslvWSDataSource	MSLVwsPool	oracle.jdbc.xa.client.OracleXADataSource	APP_INT

  d. In the **Password** field, enter the password.

  e. In the **Confirm Password** field, enter the password again to confirm it.

  f. In the **Protocol** field, enter the protocol. For example, TCP.

  g. In the **oracle.jdbc.DRCPConnectionClass** field, enter the DRCP connection class.

  h. Click **Next**.

- Select **Enter complete JDBC URL** and click **Next**.

  a. In the **Complete JDBC URL** field, enter the JDBC URL.

  b. In the **Database User Name** field, enter the database user name.

  c. In the **Password** field, enter the password.

  d. In the **Confirm Password** field, enter the password again to confirm it.

  e. In the **Protocol** field, enter the protocol.

  f. In the **oracle.jdbc.DRCPConnectionClass** field, enter the DRCP connection class.

  g. Click **Next**.

The Test GridLink Database Connection page appears, which enables you to test a database connection before the data source configuration is finalized using a

table name or SQL statement. If required, you can test additional configuration information using the **Properties** and **System Properties** attributes.

11. Click **Next**.

    The ONS Client Configuration page appears.

12. Select the **Fan Enabled** check box to subscribe to Oracle Fan Events.

13. In the **ONS host and port** field, enter the host and port for each ONS node separated by a comma.

14. If ONS is configured to use the SSL protocol, do the following:

    a. In the **ONS Wallet File Directory** field, enter the directory of the Oracle wallet file in which the SSL certificates are stored.

    b. In the **ONS Wallet Password** field, enter and confirm the ONS wallet password.

    c. In the **Confirm ONS Wallet Password** field, enter the ONS wallet password again to confirm it.

15. Click **Next**.

    The Select Targets page appears.

16. Select the servers or clusters on which you want to deploy the data source and click **Next**.

17. Click **Finish**.

18. Repeat this procedure to create the remaining Active GridLink data sources: mslvDbTraceDataSource, mslvNoneTxDataSource, mslvProcDataSource, mslvPSDataSource, and mslvWSDataSource.

19. Proceed with "Tuning the Active GridLink Data Source".

Tuning the Active GridLink Data Source

After you create the Active GridLink data sources, you must tune each data source.

To tune each data source:

1. Log in to the WebLogic administration console.

2. In the Domain Structure tree, expand **Services**, and then click **Data Sources**.

    The Summary of JDBC Data Sources page is displayed.

3. Select the target data source (for example, *mslvDataSource1*).

    The Settings for *<DataSource>* page is displayed.

4. Click the **Connection Pool** tab.

    The Connection Properties are displayed.

5. Click **Advanced** to display additional configuration items.

6. In the **Test Table Name** field, clear the **SQL SELECT 1 FROM DUAL** entry and enter **SQL ISVALID**.

7. In the **Inactive Connection Timeout** field, enter **300**.

8. Click **Save**.

9. Click **Activate Changes**.

ORACLE

10. Repeat steps 3 through 9 to tune each data source.

Creating Persistent Stores

To create a persistent store

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Services**, and then click **Persistent Stores**.

   The Summary of Persistent Stores page appears.

3. Click **New** and select **Create JDBCStore**.

   The Create a New JDBC Store page appears.

4. Do the following:

   a. In the **Name** field, enter **mssJMSStore**.

   b. From the **Target** list, select a server instance on which you want to deploy the JDBC store.

   c. From the **Data Source** list, select **mslvPSDataSource**.

   d. In the **Prefix Name** field, specify a prefix that is added to the table name in this JDBC store.

   e. Click **Finish**.

   f. Repeat this procedure to create the **pluginstore** persistent store and point it to **mslvPSDatasource**.

Creating JMS Servers

To create a JMS server

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Services**, then expand **Messaging**, and then click **JMS Servers**.

   The Summary of JMS Servers page appears.

3. Click **New**.

   The Create a New JMS Server Properties page appears.

4. Do the following:

   a. In the **Name** field, enter **mssJMSServer**.

   b. From the **Persistent Store** list, select **mssJMSStore**.

   c. Click **Finish**.

   d. Repeat this procedure to create the **pluginJMSServer** JMS server and point it to **pluginstore**.

Creating JMS Modules

To create a JMS module:

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Services**, then expand **Messaging**, and then click **JMS Modules**.

The Summary of JMS Modules page appears.

3. Click **New**.

The Create JMS System Module page appears.

4. Do the following:

    a. In the **Name** field, enter **mssJMSModule.**

    b. (Optional) In the **Descriptor File Name** field, enter a name for module's underlying descriptor file.

    c. (Optional) In the **Location in the Domain** field, enter where you want to place the descriptor for the system module.

5. Click **Next**.

The Targets page appears.

6. Select the server instance or cluster target on which you want to deploy the JMS module, and then click **Next**.

The Add resources to this JMS system module page appears.

7. Do one of the following:

    • Click **Finish**.

    The **mssJMSModule** JMS module is created. You can create the resources for the newly created JMS module later.

    • Select the **Would you like to add resources to this JMS system module?** and click **Finish**.

    The **mssJMSModule** is created and you can now continue adding resources to the newly created JMS module.

    The Setting for mssJMSModule page appears.

8. On the **Configuration** tab, click **New**.

The Create a New JMS System Module Resource page appears.

9. Select the type of resource (such as Connection Factory, Queue, Topic, and so on) you want to create and click **Next**.

10. Enter the required information for the selected resource, from the **Subdeployments** list, select **(none)**, and click **Finish**.

> ✎ **Note:**
>
> When creating a JMS module resource, do not specify a subdeployment; instead, after creating the JMS resource, edit the resource and then specify a subdeployment for that resource. See "Configuring Subdeployments for JMS Module Resources" for more information.

11. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

12. Repeat this procedure to create the **pluginModule** JMS module.

ORACLE

Configuring Subdeployments for JMS Module Resources

After the you create the resources for the JMS module, edit the resource, and then specify a subdeployment for that resource.

To configure a subdeployment for a JMS module resource:

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Services**, then expand **Messaging**, and then click **JMS Modules**.

   The Summary of JMS Modules page appears.

3. Click mssJMS module.

   The Settings for mssJMSModule page appears.

4. On the **Configuration** tab, under **Summary of Resources**, click a resource.

   The Settings for *resource* page is displayed.

5. Click the **Subdeployment** tab.

6. From the **Subdeployment** list, select a subdeployment.

7. Click **Save**.

8. Repeat this procedure to configure subdeployments for the resources of pluginModule.

Creating JDBC Active Data Sources by Updating the Configuration Files

Creating the JDBC Active GridLink data sources by updating configuration files involves doing the following tasks in the WebLogic Administration Console:

- Encrypting Clear Text Passwords in WebLogic Server Domain Configuration Files

- Deleting Multi Data Source Instances from the config.xml File

- Modifying the Classpath for the WebLogic Server Domain

- Configuring the Connection Pool Parameters

> **✎ Note:**
>
> Before converting Multi Data Sources to Active GridLink Data Sources, you must do the following:
>
> 1. Take a backup of all Multi Data Sources
>
> 2. Take a backup of the **config.xml** file that is located in the *m63domain* **\config** directory, where *m63domain* is the name of the domain directory you specified during domain configuration.

Encrypting Clear Text Passwords in WebLogic Server Domain Configuration Files

Each Active GridLink data source is represented by a configuration XML file for the RAC domain in the *m63domain***\config\jdbc** directory. For example, **mslvWSDataSource-8065-jdbc.xml**, **mslvProcDataSource-9573-jdbc.xml**, and so on.

where:

m63domain is the name of the domain directory you specified during domain configuration.

You must encrypt the clear text passwords in each domain configuration XML file for all the data sources to protect them files from unauthorized access. You encrypt passwords using the java weblogic.security. Encrypt utility, which you must run from within the *m63domain* folder.

Ensure that you encrypt passwords for the following database users: APP_MSLV, APP_API, and APP_INT.

To encrypt clear text passwords in WebLogic server domain configuration files:

1. Change directory to your domain's bin folder.

   For example:

   ```
   cd MW_HOME\user_projects\domains\m63domain\bin
   ```

2. Run the setDomainEnv script. For example, setDomainEnv.cmd (Windows) or setDomainEnv.sh (UNIX/Linux).

3. Navigate to the *m63domain* directory and run the java weblogic.security.Encrypt utility. This utility prompts you for a password, and then displays the encrypted password.

   The following is a sample output from running this utility:

   ```
   C:\MW_HOME\user_projects\domains\m63domain>java weblogic.security.Encrypt
   Password:
   {3DES}9HWsf87pJTw=
   ```

4. Navigate to the in the *m63domain***\config\jdbc** directory.

5. Copy the encrypted passwords for all the data sources and paste these passwords in the <password> element within the XML file for each data source (mslvWSDataSource, mslvProcDataSource, mslvPSDataSource, mslvNoneTxDataSource, mslvDbTraceDataSource, and mslvDataSource).

> **✎ Note:**
>
> You can generate a new password or you can copy the password from the Multi Data Source backup.

Deleting Multi Data Source Instances from the config.xml File

To delete the multi data sources instances from the **config.xml** file:

1. Edit the *m63domain***\config\config.xml** file.

2. Remove all the instances of multi data sources.

For example, remove the entries for the following data sources: mslvDataSource1, mslvDbTraceDataSource1,mslvNoneTxDataSource1, mslvProcDataSource1, mslvWSDataSource1, mslvPSDataSource1, mslvDataSource2, mslvDbTraceDataSource2, mslvNoneTxDataSource2, mslvProcDataSource2, mslvWSDataSource2, mslvPSDataSource2, and so on:

```
<jdbc-system-resource>
    <name>mslvDataSource1</name>
    <target>RacConfigServer</target>
    <descriptor-file-name>jdbc/mslvDataSource1-0700-jdbc.xml
    </descriptor-file-name>
</jdbc-system-resource>
<jdbc-system-resource>
    <name>mslvDbTraceDataSource1</name>
    <target>RacConfigServer</target>
    <de-scriptor-file-name>jdbc/mslvDbTraceDataSource1-8405-jdbc.xml
    </descriptor-file-name>
</jdbc-system-resource>
.
.
.
<jdbc-system-resource>
    <name>mslvWSDataSource2</name>
    <target>RacConfigServer</target>
    <descriptor-file-name>jdbc/mslvWSDataSource2-5599-jdbc.xml
    </descriptor-file-name>
</jdbc-system-resource>
<jdbc-system-resource>
    <name>mslvPSDataSource2</name>
    <target>RacConfigServer</target>
    <de-scriptor-file-name>jdbc/mslvPSDataSource2-5450-jdbc.xml
    </descriptor-file-name>
</jdbc-system-resource>
```

3. Save and close the **config.xml** file.

4. Restart the application server.

Modifying the Classpath for the WebLogic Server Domain

To update the classpath for the WebLogic domain:

1. Edit the *m63domain***bin\setDomainEnv.cmd** file.

2. Add the path for the **ons.jar** file to the CLASSPATH environment variable.

For example:

```
set CLASSPATH=%CLASSPATH%;C:\Oracle\Middleware\Oracle_Home\oracle_common\lib
\ons.jar;
```

3. Save and close the file.

Configuring the Connection Pool Parameters

To configure the connection pool parameters:

1. Navigate to *m63domain***config\jdbc** the folder.

2. Edit each XML file for the mslvWSDataSource, mslvDbTraceDataSource, mslvNoneTxDataSource, mslvProcDataSource, mslvPSDataSource, and

mslvWSDataSource data sources, and update the <jdbc-connection-pool-params> element as follows:

```
<jdbc-connection-pool-params>
    <initial-capacity>10</initial-capacity>
    <max-capacity>100</max-capacity>
    <min-capacity>2</min-capacity>
    <highest-num-waiters>1000</highest-num-waiters>
    <connection-reserve-timeout-seconds>60</connection-reserve-timeout-seconds>
    <test-connections-on-reserve>true</test-connections-on-reserve>
    <inactive-connection-timeout-seconds>14400
    </inactive-connection-timeout-seconds>
    <test-table-name>SQL ISVALID</test-table-name>
    <statement-timeout>0</statement-timeout>
</jdbc-connection-pool-params>
```

3. Save and close the XML file for each data source.

Example 9-1 shows sample XML for one data source.

Example 9-1   Sample of One Data Source

```
<jdbc-data-source>
   <name>DataSourceName</name>
   <datasource-type>AGL</datasource-type>
   <jdbc-driver-params>
      <url>jdbc:oracle:thin:@server:port/DB</url>
      <driver-name>oracle.jdbc.xa.client.OracleXADataSource</driver-name>
      <properties>
         <property>
            <name>user</name>
            <value>user_name</value>
         </property>
      </properties>
      <password-encrypted>password</password-encrypted>
   </jdbc-driver-params>
   <jdbc-connection-pool-params>
      <test-table-name>SQL ISVALID</test-table-name>
   </jdbc-connection-pool-params>
   <jdbc-data-source-params>
      <jndi-name>JNDIName</jndi-name>
      <global-transactions-protocol>TwoPhaseCommit
         </global-transactions-protocol>
   </jdbc-data-source-params>
   <jdbc-oracle-params>
      <fan-enabled>true</fan-enabled>
      <ons-node-list />
      <ons-wallet-file />
      <active-gridlink>true</active-gridlink>
   </jdbc-oracle-params>
</jdbc-data-source>
```

> **✎ Note:**
>
> Some lines in the example are wrapped for the display.

Tuning JDBC Multi Data Source

For each data source perform the steps in this procedure to tune the data sources.

To tune each data source:

1. Ensure you are logged into the WebLogic administration console.

2. In the Domain Structure tree, expand **Services**, and then click **Data Sources**.

   The Summary of JDBC Data Sources page is displayed.

3. Select the target data source (for example, *mslvDataSource1*).

   The Settings for *<DataSource>* page is displayed.

4. Click the **Connection Pool** tab.

   The Connection Properties are displayed.

5. Click **Lock and Edit**.

6. Scroll down to Initial Capacity and Maximum Capacity.

7. In the **Initial Capacity** field, enter **1**.

8. In the **Maximum Capacity** field, enter **15**.

   > ✎ **Note:**
   >
   > The values of the Initial Capacity and Maximum Capacity fields depend on their particular MSS deployment.

9. Scroll down to the bottom of the page and click **Save**.

   The Settings for *<DataSource>* page is displayed.

10. Click **Advanced** to display additional configuration items.

11. Select the **Test Connections On Reserve** check box.

12. Click **Save**.

    The Settings for *<DataSource>* page is displayed.

13. Click the **Transaction** tab.

    The Transaction Properties are displayed.

14. Select the **Set XA Transaction Timeout** check box.

15. In the **XA Transaction Timeout** field, enter **3600**.

16. In the **XA Retry Duration** field, enter **300**.

17. Click **Save**.

18. Click **Activate Changes**.

    The Settings updated successfully message is displayed.

19. Repeat steps 1 through 18 to tune each data source.

10

Performing Maintenance and Troubleshooting

This chapter contains basic system maintenance and database troubleshooting information.

Basic Maintenance

This section contains information about the basic maintenance tasks for Oracle Communications MetaSolv Solution (MSS). See *MetaSolv Solution System Administrator's Guide* for full system maintenance information

Starting the MSS System

When starting MSS, you must start components in the following order:

- Database
- Application server
- MSS client (user workstation)

The startup scripts are located in the domain directory. The script name includes the server name. For example, if a server is named *mslv01*, it will have a startup script named **start***mslv01***.sh** in the domain directory.

To start MSS, run the following scripts located in the domain directory:

- For Unix Linux:

  ```
  startWebLogic.sh
  ```

- For Windows:

  ```
  startWebLogic.cmd
  ```

  Starts the administration server if you are running in a domain that has a separate administration server. Start the administration server before starting the managed server(s).

- For Unix Linux:

  ```
  start<server>.sh
  ```

- For Windows:

  ```
  start<server>.cmd
  ```

  Starts an application server (either managed or single) running MSS.

If you are running an administration server and a managed server on the same machine, after the managed server is started, the administration server can be shut down to release resources that the process would otherwise consume. However, the

administration server must be running to allow access to the management console or to perform any administration function.

Uninstalling MSS

To uninstall MSS from an application server:

1. Start the administration server and log in to the WebLogic Server Administration Console.

2. To undeploy the application, do the following:

   a. From the Domain Structure tree, click **Deployments**.

   b. In the Change Center pane, click **Lock & Edit**.

   c. From the Summary of Deployments pane, click the check box for **nur.ear** (or **cluster-nur.ear)**.

   d. Click **Stop** and select **Force Stop Now**.

   e. Click **Delete**.

   f. Click **Yes** to delete the deployment.

   g. In the Change Center pane, click **Activate Changes**.

3. Repeat step 2 for each version of ASR or LSR that is installed.

4. To delete the data sources, do the following:

   a. From the Domain Structure tree, expand **Services,** expand **JDBC**, and then click **Data Sources**.

   b. In the Change Center pane, click **Lock & Edit**.

   c. From the Summary of JDBC Data Sources pane, click the check box for each data source that is to be deleted (refer to the list below).

      • **Services** > **JDBC** > **Data Sources** > **mslvDataSource**

      • **Services** > **JDBC** > **Data Sources** > **mslvDbTraceDataSource**

      • **Services** > **JDBC** > **Data Sources** >**mslvNoneTxDataSource**

      • **Services** > **JDBC** > **Data Sources** >**mslvProcDataSource**

      • **Services** > **JDBC** > **Data Sources** >**mslvPSDataSource**

      • **Services** > **JDBC** > **Data Sources** >**mslvWSDataSource**

   d. Click **Delete**.

   e. Click **Yes** to delete the data sources.

   f. In the Change Center pane, click **Activate Changes**.

5. In the file system on the machine, delete the MSS installation directory.

Changing an IP Address

When an IP address for a server changes, adjustments must be made in the configuration. The following sections indicate how to handle this change.

Changing an IP Address for Clustered Servers

The IP address or DNS name can be used to identify a machine's listen address. Oracle recommends using the DNS name.

When the IP address changes on a server's machine, you must modify the machine's IP address in the Oracle WebLogic server if it is used as the server listen address, the **gateway.ini**, **integration.xml**, **tbs.ini**, **tbs_util.ini**, and any other files that identify the server machine using the IP address.

Changing an IP Address for Single or Administration Servers

Before the IP address changes, start the server and change the listen address to the new IP address, then implement the IP address change and restart the server.

Change the **startserver.sh** file to show the new address:

```
ADMIN_URL=http://<Admin server IP address:port number>/
```

If you use the DNS name of the server's host machine rather than the IP address, there is no effect when the IP address changes.

Troubleshooting Database Issues

This section contains information about the causes and resolutions to common database problems so you can troubleshoot in MSS.

ORA-12519, TNS: No Appropriate Service Handler Found

Problem

Listener refused the connection with the following error:

```
ORA-12519, TNS: no appropriate service handler found
```

Cause

You receive this error message when activating the data sources (DS) or when starting the server.

Resolution

Check the DB parameter for the number of processes. The number of processes should be high enough to hold the number of connections that you want to create in addition to the WL internal processes.

ORA-01979: missing or invalid password for role WOTSTWTWWOO or ADMIN_ROLE

Problem

During upgrade, you receive the following error:

```
ORA-01979: missing or invalid password for role "WOTSTWTWWOO" or "ADMIN_ROLE"
```

Cause

You receive this error message when activating the data sources (DS) or when starting the server.

Resolution

Change the role passwords.

Only the database administrator can change passwords for the roles ADMIN_ROLE and WOTSTWTWWOO by running the following stored procedure:

```
===========pl/sql should be run by dba for changing role's password==========
DECLARE
  C_NAME VARCHAR2(200);
  C_PASSWORD VARCHAR2(200);
BEGIN
  C_NAME := 'role_name'; /*specify the role name, ADMIN_ROLE OR WOTSTWTWWOO*/
  C_PASSWORD := 'password'; /*specify the password*/
  SP_CREDSTORE_CHG_ROLE_PWD(C_NAME, C_PASSWORD);
END;
```

ORA-39384: Warning: User <USERNAME> Has Been Locked And The Password Expired During Import

Problem

After DataPump import, the users with 10g style verifiers are locked, the passwords are expired, and the following error message is displayed:

```
ORA-39384: Warning: User <USERNAME> Has Been Locked And The Password Expired During
Import
```

Cause

Because 10g style verifiers are no longer supported in 12.2, DataPump marks such users as locked and expires the password when they are imported.

Resolution

After the import execution, unlock the user and set a new value in the target database by running the following command:

```
ALTER USER <username> ACCOUNT UNLOCK;
ALTER USER <username> IDENTIFIED BY <password>;
```

SQL*Plus Quits During the Upgrade

SQL*Plus may unexpectedly quit while running the upgrade under the following scenarios:

- The ASAP, EBOND, EDI, JOB, and SYS user IDs do not exist on the instance.

- You entered an incorrect password.

- ASAP does not have DBA-level authority.

- The database is not at the appropriate version level when starting the upgrade.

- You do not have the standard tablespaces **data** and **indexes**.

- The full directory path for the SQL script files does not include the trailing slash, you entered an invalid path, or you do not have write access to the directory.

- The free space checks did not pass (minimum available tablespace free for the largest contiguous space and total free space). Check the output log (**upgenv.log**) for the exit reason, correct the tablespace limitation, and run the **_upgmss.sql** script again.

Restarting a Failed Upgrade Attempt With the Incorrect Mode

When failure occurs before the main upgrade sequence has begun (for example, during the interactive upgrade sequence), use your original selection of either upgrade mode 1 or 2 to restart the upgrade. Do not use upgrade mode 3 to restart the upgrade if a failure occurs during the interactive upgrade sequence.

Upgrade Failure and Losing Audits

If upgrade mode 1 was run more than once, all audits are lost and you must start the upgrade again from the beginning.

Database Graphics Not Displaying Correctly

Check to make sure you have run the **TBSGraphicLoad.exe** located in the same directory as the MSS executable on the client workstation. This executable contains new and updated graphics for the MSS database. It does not need to be run by every user. It only has to run one time on the database for the release.

No Database Log Files

When **_upgradetbs.sql** runs, you are prompted for the directory path for the script files that are used to do the upgrade. The path must end with a trailing slash. The slash is different for UNIX/Linux and Windows:

/ for UNIX and Linux

\ for Windows

If the slash is not included, no log files are written.

Troubleshooting MSS Installation Issues

This section describes how to troubleshoot some of the issues that you may encounter during the MSS installation process.

Destination Unreachable Error in AppServerLog.xml in IPv6 Environment

After you install MSS in an IPv6 environment, you may receive the following error in the **AppServerLog.xml** file:

```
Error initializing the MetaSolv Solution Sender:
javax.naming.CommunicationException:
t3:// 2606:b400:2010:484b:f13b:4672:38b7:5af9:9065:
```

```
Destination 2606:b400:2010:484b:f13b:4672:38b7:5af9,
9065 unreachable; nested exception is:
java.net.ConnectException: Connection refused: no further information;
No available router to destination [Root exception is java.net.ConnectException:
t3:// 2606:b400:2010:484b:f13b:4672:38b7:5af9:9065:
Destination 2606:b400:2010:484b:f13b:4672:38b7:5af9,
9065 unreachable; nested exception is:
java.net.ConnectException: Connection refused: no further information;
No available router to destination]
at weblogic.jndi.internal.ExceptionTranslator.
toNamingException(ExceptionTranslator.java:40)
```

This message is thrown if the Integration Server, Event Server and System Task Server are enabled. If this error repeatedly occurs (even after the server is up and running successfully), you must enable the HTTP Tunneling option through the WebLogic administrative console. To enable HTTP Tunneling perform the following:

1. Login to the WebLogic administrative console.

2. Select **Home**, **Summary of Services**, and then **Summary of Servers**.

3. Select **AdminServer**.

4. Enable the **Tunneling** option.

Once the tunneling option is set, you can ignore the single issuance of the error message.

Generation Problem or Error for the Nameservice.ior File

During the installation of MSS, you may have an issue on the creation of the **NameService.ior** file and no error messages existing in the log files. To resolve this issue, you need to ensure that the following permissions are on the directories and files within the MSS home directory structure.

Another error can occur when starting the server with any one of the CORBA servers enabled, and the server can throw the following error in the **mss.log** file:

```
Tried and failed to open file: MSLV_HOME/m63domain/appserver/ior/NameService.ior
SEVERE Exception while converting string to objectorg.omg.CORBA.BAD_PARAM:
Invalid or unreadable URL/IOR: file:///MSLV_HOME/m63domain/appserver/ior/
NameService.ior
vmcid: 0x0  minor code: 0  completed: No
```

Table 10-1 lists the directories and permissions that you need to address where *MSLV_Home* is the directory for the MSS home directory and *MSS_Server_Name* is the appropriate MSS server name.

Table 10-1   Required Directory and File Permissions

Directory/File	Owner Permissions	Group and Other Permissions
MSLV_Home/*MSS_Server_Name*/appserver	Read, Write, Execute	Read, Execute
MSLV_Home/*MSS_Server_Name*/appserver/ior	Read, Write, Execute	Read, Execute
MSLV_Home/*MSS_Server_Name*/jacORB	Read, Write, Execute	Read, Execute
MSLV_Home/*MSS_Server_Name*/jacORB/startMSLVorb.sh	Read, Write, Execute	Read, Execute

Table 10-1   (Cont.) Required Directory and File Permissions

Directory/File	Owner Permissions	Group and Other Permissions
MSLV_Home/*MSS_Server_Name*/jacORB/bin	Read, Write, Execute (You also need to set these permissions for all the sub-directories and files.)	Read, Execute

These problems can occur because of the existing permissions on the files and directories in the environment. Once you set the permissions correctly, restart your server, the IOR file should exist in the *MSLV_Home*/*MSS_Server_Name*/ **appserver/ior** directory, and no open file error should exist in the **mss.log** file.

Web Service Deployment Warning Message

You can ignore the following warning message that appears in the **appserver.mss.log** file during Web Service deployment:

```
<Warning> <com.sun.xml.ws.wsdl.PayloadQNameBasedOperationFinder> <BEA-000000> <Non
unique body parts! In a port, as per BP 1.1 R2710 operations must have unique
operation signature on the wire for successful dispatch. Methods
[getServiceLocationRequest, getEntityByKeyRequest] have the same request body block
{http://www.openuri.org/}getEntityByKeyRequest. Method dispatching may fail, runtime
will try to dispatch using SOAPAction. Another option is to enable AddressingFeature
to enabled runtime to uniquely identify WSDL operation using wsa:Action header.>
```

This Warning message is related to getServiceLocationRequest and getEntityByKeyRequest APIs, because both the APIs use the same request structure. Because customers have used these two APIs on their integrations in prior versions of MSS, such as 6.2.1, these two APIs are also available in MSS 6.3.0, for customers migrating to the MSS 6.3.0 release.

Access Problem for the WebLogic Console and MSS Application Using IPv6 Address

After you create the domain and install the MSS application using IPv6 address, you may encounter the following issues:

- You are unable to access the WebLogic Server Administration Console using Internet Explorer and the following error message appears:

  ```
  The proxy could not connect to the destination in time. Please verify the site
  you are attempting to access and retry.
  ```

- You are unable to log in to the MSS application and the following error message appears:

  ```
  The user ID you entered is not valid. Please use a valid User ID or ask your
  manager for assistance.
  ```

To resolve both the issues, do the following:

1. Start Internet Explorer.

2. From the **Tools** menu, select **Internet Options**.

    The Internet Options window appears.

3. Click the **Connections** tab, and then click **LAN Settings**.

    The Local Area Network (LAN) Settings window appears.

4. Under the Automatic configuration section and the Proxy server section, deselect all the check boxes.

5. Click **OK**, which returns you to the Internet Options window.

6. Click **OK**.

The Runtime Information Page is Not Displayed

The Runtime Information Page is not displayed and the following error message appears:

```
Error 500--Internal Server Error
From RFC 2068 HyperText Transfer Protocol -- HTTP/1.1:
10.5.1 500 Internal Server Error
The server encountered an unexpected condition which prevented it from fulfilling
the request.
```

And the MSS error log reflects the following:

```
javax.servlet.jsp.JspException: No collection found
at org.apache.struts.taglib.logic.IterateTag.doStartTag(IterateTag.java:281)
at jsp_servlet.__runtimeinfo._jspService(__runtimeinfo.java:594)
at
weblogic.servlet.internal.StubSecurityHelper$ServletServiceAction.run(StubSecurityHel
per.java:280)
at
weblogic.servlet.internal.StubSecurityHelper$ServletServiceAction.run(StubSecurityHel
per.java:254)
Truncated. see log file for complete stacktrace
```

To resolve this issue, you must enable HTTP tunneling in the WebLogic Server Administration Console.

# Enabling HTTP Tunneling

To enable HTTP tunneling:

1. Log in to the WebLogic Server Administration Console.

2. In the Domain Structure tree, expand **Environment**, and then click **Servers**.

    The Summary of Servers page appears.

3. Click a server (for example, m63ditu1server).

    The Settings for *ServerName* page is displayed.

4. Click the **Protocols** tab.

5. Under Change Center, click **Lock & Edit**.

6. On the **HTTP** tab, do the following

7. Select the **Enable Tunneling** check box.

8. Click **Save**.

ORACLE®

9. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

Check Box To Select the Server Name is Not Displayed in the MSS Installer

If you try to connect to the WebLogic Server by specifying an IPv6 address in the **Admin Host** field of the MSS installer, the check box to select the server name is not displayed under the domain tree.

Figure 10-1   Check Box to Select the Server Name
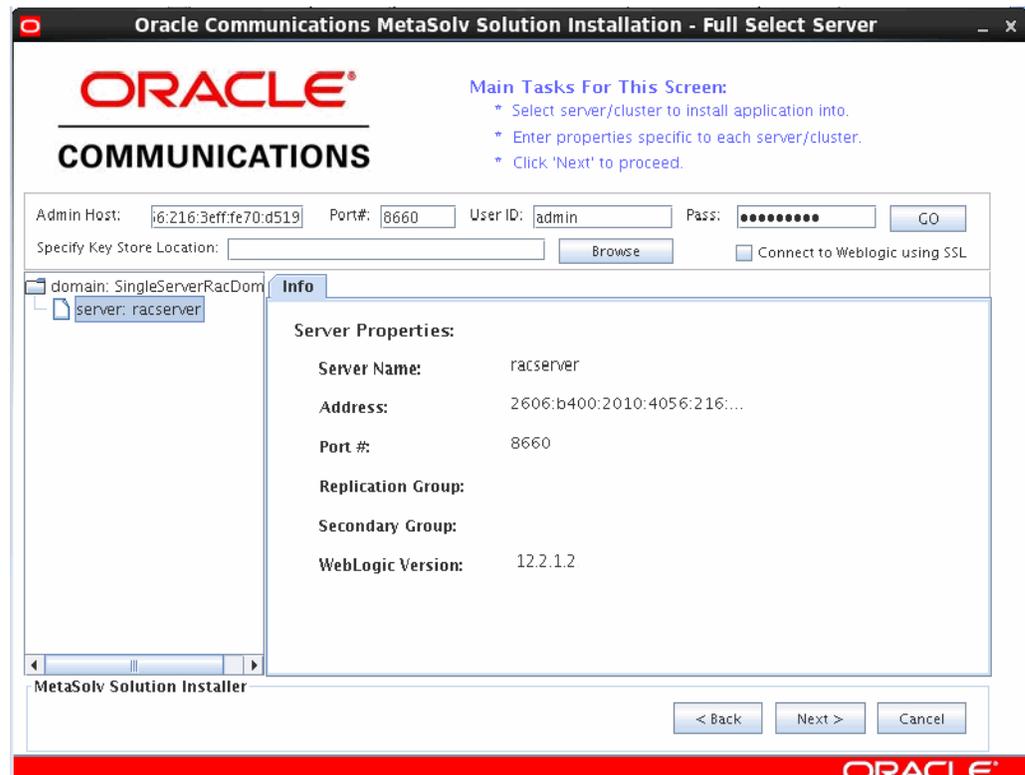
To resolve this issue, ensure that the IPv6 address of the Admin Host is added in the **hosts** file of the Operating System, as follows:

```
2606:b400:2010:484b:f13b:4672:38b7:5af9   slc04wro.example.com   slc04wrolocalhost
```

On Windows, the **hosts** file is typically located at **C:\Windows\System32\drivers\etc**. On Unix and Solaris, the hosts file is located at **/etc/hosts**.

My Desktop Page is Not Displayed

If you install and deploy MSS on a single server using IPv6 address with SSL enabled, the My Desktop page is not displayed in the MSS application.

To resolve this issue, you must enable HTTP tunneling in the WebLogic Server Administration Console. See "Enabling HTTP Tunneling" for more information.

Number Format Exception When Starting the Proxy Server

When starting the proxy server, you may receive the following number format exception:

```
java.lang.NumberFormatException: For input string: "b400:2010:484b:f13b:
4672:38b7:5af9"
at java.lang.NumberFormatException.forInputString(NumberFormatException.java:65)
at java.lang.Integer.parseInt(Integer.java:580)
at java.lang.Integer.parseInt(Integer.java:615)
at weblogic.servlet.proxy.HttpClusterServlet$Server.parsePorts
(HttpClusterServlet.java:2042)
at weblogic.servlet.proxy.HttpClusterServlet$Server.<init>
(HttpClusterServlet.java:1898)
at weblogic.servlet.proxy.HttpClusterServlet$ServerList.<init>
(HttpClusterServlet.java:2078)
at weblogic.servlet.proxy.HttpClusterServlet.init
(HttpClusterServlet.java:141)
```

To resolve this issue, ensure that you specify the IPv6 addresses within [] (brackets) in the WebLogicCluster init parameter of the HttpClusterServlet in the **web.xml** of the proxy server.

For example:

```
<init-param>
  <param-name>WebLogicCluster</param-name>
  <param-value> [IPv6_address1]:port1|[IPv6_adress2]:port2</param-value>
</init-param>
```

Unable to Log In to the MSS Application

When logging in to the MSS application, you may receive the following error:

```
Unable to communicate with application server selected.
```

To resolve this issue, do the following:

- If you are connecting to an IPv6 proxy server for accessing MSS client application, ensure that you specify the proxy server's IPv6 address in the client machine's **etc/hosts** file, as follows:

  ```
  IPv6address              ipv6machine@example.com       ipv6machine
  ```

- Install the self-signed certificate on the client machine. See "Installing the Self-Signed Certificate on the Client Machine" for more information.

Updates to the web.xml File of the Proxy Server are Not Reflected

Your updates are not reflected in the **web.xml** file of the proxy server.

To resolve this issue, do the following before starting the proxy server for the first time:

- Make your changes in the **web.xml** file
- Specify the IPv6 addresses within [] (brackets) in the WebLogicCluster init parameter of the HttpClusterServlet in the **web.xml** file

- Add the SecureProxy init parameter to the HttpClusterServlet in the **web.xml** file for a cluster that has SSL enabled

If you have already started the proxy server and still unable to see your changes in the **web.xml** file, redeploy the Oracle Cluster Proxy web application using the WebLogic Server Administration Console.

Updates to orb.properties for SSL and AIX Platform

If you create a domain using SSL on an AIX platform, you must make additional updates to the **orb.properties** file. Ensure the following property values are set:

1. Open the file *MSLV_Home\mslv01***\jacORB\orb.properties**

   where:

   - *MSLV_Home* is the directory in which the MSS software is installed

   - *mslv01* is the server home directory

2. Provide the appropriate values for the following properties:

   ```
   jacorb.security.jsse.server.key_manager_algorithm=IbmX509
   jacorb.security.jsse.server.trust_manager_algorithm=IbmX509
   jacorb.security.jsse.client.key_manager_algorithm=IbmX509
   jacorb.security.jsse.client.trust_manager_algorithm=IbmX509
   ```

Managed Server Startup Warning When Servers on Different Machines

When the admin server and the managed server are on different machines, a warning can occur during a cluster installation. You can encounter the following warning when trying to start the managed server:

```
####<Warning> <DeploymentService> <BEA-290074> <Deployment service servlet
received file download request for file>
```

To resolve this issue, you add the following java option:

```
-Dweblogic.data.canTransferAnyFile=true
```

to the **startWeblogic.sh** file on the managed server.

DLL Error when Connecting to the Database

A DLL error can occur if an incorrect version of the Oracle Database Client was installed and you run any of the following applications:

- Location and Routing Gateway

- NPA Split Utility

- Data Selection

- Pre-Migration Analysis Tool

- MetaSolv Solution Utilities

The DLL error is the following:

```
Cannot make a connection to the database.
Oracle library OCI.DLL or ORAC803.DLL could not be loaded.
```

This error can occur if the 64-bit version of the Oracle Database Client was installed instead of the 32-bit version. See *MSS Planning Guide* for more information on software version requirements.

Window Response Delay from MSS in SSL Environment After No Activity

When running MSS in an SSL environment, it is possible to experience a response delay when moving outside the application and then returning back to MSS. If you leave the MSS application for a few minutes (with no activity), and then later attempt to move to a new MSS window, then there can be a delay of few seconds before it responds. Also, the window header title can include "Not Responding" for few seconds.

This issue occurs due to the idle connection time-out set in the Oracle WebLogic console. To resolve this issue, log in to the WebLogic console, and under Server->Protocol->General, set the option for the idle connection time-out to a higher number. The default is 60 seconds, and after 60 seconds of no activity, it drops the connection to the client. Increase the idle connection time-out value to the appropriate value for your requirements.

CORBA Error During Integration Between MSS and Network Integrity

During the integration between MSS and Network Integrity, when a connection is made to the MSS application from Network Integrity through the CORBA server, Network Integrity returns the following error message:

```
Can't establish Corba connection with MSS
IDL:omg.org/CosNaming/NamingContext/NotFound1.0.
```

To resolve this issue, do the following:

1. Navigate to the *MSLV_Home*/**appserver/gateway** directory and edit the **gateway.ini** file.

2. Uncomment the INFRASTRUCTURESERVER entry in the [Servers] section.

Known Issues with Reconfiguration Wizard (Only if Reconfiguration Wizard is used to Migrate WebLogic Domain)

After executing the WebLogic Reconfiguration wizard to migrate from 12.2.1.2 to 12.2.1.3/12.2.1.4 domain, the start scripts to start up the MetaSolv application server/cluster throws error "No such file or directory" and the server fails to start.

To resolve this issue, follow the Knowledge Article 2607740.1 - *After Execute WebLogic Reconfiguration Wizard Receive "No Such File or Directory" Errors When Starting the Server(s)* on the My Oracle Support website:

https://support.oracle.com/epmos/faces/DocumentDisplay?id=2607740.1

A

Proxy Server Setup

In a clustered environment, you typically have multiple servers running on different machines. To transparently connect to one of the servers, a central routing server is required to direct the client to one of the clustered servers. The routing server can be a hardware-based (load balancer) or software-based (proxy server) solution. This appendix describes how to configure and set up the optional Oracle-provided proxy server.

The Oracle proxy server is not recommended because it cannot support more than 150 concurrent user sessions.

Figure A-1 shows a proxy server in a clustered environment. The proxy server directs the data traffic between the clustered servers, mslv01 and mslv02.

Figure A-1   Proxy Server
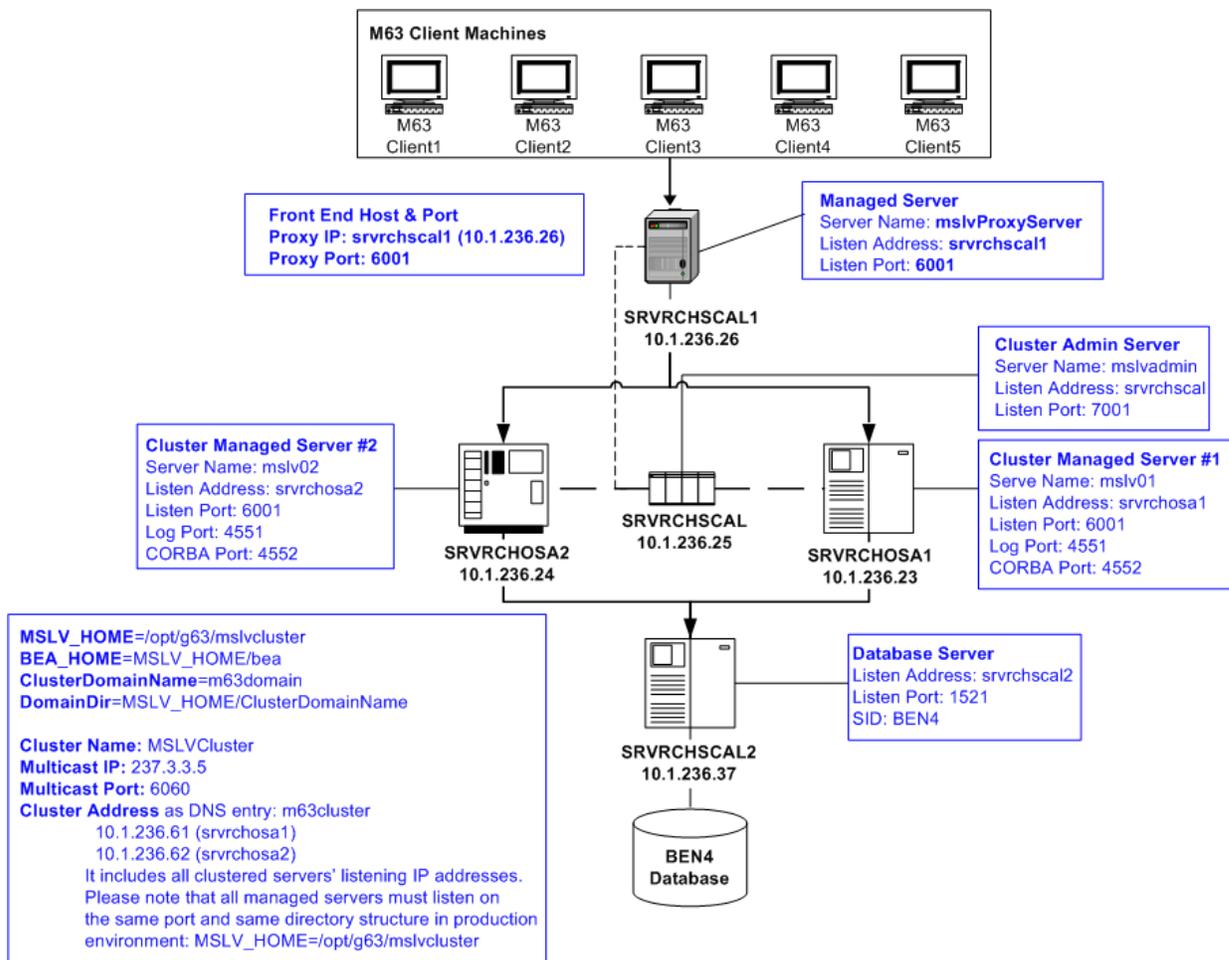
Proxy Server Files

The following files (**web.xml** and **weblogic.xml**) are necessary for the proxy server setup. Refer to "Setting up the Proxy Server" for the steps required to create the files.

- **web.xml**

```
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
<servlet>
  <servlet-name>HttpClusterServlet</servlet-name>
    <servlet-class>
      weblogic.servlet.proxy.HttpClusterServlet
    </servlet-class>
<init-param>
    <param-name>WebLogicCluster</param-name>
    <param-value>
       srvrchosa1:6001|srvrchosa2:6001
    </param-value>
  </init-param>
<!--The following two init-parameter tags are required if the proxy server is set up
using SSL in a clustered environment.-->
<init-param>
  <param-name>SecureProxy</param-name>
  <param-value>ON</param-value>
</init-param>
<init-param>
  <param-name>DebugConfigInfo</param-name>
  <param-value>ON</param-value>
</init-param>
</servlet>
<servlet-mapping>
  <servlet-name>HttpClusterServlet</servlet-name>
  <url-pattern>/</url-pattern>
</servlet-mapping>
<servlet-mapping>
  <servlet-name>HttpClusterServlet</servlet-name>
  <url-pattern>*.jsp</url-pattern>
</servlet-mapping>
<servlet-mapping>
  <servlet-name>HttpClusterServlet</servlet-name>
  <url-pattern>*.htm</url-pattern>
</servlet-mapping>
<servlet-mapping>
  <servlet-name>HttpClusterServlet</servlet-name>
  <url-pattern>*.html</url-pattern>
</servlet-mapping>
</web-app>
```

- **weblogic.xml**

```
<!DOCTYPE weblogic-web-app PUBLIC "-//BEA Systems, Inc.//DTD Web Application 8.1//
EN" "http://www.bea.com/servers/wls810/dtd/weblogic810-web-jar.dtd">
  <weblogic-web-app>
    <context-root>/</context-root>
  </weblogic-web-app>
```

Setting up the Proxy Server

Figure A-2 shows the procedure for setting up the proxy server.

Figure A-2   Setting Up a Proxy Server
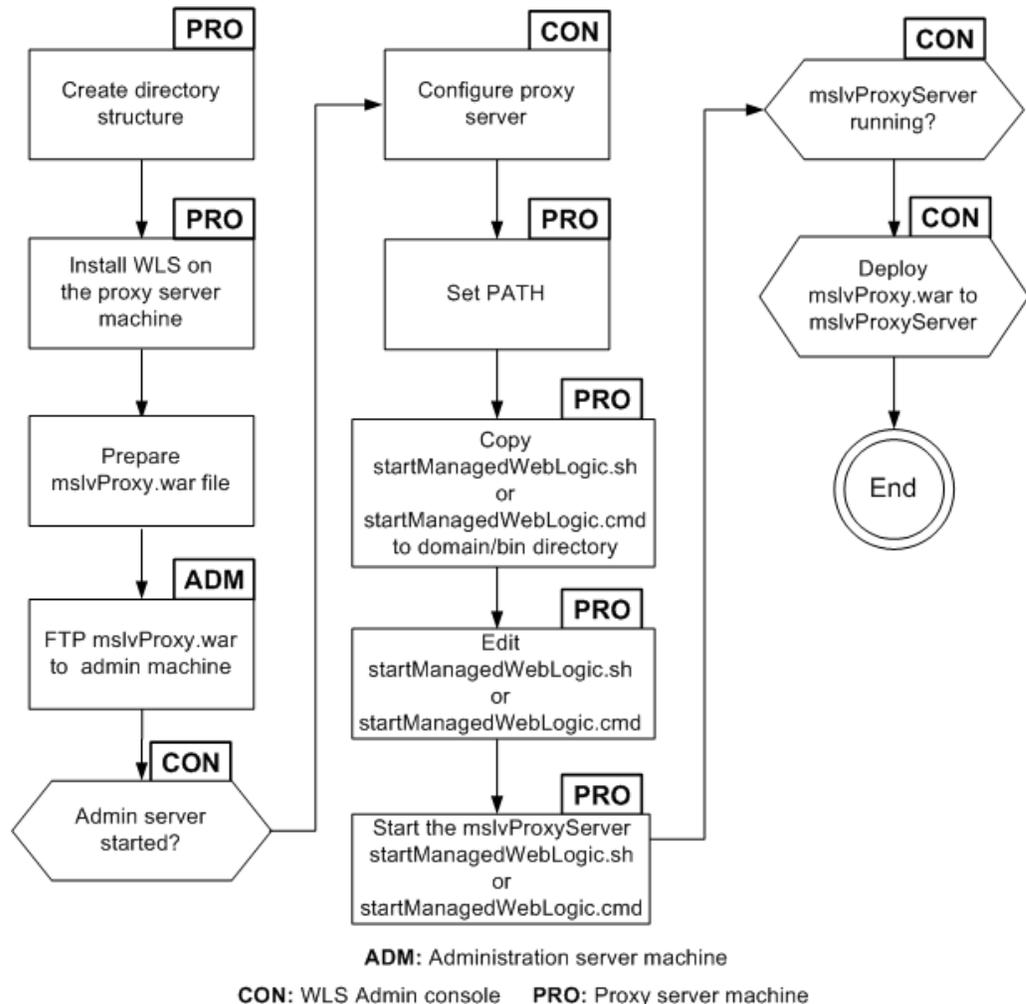
To set up a proxy server:

1. Create the directory structure.

    For example: **/opt/g63/mslvcluster/***m63domain*.

2. Install Oracle WebLogic Server on the proxy server machine.

    For example: **srvrchscal1**

3. Prepare the **mslvProxy.war** file

    a. Create a **WEB-INF** directory under the proxy directory.

    b. On the proxy server machine, create a file named **web.xml** and copy the contents as shown previously, in "Proxy Server Files".

    c. Copy the file into the **WEB-INF** directory.

- For Windows, enter the following command:

  ```
  notepad web.xml
  ```

- For UNIX/Linux, enter the following command:

  ```
  touch web.xml
  ```

    d. On the proxy server machine, create a file named **weblogic.xml** and copy the contents as shown previously, in "Proxy Server Files".

    e. Copy the file into the **WEB-INF** directory.

- For Windows, enter the following command:

  ```
  notepad weblogic.xml
  ```

- For UNIX/Linux, enter the following command:

  ```
  touch weblogic.xml
  ```

Figure A-3 shows the files copied into the newly created **WEB-INF** directory.

Figure A-3   Command Prompt Window Showing WEB-INF Directory
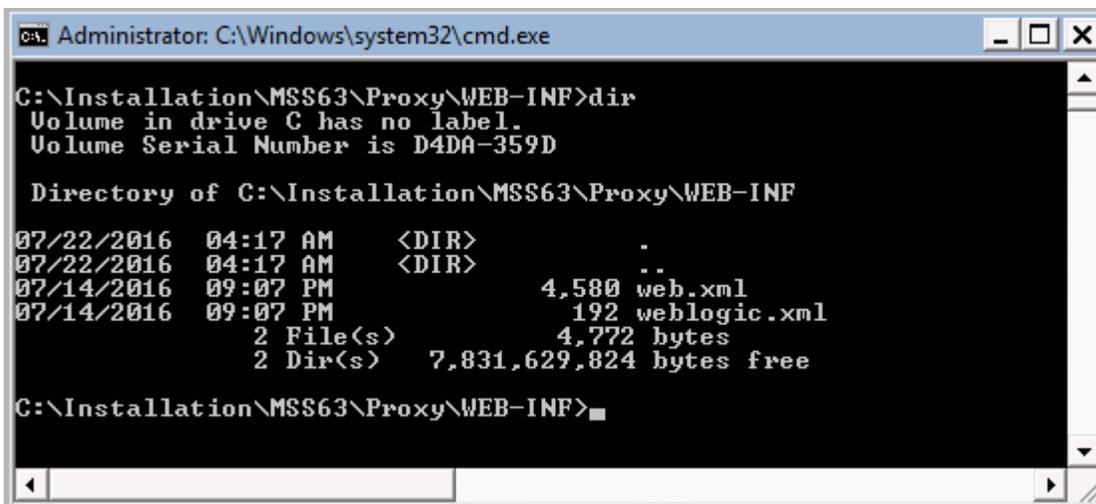
    f. In the **web.xml** file, add all managed server host machine names and ports in the manner shown in the bold text in Figure A-4.

Figure A-4   web.xml File


g. Go to the parent of the **WEB-INF** directory and type the following command and press ENTER:

```
jar cvf mslvProxy.war WEB-INF
```

Figure A-5 shows the command typed at the command line.

Figure A-5   Command Prompt Window

4. FTP the **proxy.war** file to the administration server.

5. Start the administration server if it is not running.

6. Create a WebLogic machine for the proxy server by completing the following tasks:

   a. Log in to the WebLogic Server Administration Console.

   b. In the Domain Structure tree, expand **Environment** and then select **Machines**.

   c. In the Summary of Machines pane, click **New**.

   d. In the Create a New Machine pane, enter the name of the machine that will host the proxy server in the **Name** field, select the **Machine OS** type, and click **Ok**.

   e. In the Change Center pane, click **Activate Changes**.

7. To configure the proxy server, in the left pane, select **Environment**, select **Servers**, and then select **New** in the right pane.

   The Create a New Server pane appears.

8. In the Create a New Server pane, enter the following information into the appropriate fields for the proxy server: **Name**, **Machine**, **Listen Address**, and **Listen Port** and click **Finish**.

   Worksheet references and example values:

Field Name	Worksheet Reference Number	Example Value
Name	Proxy-0610	mslvProxyServer
Machine	Proxy-0620	srvplscal1
Listen Address	Proxy-0620	srvplscal1
Listen Port	Proxy-0630	6001

9. Copy the **startManagedWeblogic** file to the **domain/bin** directory. (This script will be used to start the proxy server.)

   Figure A-6 shows the srvplscal1_mss63 window.

Figure A-6   srvplscal1_mss63 Window


```
srvplscal1:/opt/mss63/mslvcluster/m63domain>cp /opt/mss63/mslvcluster/Oracle/Middleware/Oracle_Home/wlserver/common/bin/startManagedWeblogic.sh
```
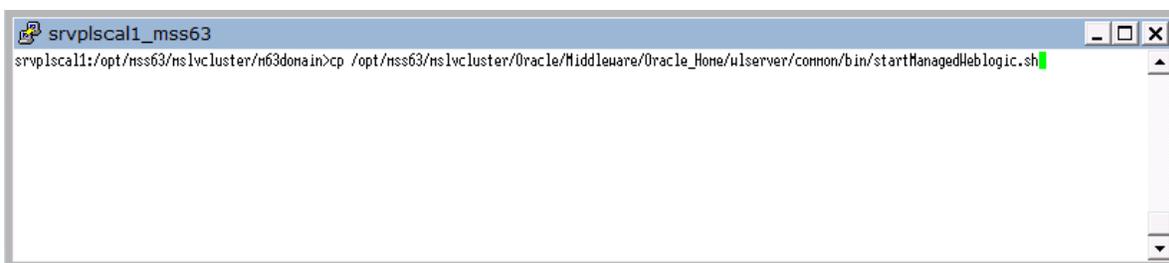
10. Edit the **startManagedWebLogic** file, including new values for the parameters in the following list.

    Example values from the proxy worksheet are included in the list.

    ```
    ADMIN_URL=http://srvrchscal:7001
    SERVER_NAME=mslvProxyServer
    WLS_USER=weblogic
    WLS_PW=web_logic
    ```

```
JAVA_VM=-server
MEM_ARGS=-Xms512m -Xmx512m -XX:NewRatio=4
```

11. Start the proxy server.

Figure A-7 shows the command for starting the proxy server.

Figure A-7 Command for Starting the Proxy Server
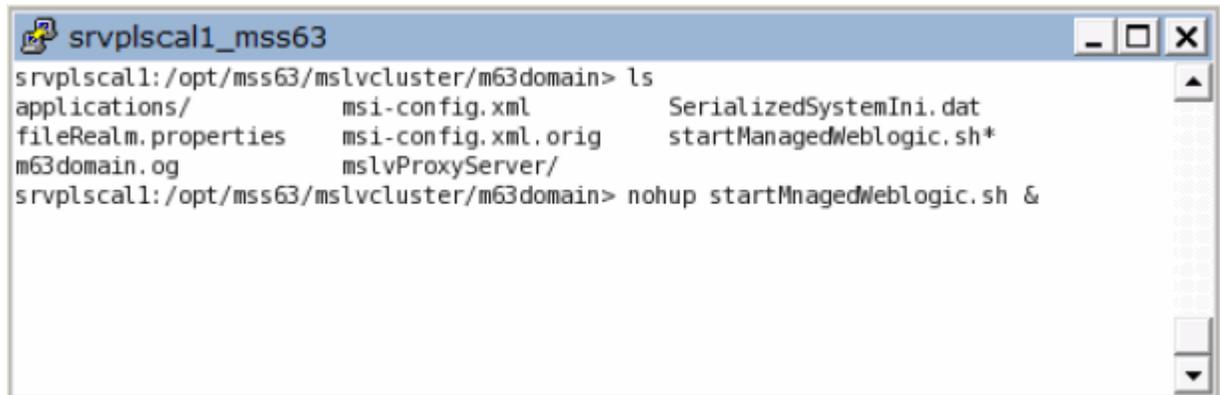
12. From the WebLogic Server Administration Console, under the Domain Structure tree, expand **Environment** and then select **Servers** to see the updated list of servers and to view the state of the proxy server.

13. Configure the server and deploy the **proxy.war** file by completing the following tasks

    a. In the Change Center pane, click **Lock and Edit**.

    b. Expand the **Domain Structure** tree and click **Deployments**.

       The Summary of Deployments pane appears.

    c. On the **Control** tab, click **Install**.

       The Install Application Assistant pane appears.

    d. Under **Current Location**, navigate to the **deploy** directory and select **mslvProxy.war**, then click **Next**.

       The Choose targeting style pane appears.

    e. Select **Install this deployment** as an application and click **Next**.

       The Select deployment targets pane appears.

    f. Under **Clusters**, select the proxy server that was created in step 7.

    g. Under **Source accessibility**, select **I will make the deployment accessible from the following location**.

    h. Click **Finish**.

    i. In the Change Center pane, click **Activate Changes**.

    j. Expand the **Domain Structure** tree and click **Deployments**.

       The Summary of Deployments pane appears.

    k. Select **mslvProxy**.

    l. From the **Start list**, select **Servicing all requests**.

The Start Application Assistant pane appears.

m. Click **Yes**.

Ensure that the state of the mslvProxy application has changed from **Prepared** to **Active**.

B

Oracle Communications MetaSolv Solution Components

Table B-1 shows which software components are included in the Oracle Communications MetaSolv Solution (MSS) core product, which are separate software options, and which are separate applications included with MSS.

Table B-1   MSS Components Included In This Release

Component	Core component, software option, or separate application	Where installed
Engineering	-	-
AutoDesign	Software option	Client
Diversity	Software option	Client
Equipment	Core	Client
Groom Tool	Core	Client
Network Design Canvas	Core	Client
Ownership of Inventory	Core	Client
Path Analysis	Core	Client
Plant Administration Module	Software option	Client
Provisioning Assistant	Core	Client
OSS Gateways and APIs	-	-
ASR API	Software option	Application server
End User Billing API	Software option	Application server
Internet Services API	Software option	Application server
Inventory and Capacity Management API	Software option	Application server
LSR Interconnection API	Software option	Application server
Plant API	Software option	Application server
PSR End User Order Entry API	Software option	Application server
Switch Provisioning Activation API	Software option	Application server
Transportation Provisioning Activation API	Software option	Application server
Trouble Management API	Software option	Application server
Work Management API	Software option	Application server
Service Requests	-	-
ASR	Software option	Application server
ASR and ISR using templates	Core	Client
Customer Management Module	Software option	Client
Engineering Work Order (EWO)	Software option	Client

Table B-1   (Cont.) MSS Components Included In This Release

Component	Core component, software option, or separate application	Where installed
Generate ASR (PSR to ASR mapping)	Software option	Client
Internal Service Request (ISR)	Software option	Client
LSR	Software option	Application server
Product Catalog Module	Software option	Client
Product Service Request (PSR)	Software option	Client
PSR to LSR mapping	Core	Client
Service Request Worksheet Module	Software option	Client
USO	Software option	Client
Technology Modules	-	-
ATM/Frame Relay Technology Module	Software option	Client
Digital Loop Carrier Technology Module	Software option	Client
DSL Technology Module	Software option	Client
Ethernet Technology Module	Software option	Client
IP Technology Module	Software option	Client
MPLS Technology Module	Software option	Client
Optical/TDM Technology Module	Software option	Client
SONET Technology Module	Software option	Client
Wireless Technology Module	Software option	Client
Trouble Management	-	-
Notifications	Core	Client
Trouble Management Subsystem	Software option	Client
Utilities	-	-
Background Processor	Core Separate application	Separate machine
Location and Routing Gateway	Software option Separate application	Client
MetaSolv Solution Utilities	Core Separate applications	Client
NPA Split Utility	Software option	Client
Web Service	-	-
MSS WebService	Core	Application server
Work Management	-	-
Provisioning Plans	Core	Client
Rules and Behaviors for all areas	Core	Client
Work Queues	Core	Client

C

Planning Worksheets

This appendix contains worksheets to help you determine the values you need to complete an installation of Oracle Communications MetaSolv Solution (MSS).

Each worksheet contains columns for the following information:

- **R/O**: This field indicates whether a value for the item is required or optional.

- **Reference number**: This is a number used in the installation procedures in "Installing and Deploying MetaSolv Solution on a Single Server " or "Installing and Deploying MetaSolv Solution on a Clustered Server" to identify a value and show where the value is used. When the number is referred to in a procedure, you can look it up on a worksheet to see an example and a definition.

- **Item name**: This field indicates the item you must identify for your system, for example, a name for the administration server or an HTTP port for a managed server.

- **Example value in Windows/UNIX/Linux**: Examples are provided for all items on the worksheet.

- **Your value**: This is the installation value you must provide on the worksheet for an item.

- **Item description**: A description of the item you are being asked to provide an installation value for.

MSS Installation

This section lists the worksheets that help you determine the values you need to complete the installation of MSS.

Application Server Common Installation Worksheet

Table C-1 shows the worksheet that applies to MSS installation. Complete the values and use the worksheet as you install required software and MSS 6.3.*x*.

Table C-1 Application Server Common Installation Worksheet

R/O	Reference number	Item name	Example value	Your value	Item description
R	COMM-0010	Application server domain name	m63domain		WebLogic domain name
R	COMM-0020	Application server user name	weblogic		WebLogic server logon user name
R	COMM-0030	Application server password	*password*		WebLogic server logon password

Table C-1   (Cont.) Application Server Common Installation Worksheet

R/O	Reference number	Item name	Example value	Your value	Item description
R	COMM-0040	APP_MSLV passwd	mss6mslv		APP_MSLV database password
R	COMM-0050	APP_API passwd	mss6api		APP_API database password
R	COMM-0055	APP_INT passwd	mss6int		APP_INT database password
R	COMM-0090	MetaSolv Home	/opt/m63Single/single or /opt/m63Cluster/cluster		MetaSolv home directory
R	COMM-0100	MW_HOME	/opt/Oracle/Middleware/ Oracle_Home		WebLogic home directory
R	COMM-0110	WebLogic domain directory	/opt/m63Single/single/ or /opt/m63Cluster/cluster/		Directory that holds the files for the WebLogic domain.
R	COMM-0115	Application directory	/opt/m63Single/single/ application or /opt/m6Cluster/cluster/ application		Directory that holds the files for the Application server.
R	COMM-0120	PATH	WIN: %MW_HOME% \jdk*Version*\bin;%PATH% UNIX/Linux: %PATH %:$MW_HOME/jdk*Version*/ bin:$PATH		Directory where jre\bin is located. Must be part of the PATH environment variable.
R	COMM-0130	Oracle Database Server Name	srvrchscal2		The name of the server where the Oracle database resides.
R	COMM-0140	Oracle Database Port	1521		Port used to communicate with the Oracle database.
R	COMM-0150	Oracle Database Service Name	BEN6		Database SID
R	COMM-0160	Oracle Database Server Name1	srvrchscal1		The name of the server where the Oracle RAC database resides.

Table C-1   (Cont.) Application Server Common Installation Worksheet

R/O	Reference number	Item name	Example value	Your value	Item description
R	COMM-0165	Oracle Database Port#1	1521		Port used to communicate with the Oracle RAC database.
R	COMM-0170	Oracle Instance Name1	drac1		The name of the Oracle RAC database instance.
R	COMM-0175	Oracle Database Server Name2	srvrchscal2		The name of the server where the Oracle RAC database resides.
R	COMM-0180	Oracle Database Port#2	1521		Port used to communicate with the Oracle RAC database.
R	COMM-0185	Oracle Instance Name2	drac2		The name of the Oracle RAC database instance.

Single Server Installation Worksheet

Table C-2 shows the worksheet for single server installation.

Table C-2   Single Server Installation Worksheet

R/O	Reference number	Item Name	Example value	Your value	Item description
R	Single-0150	Application server name	mslv01		Logical name for theWebLogic application server instance.
R	Single-0160	Application server DNS hostname	srvrchosa1		Name of the host machine on which theWebLogic application server resides.
R	Single-0170	Application server HTTP port	7070		Application server HTTP port.
R	Single-0180	Application server HTTPS port	7071		Application server SSL port.

Table C-2   (Cont.) Single Server Installation Worksheet

R/O	Reference number	Item Name	Example value	Your value	Item description
R	Single-0190	Application server log port	4501		Used for MSS application server logging purposes. This value must be unique across all MSS application servers running on the same host machine.
R	Single-0200	Application server CORBA port	2507		CORBA initialPort. This value must be unique across all MSS application servers running on the same host machine.
R	Single-0205	Single server DEBUG_PORT	8453		Single server debug port. This value must be unique for each machine.
O	Single-0210	Proxy URL	http://srvrchosa1:7070 (default to http:// Single-0160:Single-0170)		Proxy/Load balancer URL
R (Only if SSL is enabled)	Single-2015	JacORB security keystore	/opt1/stores/identity.jks		The full path of the JacORB security keystore.
R (Only if SSL is enabled)	Single-2020	JacORB security keystore password	*password*		The password for the JacORB security keystore.
R (Only if SSL is enabled)	Single-2025	JacORB security default username	mycert		The default user name for JacORB security.
R (Only if SSL is enabled)	Single-2030	JacORB security default password	*password*		The default password for JacORB security.

Admin Server Installation Worksheet

Table C-3 shows the worksheet for administration server installation.

Table C-3   Admin Server Installation Worksheet

R/O	Reference number	Item Name	Example value	Your value	Item description
R	Admin-0240	Admin server name	mslvadmin		Logical name for a WebLogic admin server instance.
R	Admin-0250	Admin server DNS hostname	srvrchscal		The name of the host machine on which the admin server resides.
R	Admin-0260	Admin server HTTP port	7001		Admin server HTTP port. It is unique for each machine.
R	Admin-0270	Admin server HTTPS port	7002		Admin server SSL port. It is unique for each machine.

Clustered Server General Installation Worksheet

Table C-4 shows the worksheet for clustered server general installation.

Table C-4   Clustered Server General Installation Worksheet

R/O	Reference number	Item Name	Example value	Your value	Item description
R	Cluster-0410	Cluster Name	MSLVCluster		Logical name for the WebLogic cluster.
R	Cluster-0420	Cluster Address	Test/development environment: srvrchosa1:6001 (HTTP port), srvrchosa1:6002 (HTTPS port) srvrchosa2:6001 (HTTP port), srvrchosa2:6002 (HTTPS port) (2-node cluster) Production environment requires a DNS entry: m63cluster: 192.0.2.23 (srvrchosa1), 192.0.2.24 (srvrchosa2)		Comma separated list of single address host machine names or IP addresses and ports for each server in this cluster.
R	Cluster-0430	Multicast Address	2xx.3.3.5		Valid Range: 224.0.0.0 - 239.255.255.255 (Class D address)
R	Cluster-0440	Multicast Port	6060		Valid range: 1 - 65535
R	Cluster-0450	Front End Host	http://192.0.2.57:6001		For a cluster, you must provide this value for a proxy server or a load balancer URL. See LB-0100 and LB-0200.

Clustered Server Installation Worksheet

Table C-5 shows the worksheet for clustered server installation.

Table C-5   Clustered Server Installation Worksheet

R/O	Reference number	Item Name	Example value	Your value	Item description
R	Cluster-0520	Managed server name	(1) mslv01 (2) mslv02		Logical name for the WebLogic managed server instance.
R	Cluster-0550	Cluster managed server listen address	(1) srvrchosa1:10.1.236.23 (2) srvrchosa2:10.1.236.24		The name of the host machine on which the WebLogic managed server resides.
R	Cluster-0570	Cluster managed server listen port	(1) 6001 (2) 6001 This must be the same port in a production environment.		Managed server HTTP port. It is unique for each machine.
R	Cluster-0580	Cluster-managed server SSL listen port	(1) 6002 (2) 6002		Managed server SSL port. This value is unique for each machine.
R	Cluster-0590	Cluster-managed server log port	(1) 4551 (2) 4551		Used for MSS clustered server logging purposes. This value must be unique for each machine.
R	Cluster-0600	Cluster server CORBA port	(1) 4552 (2) 4552		CORBA initialPort. This value must be unique for each machine.
R	Cluster-0610	Cluster server DEBUG_PORT	(1) 8444 (2) 8444		Managed server debug port. This value must be unique for each machine.

WebLogic Proxy Server Installation Worksheet

Table C-6 shows the worksheet for WebLogic proxy server installation.

Table C-6   WebLogic Proxy Server Installation Worksheet

R/O	Reference number	Item Name	Example value	Your value	Item description
O	Proxy-0610	Proxy managed server name	M63Proxy		Logical name for the WebLogic proxy server instance.
O	Proxy-0615	Machine name	srvProxyServer		The name of the host machine on which the WebLogic proxy managed server resides.
O	Proxy-0620	Proxy managed server listen address	srvProxyServer		The name of the host machine on which the WebLogic proxy managed server resides.
O	Proxy-0630	Proxy managed server listen port	7001		Proxy managed server HTTP port. This value is unique for each machine.
O	Proxy-0640	Proxy managed server SSL listen port	7002		Proxy managed server SSL port. This value is unique for each machine.

Hardware Load Balancer Installation Worksheet

Table C-7 shows the worksheet for hardware load balancer installation.

Table C-7   Hardware Load Balancer Installation Worksheet

R/O	Reference number	Item Name	Example value	Your value	Item description
O	LB-0100	Front end host virtual IP address	192.0.2.57		The virtual IP address for a load balancer machine.
O	LB-0200	Front end HTTP port	6001		The HTTP port used by the load balancer machine.

D
Configuration Values

The installer sets certain configuration values for the domain automatically during the installation process. You can change these values through the WebLogic Server Administration Console, but the values are recommended by Oracle. The location in the console are enclosed in parentheses.

- Bridging: 1 (**Services** > **Messaging** > **Bridges**)
- Domain Logging (*Domain*> **Logging** tab)
  - Files to retain: 100
  - Rotation file Size: 65535
  - Rotation Type: By Size
  - Limit number of retained files: Selected
- Server Logging (**Environment** > **Servers** > *servername* >**Logging** tab >**General** tab)
  - Files to retain: 100
  - Rotation file Size: 65535
  - Rotation Type: By Size
  - Limit number of retained files: Selected

E
Load Balancer Configuration Example

Figure E-1 shows a configuration that includes a load balancer for the M63 cluster used in the scenario in this document.

Figure E-1   Example of a Load Balancer Used With the MSS Cluster
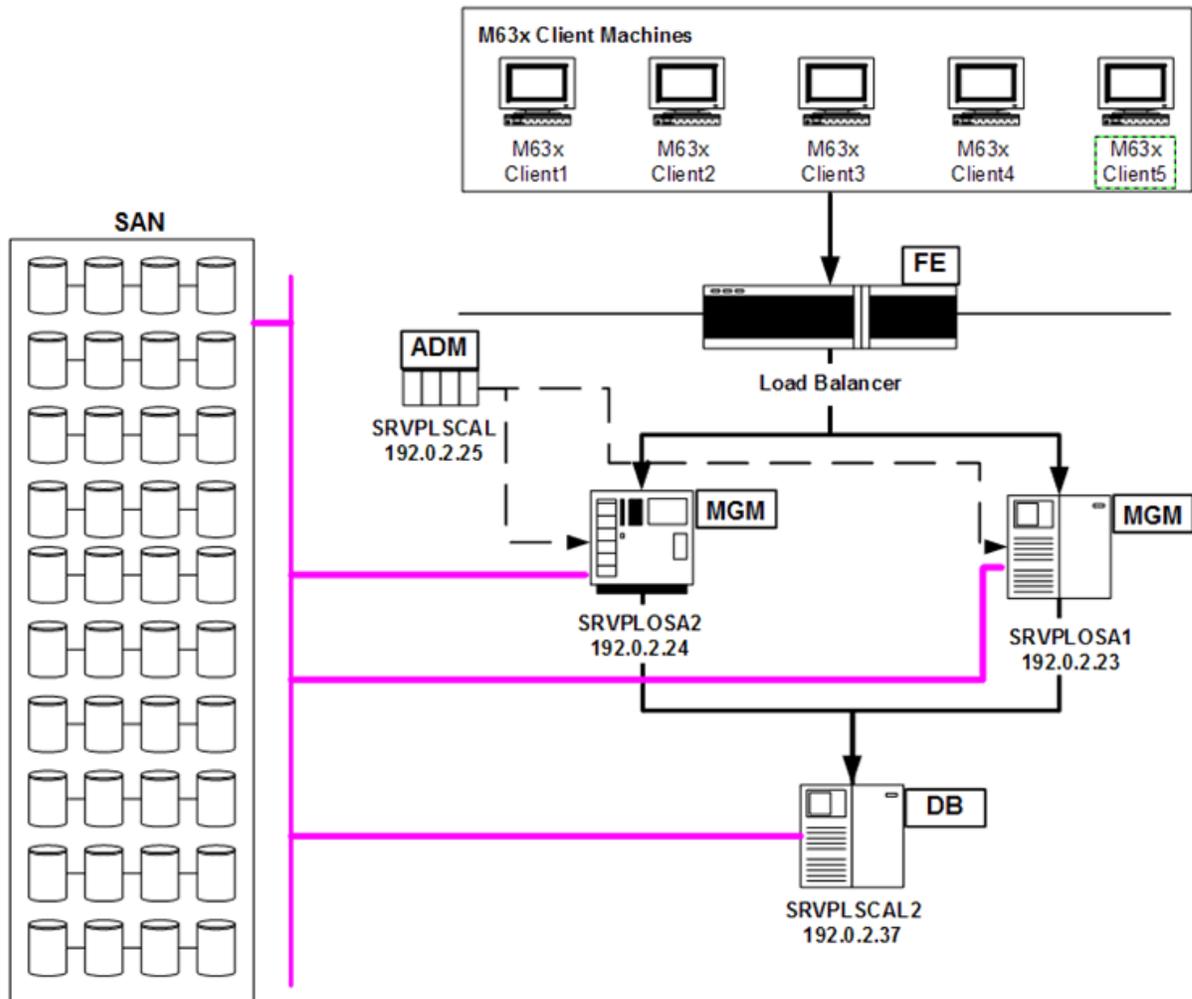
Contact your network engineering team or other IT support to set up the load balancer. One requirement for the load balancer service is server affinity, also known as Sticky session.

See the Oracle WebLogic Server documentation for more information.

F

Tuning Servers For Performance

This appendix provides recommended configurations to tune your servers for performance.

Information on Tuning the Application Server

The configuration information given in this document is for a baseline setup.To achieve optimum performance for individual business needs, load and performance testing in a test environment that represents your true production environment is required. The test environment should mimic how you use your production system, including the transaction mix, number of users, hardware and software infrastructures, database, network usage, and all other relevant factors. Setting up a test environment will allow you to determine the settings that you should have for your production environment for:

- Connection pool sizing
- Java memory management

See the Oracle WebLogic Server documentation for more information about setting parameters for items such as execute queues, connection pools, and timeouts.

Connection Pool Settings

For the **MSLVPool,** set the Maximum Capacity = **Threads Maximum**

1. Log in to the WebLogic Server Administration Console.
2. In the Domain Structure tree, expand **Services**, and then click **Data Sources**.

    The Summary of JDBC Data Sources page appears.
3. Select **mslvDataSource**.

    The Settings for mslvDataSource page appears.
4. Select the **Configuration** tab.
5. Select the **Connection Pool** tab.
6. Set the **Maximum Capacity** field to **100**.
7. Click **Save**.
8. Under the Change Center pane, click **Activate Changes**.

JVM Memory Argument Settings

This section describes how to setup the JVM memory argument settings. The MSS startup scripts are located under the *MSLV_Home*/**domain** directory where *MSLV_Home* is the path of your MSS domain. The following lists the startup script files

with the first script in the list used for single servers and the remaining scripts used for clustered servers:

For Windows Operating Systems

- **startMSLVSingle.cmd**
- **startMSLVManaged.cmd**
- **startAdminServer.cmd**
- **startProxyServer.cmd**

For Windows Operating Systems

- **startMSLVSingle.sh**
- **startMSLVManaged.sh**
- **startAdminServer.sh**
- **startProxyServer.sh**

The following is an example of the settings which can be configured. (The parameters are separated onto separate lines for readability.)

```
set MEM_ARGS=
-Xms8g
-Xmx8g
-XX:NewRatio=4
-XX:SurvivorRatio=4
-XX:TargetSurvivorRatio=80
-XX:MaxMetaspaceSize=386m
```

You can configure the following parameters:

- **Xms**: This option sets the initial and minimum Java heap size. The Java heap is the memory portion where blocks of memory are allocated to objects and freed during garbage collection. The MSS default value for 64-bit operating systems is "1g" for Windows and "8g" for all other platforms.

- **Xmx**: This option sets the maximum Java heap size. The optimum value varies based on your operating system. The MSS default value for 64-bit operating systems is "4g" for Windows and "8g" for all other platforms.

- **NewRatio**: This option sets the ratio between young and tenure or old generation. This sets the young generation size in relation to the size of the old generation. The young generation contains the pool of objects that have survived garbage collection of the Eden space. The tenure generation contains the pool of objects that exist in the survivor space. The MSS default value is "4." With this setting, the old generation will be four times as large as the young generation.

- **SurvivorRatio**: This option specifies how large of a size the Eden space is relative to one of the two survivor spaces. This value sets the ratio of Eden size to one survivor space size. The MSS default value is "4."

- **TargetSurvivorRatio**: This option specifies the target percentage and the allowable fullness of the survivor space. The MSS default value is "80" or 80%. This setting allows more memory to be utilized and aids high throughput applications.

- **MaxMetaspaceSize**: This option allows you to limit the amount of native memory used for class metadata. Without a setting, the Metaspace will dynamically re-size depending of the application demand at runtime. With this Java version, class

metadata is stored in the native heap and this space is called Metaspace. By default class metadata allocation is only limited by the amount of available native memory. The MSS default value is "386m."

There are no standard memory argument settings for the JVM. The MSS default values are suggestions and can be changed to optimally tune your JVM, given your current configuration (operation system and the number of CPUs for example). At a minimum, set the initial heap size (Xms) and maximum heap size (Xmx) to equal values. The startup time can be slightly longer, but for long-running applications it provides an overall better performance. Please review your operating system and set the best possible memory argument values for your configuration. See the Oracle WebLogic Server documentation for more information.

G
Configuration Files

This appendix provides additional information about the configuration files involved in the Oracle Communication MetaSolv Solution (MSS) installation process.

> **Note:**
>
> After you make changes to any of the configuration files, ensure that you restart each server or clustered server. The changes that you make in the configuration files do not take effect until the server(s) are restarted.

loggingconfig.xml File

Not all windows in the application allow you to limit the number of rows that are retrieved when performing a query. If you are not able to specify a limit and your query retrieves a large number of rows, the application server may display a java.lang.OutOfMemory error or a 500 server error. If this occurs, you must restart the application server. To eliminate this problem, you can edit the **jdbc-trace** query parameters of the **loggingconfig.xml** file.

See *MetaSolv Solution System Administrator's Guide* for more information.

gateway.ini File

Compare the new **gateway.ini** file against your original **gateway.ini** file for the following sections:

- [Servers]: For API servers
- [ThreadProcs]: For event servers
- [System]: For URLNamingServicePort
- [CA]: For Custom attribute refresh interval

See *MetaSolv Solution System Administrator's Guide* for more information on the **gateway.ini** file.