Oracle® Communications Network Integrity

Installation Guide

Release 7.5
G13615-01
December 2024

ORACLE

Oracle Communications Network Integrity Installation Guide, Release 7.5

G13615-01

Contents

4 Installing and Configuring Oracle WebLogic Server

5 Installing and Configuring Additional Software

6 Installing Network Integrity

13 Troubleshooting the Network Integrity Installation

Preface

This guide provides instructions for installing Oracle Communications Network Integrity.

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Audience

This document is for system administrators, database administrators, and developers who install and configure Network Integrity. The person installing the software should be familiar with the following topics:

- Operating system commands
- Database configuration
- Oracle WebLogic Server
- Network management

Before reading this guide, you should have familiarity with Network Integrity. See *Network Integrity Concepts*.

Network Integrity requires Oracle Database and Oracle WebLogic Server. See the documentation for these products for installation and configuration instructions.

1

Network Integrity Installation Overview

This chapter provides an overview of the installation process of Oracle Communications Network Integrity.

Directory Placeholders Used in This Guide

Table 1-1 lists the placeholders that are used in this guide:

Table 1-1 Network Integrity Directory Placeholders

Placeholder	Description
NI_Home	The directory in which the Network Integrity software is installed.
MW_Home	The directory in which the Oracle Fusion Middleware products, files, and folders are installed, such as WebLogic Server. Also contains the **utils** directory.
WL_Home	The directory in which WebLogic Server is installed. *WL_Home* is located in *MW_Home*.
Domain_Home	The directory containing the configuration for the domain into which Network Integrity is installed. The default location is *MW_Home***/user_projects/domains/***domain_name*, where *domain_name* is the name of the WebLogic Server domain for Network Integrity.

Overview of the Installation Procedure

The following is an outline of the installation procedure for Network Integrity:

1. Plan your installation, including:
   - Determine the scale of your implementation; for example, is it a small test system, or a large production system. To determine the scale, you may need to assess the scale of the network or data set to be discovered or reconciled.
   - Assess how many physical systems you need, and which software components to install on which systems.
   - Plan the system topology; for example, determine whether you want a single managed server deployment or a clustered deployment.
2. Review the system requirements, as described in "Network Integrity System Requirements ".
3. Install and configure the Oracle Database, as described in "Installing and Configuring the Oracle Database".
4. Install and configure the Oracle WebLogic server, as described in "Installing and Configuring Oracle WebLogic Server ".
5. Install and configure additional software, as described in "Installing and Configuring Additional Software".
6. Install Network Integrity, as described in "Installing Network Integrity".

7. Perform post-installation configuration tasks, as described in "Network Integrity Post-Installation Tasks".
8. Verify the installation, as described in "Verifying the Network Integrity Installation".

About the Installer

You install Network Integrity using the Oracle Universal Installer. The Installer installs the core application and configures connections with the components, according to the connection details you provide during installation. See the Oracle Universal Installer (OUI) User's Guide for more information about the Installer.

Installation Options

You can install Network Integrity in GUI mode (using the Installer) or in silent mode.

- **GUI mode:** Use the Installer when you want to interact with the graphical installation screens during the installation process.
- **Silent mode:** Use silent mode when you are repeatedly installing Network Integrity using the same configuration. Silent mode does not use the GUI and runs in the background.

Ensuring a Successful Installation

Network Integrity installations should be performed only by qualified personnel. You must be familiar with the following before you begin the installation:

- UNIX operating system
- Oracle WebLogic Server administration
- Oracle Database administration
- Installing Java-related packages

Oracle recommends that the installation and configuration of the Oracle database be performed by an experienced database administrator.

Follow these guidelines:

- As you install each component verify that the component installed successfully before continuing the installation process.
- Pay close attention to the system requirements. Before you begin installing the application, ensure your system has the required base software. In addition, ensure that you know all of the required configuration values, such as host names and port numbers.
- Make a note of any new configuration values as you create them. You are required to enter configuration values later in the procedure.

2
Network Integrity System Requirements

This chapter describes the hardware, operating system, software, server, and database requirements for installing Oracle Communications Network Integrity.

Software Requirements

Network Integrity consists of a base application that is installed on an Oracle WebLogic server domain. It connects with an Oracle database to store all relevant information, and can connect to a report publishing tool if you require reports to be published. You must install and connect all required software with Network Integrity for optimal performance.

Supported Operating Systems

Table 2-1 lists operating systems that support the Network Integrity server. Use the My Oracle Support Certifications tab to access the latest software platform support information. See knowledge article 1491004.1 or the My Oracle Support Help on the My Oracle Support Web site for additional information:

https://support.oracle.com

Table 2-1 Supported Server-Side Operating Systems

Product	Version
Oracle Linux on x86 (64-bit)	Linux 8.x or higher (with the latest available updates) Linux 9.x or higher (with the latest available updates)

> **Note:**
>
> When installing Network Integrity in a multi-host shared-disk cluster environment, you must have full permissions on the *NI_Home*, *MW_Home*, *WL_Home*, and *Domain_Home* directories.
>
> Refer to "Directory Placeholders Used in This Guide" for information on these directories.

Required Software

Table 2-2 lists software required on the server for installing and running Network Integrity.

Table 2-2 Required Server-Side Software

Product	Version
Oracle WebLogic Server Enterprise Edition (included with the Oracle Fusion Middleware WebLogic Server and Coherence distribution in the Oracle Fusion Middleware 12c software)	12*c* (12.2.1.4)
Oracle Fusion Middleware Application Development Runtime, including Enterprise Manager and Repository Creation Utility (included with the Oracle Fusion Middleware Infrastructure distribution in the Oracle Fusion Middleware 12c software)	12*c* (12.2.1.4)
Oracle Fusion Middleware Repository Creation Utility (RCU) for Linux (included with Oracle Data Integrator)	12*c* (12.2.1.4)
Oracle Java SE Development Kit (JDK) for Linux	Java 8 with latest critical patch update
Oracle Database Enterprise Edition	19*c* (19.25)
Oracle Access Manager (OAM), included with Oracle Identity and Access Management	12*c* (12.2.1.4.0)

The Network Integrity Installer checks for all required software and displays errors if it detects any missing or unavailable components, or if there are any connectivity related issues.

Table 2-3 lists software required to access the Network Integrity UI.

Table 2-3 Required Client-Side Software

Product	Version
Operating System	Microsoft Windows 10, 11 (Windows is for development only)
Java Runtime Environment (JRE)	Java 8 with latest critical patch update
Web Browser	Google Chrome 131.x or later Mozilla Firefox 132.0 or later
Oracle Communications Service Catalog and Design	See "Service Catalog and Design Compatibility" in *SCD Compatibility Matrix* (included in the Design Studio documentation) for Design Studio compatibility information.
Oracle Fusion Middleware JDeveloper Studio Generic	12*c* (12.2.1.4.0)

Design Studio is required for developing cartridges that extend Network Integrity. Install Design Studio on a computer with network access to the Network Integrity server.

For Oracle Communications Service Catalog and Design - Design Studio plug-in installation information, see "Design Studio Installation Overview (1)" in *Design Studio Installation Guide*.

Supported Software

Table 2-4 lists additional software that is supported by Network Integrity.

Table 2-4 Supported Software

Product	Version
Oracle Analytics Publisher	6.4.0 Oracle Analytics Publisher is required to use the reporting templates included with Network Integrity.
Oracle Communications Unified Inventory Management (UIM)	7.7.0.0.0
Oracle Communications MetaSolv Solution (MSS)	6.3
Oracle Internet Directory	12.2.1.4 or higher

Supported software is installed and licensed separately from Network Integrity.

Hardware Requirements

The number and configuration of the systems that you employ for your Network Integrity installation depends on the scale and the kind of deployment you have planned according to your network(s).

> **Note:**
>
> The sizing estimates contained in this section are based on the assumptions of proper application configuration and tuning, in a manner consistent with leading practices of Oracle Communications consulting and performance engineering. This information is provided for informational purposes only and is not intended to be, nor shall it be construed as a commitment to deliver Oracle programs or services. This document shall not form the basis for any type of binding representation by Oracle and shall not be construed as containing express or implied warranties of any kind. You understand that information contained in this document will not be a part of any agreement for Oracle programs and services. Business parameters and operating environments vary substantially from customer to customer and as such not all factors, which may impact sizing, have been accounted for in this documentation.

Table 2-5 provides the minimal hardware requirement for Network Integrity installed on a single managed server in a WebLogic domain.

Table 2-5 Network Integrity Minimum Hardware Requirements

Component	Requirement
Hard disk	Minimum 150 GB on each managed server.
Processor	Oracle recommends using a minimum of 4 OCPUs on each managed server.
Memory	Minimum 32 GB physical memory on each managed server.
Temporary disc space	Minimum 20 GB. The Network Integrity Installer uses a temporary directory to extract all installation files.

Information Requirements

During Network Integrity installation, you must enter configuration values such as host names and port numbers. This section describes the information that you must provide during the installation process. You define some of these configuration values when you install and configure the Oracle database and WebLogic Server.

If you have already installed other Oracle Communications products, the installer reads the values from the existing Oracle Communications products and uses them as default values. If no existing Oracle Communications products are installed, the installer proposes default values.

WebLogic Connection Information

Table 2-6 lists WebLogic Server and domain connection details that you are required to provide during installation.

Table 2-6 Application Server Connection Information

Information Type	Description
Host name	The host name for the particular WebLogic server instance to define it uniquely for the specific purpose of installing, and working with, Network Integrity.
Port number	This is the number assigned to this specific service. Port numbers are usually pre-defined and you can accept the provided default value.
User name	Your WebLogic Server user name. You define this name when you install Oracle WebLogic Server.
Password	Your password to connect to the WebLogic server as the user for which you provided the user name. You define this password along with the user name during the Oracle WebLogic Server installation.

Database Connection Information

Table 2-7 lists database connection details that you are required to provide during installation.

Table 2-7 Database Connection Information

Information Type	Description
Host name	Host name or IP address of the Oracle Database server for Network Integrity.
Port number	This is the number assigned to this specific service. Port numbers are usually pre-defined and you can accept the provided default value.
User name	Your database user name. You define the user name when you install the database.
Password	Your password to connect to the database as the user for which you provided the user name. You define this password along with the user name during database installation.
Service name	This is the name of the database service or instance to remotely connect to the database. For example, **oracle.com**.

Database Connection Information for Real Application Cluster Database

Table 2-8 lists database connection details for an Oracle Real Application Cluster (RAC) database that you are required to provide during installation.

Table 2-8 Database Connection Information for Oracle RAC Database

Information Type	Description
Oracle RAC database connection string	The information string that is used to connect to the Oracle RAC database. For example, **HOST NAME1:PORT1:SERVICE NAME1, HOST NAME2:PORT2:SERVICE NAME2**.
User name	A database user name with SYS privileges. You define the user name when you install the database.
Password	Your password to connect to the database as the user for which you provided the user name. You define this password along with the user name during database installation.

Schema User Name Information

Table 2-9 lists schema user details that you are required to provide during installation.

Table 2-9 Schema user Information

Information Type	Description
Schema user name	Your schema user name that you use to access the Network Integrity schema.
Schema user password	The password to access the Network Integrity schema for the schema user you defined.

Hardware Sizing Considerations

Use Table 2-10, Table 2-11, and Table 2-12 as a general guideline when planning the hardware for your Network Integrity system.

Note:

- The information in this section is meant as a guideline only. The values in this section are approximate. Accurate sizing for a production system requires a detailed analysis of the proposed business requirements. The guidelines do not account for High Availability, Disaster Recovery environments or lower test and dev environments.
- The below sizing information for each network domain is mutually exclusive and is considered at 70% CPU utilization. In case multiple domains need to be supported, it is necessary to add suggested sizing per domain and procure the resulting total.
- Additionally, 4 OCPUs are required on the Inventory system (UIM) during the reconciliation and import process to ensure no impact on ongoing inventory/UIM system processing.

Table 2-10 Network Integrity Hardware Planning Guideline

Product Cartridge	Network Domain	Protocol	NI Actions benchmarked	Network Resources
TMF814Discovery_Cartridge Optical_UIM_Cartridge	Optical (SDH/DWDM/ SONET)	CORBA	Discovery, Discrepancy Detection, Reconciliation, Import	Physical Network Resources (Node, Equipment, Slot, Card, Port and Interface)
SDH_Discovery_Cartridge SDH_UIM_Cartridge	SDH	FTP	Discovery, Discrepancy Detection, Reconciliation, Import	Logical Network Resources (Topological links, Trails, Tunnels and Services)
DWDM_Logical_Discovery_Cartridge DWDM_Logical_Assimilation_Cartridge	DWDM	CORBA	Discovery, Discrepancy Detection, Reconciliation, Import	Logical Network Resources (Services, ODU, OTU, OCH, OMS and OTS)
Generic_SNMP_Cartridge UIM_Integration_Cartridge	IP	SNMP	Discovery, Discrepancy Detection, Reconciliation, Import	Physical Network Resources (Node, Equipment, Slot, Card, Port and Interface)

Table 2-11 Network Integrity Hardware Planning Guideline

Network Domain	Supported chunk size in single scan	Minimum Required Resources	Oracle Cloud Infrastructure Equivalent
Optical (SDH/DWDM/ SONET)	5k Devices	NI 4*4 OCPU and 128 GB RAM (4 MS each with 4 OCPUs and 32 GB RAM)	4 * VM.Standard3.Flex
SDH assimilated topology	100k Resources	NI 4*4 OCPU and 128 GB RAM (4 MS each with 4 OCPUs and 32 GB RAM)	4 * VM.Standard3.Flex
DWDM assimilated topology	100k SNCs	NI 4*4 OCPU and 128 GB RAM (4 MS each with 4 OCPUs and 32 GB RAM)	4 * VM.Standard3.Flex
IP	2k Devices	NI 4*4 OCPU and 128 GB RAM (4 MS each with 4 OCPUs and 32 GB RAM)	4 * VM.Standard3.Flex

Minimum Required Resources

Example: NI 4*4 OCPU and 128 GB RAM

- NI Admin Server → Machine 1 → 4 OCPU → 2 GB RAM

- NI Proxy → Machine 1 → 4 OCPU → 2 GB RAM
- NI MS1→ Machine 1 → 4 OCPU → 24 GB RAM
- NI MS2 → Machine 2 → 4 OCPU → 28 GB RAM
- NI MS3 → Machine 3 → 4 OCPU → 28 GB RAM
- NI MS4 → Machine 4 → 4 OCPU → 28 GB RAM

> **Note:**
>
> It is recommended to reserve approximately 4 GB of RAM accessible for Linux utility tasks rather than using the entire 32 GB of RAM of the system for NI application processes.

Table 2-12 Hardware Sizing Guideline for Network Integrity Deployment

System Size and Range	Linux	Oracle Database Server	Sample Scan Configuration
Small • Up to 20k device • Up to 50k assimilated topology	• CPU: 4 x 4 core - 2.55 GHz • AMD EPYC™ 77J3: 8 threads • RAM: 4 x 32 GB • HDD: 4 X 150 GB	• CPU: 1 x 8 core - 2.55 GHz • AMD EPYC™ 77J3: 16 threads • RAM: 1 x 120 GB • Initial storage: 500 GB • Network Integrity tablespace: 200 GB	Up to 20k device • **Scenario 1:** Four scan for 5k chunk size for optical domain covering 20k device. • **Scenario 2:** Ten scan for 2k chunk size for IP domain covering 20k device. • **Scenario 3:** Five scans for a 2k chunk size for IP domains spanning 10k devices and two scans for a 5k chunk size for Optical domain spanning 10k devices. Up to 50k assimilated topology • **Scenario 1:** One scan for 50k chunk size covering 50k SDH assimilated topology. • **Scenario 2:** One scan for 50k chunk size covering 50k DWDM assimilated topology. • **Scenario 3:** One scan for a 25k chunk size for SDH domains spanning 25k SDH topology and one scans for a 25k chunk size for DWDM domain spanning 25k DWDM topology.

Table 2-12 (Cont.) Hardware Sizing Guideline for Network Integrity Deployment

System Size and Range	Linux	Oracle Database Server	Sample Scan Configuration
Medium • Up to 50k device • Up to 100k assimilated topology	• CPU: 8 x 4 core - 2.55 GHz • AMD EPYC™ 77J3: 16 threads • RAM: 8 x 32 GB • HDD: 8 X 150 GB	• CPU: 2 x 16 core - 2.55 GHz • AMD EPYC™ 77J3: 64 threads • RAM: 2 x 240 GB • Initial storage: 800 GB • Network Integrity tablespace - 300 GB	Up to 50k device • **Scenario 1:** Ten scans for 5k chunk size for optical domain covering 50k device. • **Scenario 2:** Twenty five scans for 2k chunk size for IP domain covering 50k device. • **Scenario 3:** Ten scans for a 2k chunk size for IP domains spanning 20k devices and six scans for a 5k chunk size for Optical domain spanning 30k devices. Up to 100k assimilated topology • **Scenario 1:** One scan for 100k chunk size covering 100k SDH assimilated topology. • **Scenario 2:** One scan for 100k chunk size covering 100k DWDM assimilated topology. • **Scenario 3:** One scan for a 50k chunk size for SDH domains spanning 50k SDH topology and one scans for a 50k chunk size for DWDM domain spanning 50k DWDM topology.

Table 2-12 (Cont.) Hardware Sizing Guideline for Network Integrity Deployment

System Size and Range	Linux	Oracle Database Server	Sample Scan Configuration
Large • Up to 75k device • Up to 200k assimilated topology	• CPU: 12 x 4 core - 2.55 GHz • AMD EPYC™ 77J3: 64 threads • RAM: 12 x 32 GB • HDD: 12 X 150 GB	• CPU: 2 x 24 core - 2.55 GHz • AMD EPYC™ 77J3: 96 threads • RAM: 2 x 320 GB • Initial storage: 2 TB • Network Integrity tablespace: 400 GB	Up to 75k device • **Scenario 1:** Fifteen scans for 5k chunk size for optical domain covering 75k device. • **Scenario 2:** Thirty eight scans for 2k chunk size for IP domain covering 75k device. • **Scenario 3:** Ten scans for 2k chunk size for IP domains spanning 20k devices and eleven scans for 5k chunk size for Optical domain spanning 55k devices. Up to 200k assimilated topology • **Scenario 1:** Two scans for 100k chunk size covering 100k SDH assimilated topology. • **Scenario 2:** Two scans for 100k chunk size covering100k DWDM assimilated topology. • **Scenario 3:** One scan for a 100k chunk size for SDH domains spanning 100k SDH topology and one scans for a 100k chunk size for DWDM domain spanning 100k DWDM topology.

Table 2-12 (Cont.) Hardware Sizing Guideline for Network Integrity Deployment

System Size and Range	Linux	Oracle Database Server	Sample Scan Configuration
Extra-large • Up to 200k device • Up to 400k assimilated topology	• CPU: 16 x 4 core: 2.55 GHz • AMD EPYC™ 77J3: 112 threads • RAM: 16 x 32 GB • HDD: 16 X 150 GB	• CPU: 2 x 24 core - 2.55 GHz • AMD EPYC™ 77J3: 96 threads • RAM: 2 x 320 GB • Initial storage: 3.5 TB • Network Integrity tablespace: 500 GB	Up to 200k device • **Scenario 1:** Forty scans for 5k chunk size for optical domain covering 200k device. • **Scenario 2:** Hundred scans for 2k chunk size for IP domain covering 200k device. • **Scenario 3:** Ten scans for 2k chunk size for IP domains spanning 20k devices and thirty six scans for a 5k chunk size for Optical domain spanning 180k devices. Up to 400k assimilated topology • **Scenario 1:** Four scans for 100k chunk size covering 400k SDH assimilated topology. • **Scenario 2:** Four scans for 100k chunk size covering 400k DWDM assimilated topology. • **Scenario 3:** Two scans for 100k chunk size for SDH domains spanning 200k SDH topology and two scans for a 100k chunk size for DWDM domain spanning 200k DWDM topology.

Note:

Tablespace needs to be increased periodically, based on the scan's frequency and data volume.

3
Installing and Configuring the Oracle Database

This chapter describes the process of installing the Oracle database and configuring the Oracle Database for Oracle Communications Network Integrity.

Oracle Database Installation

Network Integrity must be installed in an Oracle Database tablespace. See Table 2-2 for database requirements.

For information on installing Oracle Database, see the Oracle Database installation documentation.

> **Note:**
>
> Configure the Oracle Database with the XDB component.

Oracle Database Configuration

The Oracle database must be configured for Network Integrity. Specifically, this section covers the following:

- Creating a Tablespace for Network Integrity
- Setting the Database Time Zone
- Creating the Database (MetaData) Schema for Network Integrity
- Installing and Configuring Database Real Application Clusters
- Tuning the Database

Creating a Tablespace for Network Integrity

Create a Network Integrity specific tablespace according to the Oracle Database documentation. See Hardware Sizing Considerations for tablespace sizing guidelines.

Setting the Database Time Zone

Oracle Database must have the correct time zone setting, because Network Integrity uses the datatype TIMESTAMP WITH LOCAL TIME ZONE in its database schema.

See Oracle Database Globalization Support Guide for information and instructions on setting the time zone.

> **Note:**
>
> After Network Integrity has been installed, the database time zone cannot be changed. Ensure the time zone is correctly set before installing Network Integrity.

Creating the Database (MetaData) Schema for Network Integrity

The MetaData schema is an Oracle Fusion Middleware component that is required by Network Integrity. You create the schema using the Repository Creation Utility (RCU).

> **Note:**
>
> A new schema must be created for all new Network Integrity installations. Upgrade installations will use the schema created during the installation of that Network Integrity instance.
>
> The Repository Creation Utility can run on the Linux (32-bit) and Microsoft Windows platforms. A Linux or Windows system can be used to remotely access and configure the database.

To create the schema for Network Integrity using RCU:

1. Export the environment variables by running one of the following commands:

   ```
   export JAVA_HOME=$JDK_HOME
   ```

   or

   ```
   export ORACLE_HOME=$mw_home
   ```

2. Run the following command:

   ```
   ./MW_Home/oracle_common/bin/rcu
   ```

   where *MW_Home* is the installation directory of Oracle Fusion Middleware.

   The Welcome screen of the Repository Creation Utility appears.

3. Click **Next**.

   The Create Repository screen appears.

4. Select **Create Repository** and click **Next**.

   The Database Connection Details screen appears.

5. Do the following:

   a. From the **Database Type** list, select **Oracle Database**.

   b. In the **Host Name** field, enter the database system host name or IP address.

   c. In the **Port** field, enter the port number for the system hosting the database.

   d. In the **Service Name** field, enter the service name.

   e. In the **Username** field, enter the user name for the database user.

> **Note:**
>
> This user account must have the following privileges: CATALOG, CONNECT, Create User, Create Session, Grant Any Privilege, Grant Any Role, Select Any Table, Select any Dictionary.

> **Caution:**
>
> You must use the same user name and password when providing database user information during Network Integrity installation.

f. In the **Password** field, enter the password for the database user.

g. From the **Role** list, select **SYSDBA**.

h. Click **Next**.

The Checking Global Prerequisites screen appears, displaying the progress of establishing the connection with the specified database.

i. Click **OK**.

The Select Components screen appears.

6. On the Select Components screen, do the following:

a. Select **Create new Prefix** and enter the prefix value.

The prefix is any appropriate name for your schema. RCU adds a suffix to this name.

b. Expand **Oracle AS Repository Components**.

c. Expand **AS Common Schemas** and select **Metadata Services**, **Audit Services**, **Audit Services Append**, **Audit Services Viewer**, and **Oracle Platform Security Services**.

> **Note:**
>
> The Service Table (*prefix*_**STB** & *prefix*_**WLS**) schema is a default selection and you cannot change this selection.
>
> where:
>
> *prefix* is the prefix that you define in step 6.a.

d. Click **Next**.

The Checking Component Prerequisites screen appears, displaying the progress of the component prerequisites check before the schemas are created.

e. Click **OK**.

The Schema Passwords screen appears.

7. Select **Use same passwords for all schemas**.

8. In the **Password** field, enter the password for the schema.

9. In the **Confirm Password** field, enter the password for the schema again and click **Next**.

The Map Tablespaces screen appears.

10. Review the entries on the Map Tablespaces screen and click **Next**.

    The Summary screen appears.

11. Review and verify the information you have provided and click **Create**.

    The Completion Summary screen appears, displaying details of the newly created repository.

12. Click **Close**.

Installing and Configuring Database Real Application Clusters

Oracle recommends Oracle Real Application Clusters (RAC) for high availability and scalability if your network data requires multiple databases for storage purposes. Refer to the Oracle Real Application Clusters documentation on the Oracle Help Center.

Tuning the Database

Table 3-1 and Table 3-2 provide the recommended database parameters for tuning your database for the Network Integrity installation. These are the minimum requirements for Network Integrity.

Table 3-1 Database Creation Parameters

Parameter	Recommended Value
SGA+PGA	At least 4 GB in total. Oracle recommends that you use as much memory as you have available in the system, and also use Automatic Memory Management.
Processes	2000
Connection mode	Dedicated server
Redo log file size	1024 MB

Table 3-2 Database Initialization Parameters

Parameter	Recommended Value
db_file_multiblock_read_count	16
distributed_lock_timeout	7200
dml_locks	9700
job_queue_processes	10
log_buffer	31457280
open_cursors	5000
parallel_max_servers	640
plsql_code_type	NATIVE

4

Installing and Configuring Oracle WebLogic Server

Oracle Communications Network Integrity is installed and run on an instance of the WebLogic Administration Server. This chapter describes procedures relating to installing the WebLogic Administration Server and other required applications, and also configuring the WebLogic Server domain where you install Network Integrity.

> **Note:**
>
> Ensure that the Administration Server is running in the WebLogic Server domain before you install Network Integrity.

Installation and configuration tasks include:

- Installing JDK
- Downloading and Installing WebLogic Server
- Installing Application Development Runtime
- Creating/Extending a WebLogic Server Domain for a Single Managed Server Installation
- Creating a WebLogic Server Domain for a Server Cluster Installation
- Configuring Automatic Service Migration (ASM) on the WebLogic Server

About Java Requirements

Oracle WebLogic Server is a Java application and needs a Java environment in which to run. See "Required Software" for information about Java version requirements.

Installing JDK

Download JDK for the required platform from the Oracle Technology Network Web site:

`http://www.oracle.com/technology`

For information on installing JDK, see the JDK installation documentation.

Downloading and Installing WebLogic Server

Oracle WebLogic Server is available as a component of the Oracle Fusion Middleware software.

Download Oracle WebLogic Server from the Network Integrity software on the Oracle software delivery website:

`https://edelivery.oracle.com/`

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

Installing Patches

After you install Oracle WebLogic Server, you must install any applicable patches.

See "Required Software" for information about patches for Oracle WebLogic Server.

Download the required patches from the My Oracle Support Web site:

`https://support.oracle.com`

You apply patches using the OPatch tool. For information about downloading and applying patches, see *Oracle Fusion Middleware Install, Patch and Upgrade* at this website:

`https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/install-patch-tasks.html`

For additional information about using the OPatch tool, refer to this document:

`https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/opatc/patching-opatch.pdf`

Installing Application Development Runtime

Download Oracle Application Development Runtime from the Network Integrity software on the Oracle software delivery website:

`https://edelivery.oracle.com/`

For installing Oracle Application Development Runtime, see the Oracle Fusion Middleware documentation on the Oracle Help Center.

> **Note:**
>
> The Oracle Fusion Middleware Application Developer Installer installs both Oracle Application Development Runtime and Oracle Enterprise Manager.
>
> Install Application Developer with the same credentials used to install WebLogic Server.

For more information on the Application Development Framework, see Oracle Fusion Middleware Understanding Oracle Application Development Framework.

Installing Patches

After you install Oracle Application Development Runtime, you must install any applicable patches.

See "Required Software" for information about patches for Oracle Application Development Runtime.

Download the required patches from the My Oracle Support Web site:

`https://support.oracle.com`

Apply the patches using the OPatch tool.

Creating/Extending a WebLogic Server Domain for a Single Managed Server Installation

You extend the WebLogic Server domain when upgrading Network Integrity.

Before creating or extending a WebLogic Server domain, you must have finished installing Oracle Application Development Runtime. See "Installing Application Development Runtime" for more information.

To create or extend a WebLogic Server domain for a single managed server:

1. Go to *MW_Home*/**oracle_common/common/bin** and run the WebLogic domain configuration script:

   ```
   ./config.sh
   ```

   The Configuration Type screen of the Fusion Middleware Configuration Wizard appears.

2. Select the **Create a new domain** option and in the **Domain Location** field, enter the full path for the domain or click **Browse** to navigate to the directory in which your domains are located, and then click **Next**.

   The Templates screen appears.

3. Select the **Create Domain Using Product Templates** option and from the provided list, select the following products:

   - **Basic WebLogic Server Domain - 12.2.1.4 [wlserver]** (This product is selected by default and you cannot deselect it.)
   - **Oracle Enterprise Manager - 12.2.1.4 [em]**
   - **Oracle JRF - 12.2.1.4 [oracle_common]**
   - **WebLogic Coherence Cluster Extension - 12.2.1.4 [wlserver]**

   > **Note:**
   >
   > The selection of the **WebLogic Coherence Cluster Extension** template for this step does not imply or require the use of the Oracle Coherence product.

4. Click **Next**.

   The Application Location screen appears.

   The **Domain name** and **Domain location** fields are populated by default.

5. In the **Application location** field, enter the path and directory for the application files. For example, enter the value:

   MW_Home/user_projects/applications/*application_name*

6. Click **Next**.

   The Administrator Account screen appears.

7. In the **Name** field, enter the administrator user name.

8. In the **Password** field, enter the administrator user password. The password must be a minimum of 8 alphanumeric characters, and must contain at least one number or special character.

   In the **Confirm Password** field, reenter your password.

9. Click **Next**.

   The Domain Mode and JDK screen appears.

10. In the Domain Mode section, select the **Production** option.

    In the JDK section, select the required JDK.

11. Click **Next**.

    The Database Configuration Type screen appears.

12. Select the **RCU Data** option and enter the connection information that you specified for the Service Table (STB) schema component in the Repository Creation Utility (RCU):

    a. In the **Vendor** field, select the vendor name for the component schema.

    b. In the **DBMS/Service** field, enter the database management system or service name for the component schema.

    c. In the **Driver** field, select the driver used by the component schema.

    d. In the **Host Name** field, enter the host name/IP address for the component schema.

    e. In the **Port** field, enter the port number used by the schema component.

    f. In the **Schema Owner** field, enter the owner name for the schema component.

    > **Note:**
    >
    > The default schema owner name is *prefix*_**STB**, where *prefix* is the prefix that you defined in RCU for the Service Table schema.

    g. In the **Schema Password** field, enter the password for the schema component.

    h. Click **Get RCU Configuration**, which retrieves the schema information.

    i. After the schema information is retrieved successfully, click **Next**.

       The JDBC Component Schema screen appears.

13. Verify the values in the fields and click **Next**.

    The Test Component Schema screen appears, which enables you to test the configurations for the schemas.

14. Select the check boxes beside the schemas you want to test and click **Test Selected Connections**.

15. Verify that all the JDBC component connections pass the validation test and click **Next**.

    The Advanced Configuration screen appears.

16. Select the services to install in the WebLogic Server domain:

    - **Administration Server**
    - **Managed Servers, Clusters and Coherence**
    - **Deployments and Services**

> **Note:**
>
> Oracle recommends that production environments for Network Integrity use a minimum of an Administration Server and one or more Managed Servers or Clusters. Lab environments can be installed on an Administration Server only, if desired.
>
> If you select only **Administration Server**, the Domain Creation wizard does not display some dialog boxes pertaining to managed servers or clusters.
>
> The selection of the **WebLogic Coherence Cluster Extension** template does not imply or require the use of the Oracle Coherence product.

17. Click **Next**.

    The Administration Server screen appears.

18. Do the following:

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

       This single server serves as the Network Integrity domain Administration Server.

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

       > **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.

    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.

    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.

    g. Click **Next**.

       The Managed Servers screen appears.

19. Do the following:

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

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

       > **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.

c. In the **Listen Port** field, enter the number of the port where the managed server listens for incoming messages.

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

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

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. (Optional) Create additional managed servers as required on your Network Integrity deployment by clicking **Add**, and then configure the settings for the new managed servers.

g. Click **Next**.

   The Clusters screen appears.

20. Click **Next** until the Deployments Targeting screen appears.
21. Under **Targets**, select the Administration Server; under **Deployments**, select the deployments; and then click the right arrow, which moves the applications to the Administration Server for deployment.
22. Repeat step 21 to target applications for deployment on the Network Integrity target server.
23. Click **Next**.

    The Services Targeting screen appears.
24. Under **Services**, select the services; under **Targets**, select the Administration Server, and then click the right arrow, which moves the services to the Administration Server.
25. Repeat step 24 to target services to the Network Integrity target server.
26. Click **Next**.

    The Configuration Summary screen appears.
27. 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.
28. Click **Finish**.

    See Oracle Fusion Middleware documentation for more information.
29. To set memory requirements, see "Setting Memory Requirements for Network Integrity".
30. Continue with the procedures in "Starting the WebLogic Server".

    You can now log in to the Administration console and start the Administration Server manually.

Setting Memory Requirements for Network Integrity

You must set appropriate memory requirement values in the WebLogic server to be able to install multiple cartridges after Network Integrity installation. Not allotting enough memory space for the WebLogic domain can cause errors during cartridge deployment.

The following example shows the entries in the **setDomainEnv.sh** file for setting the memory requirement values for Network Integrity:

1. In the WebLogic domain bin folder, open the **setDomainEnv.sh** file.
2. Set the memory arguments for your JVM as follows:

```
WLS_MEM_ARGS_64BIT="-Xms20g -Xmx20g"
```

> **Note:**
>
> Although these values can be adjusted based on system memory availability, when using high-end systems, the above configuration is recommended for running Network Integrity.

Creating a WebLogic Server Domain for a Server Cluster Installation

A server cluster arrangement is used for load balancing, scalability, and failover. 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 as one unit, rather than as several independent processing units. This is the configuration Oracle recommends because it provides protection if a server fails.

When working with a cluster, install the Cartridge Management Web Services (CMWS) and Network Integrity adapters on the system where the Administration server is running.

> **Caution:**
>
> Ensure that you run the Network Integrity Installer from the Administration server.

Installation Scenario

This installation scenario includes two clustered Managed Servers (networkintegrity01 and networkintegrity02) that are separate from the Administration Server, an Administration server, and a hardware load balancer, used for load balancing. Managed Servers are instances of WebLogic used to host enterprise applications, in this case, Network Integrity.

> **Note:**
>
> For more information on configuring the load balancer, see "Configuring the Server Load Balancer" in *Network Integrity System Administrator's Guide.*

This example uses a shared disk storage environment.

The advantages of using shared disk storage are: easier Network Integrity installation, maintenance, and cartridge deployment.

Using shared disk storage allows the Administration Server and all of the managed servers in the cluster to use the same instance of WebLogic. The systems on which the servers reside must have access to the shared storage.

Network Integrity does not support session replication; however, Network Integrity does support server failover.

Server Cluster Example

Refer to the values in Table 4-1 and Table 4-2 to set up the cluster arrangement.

Table 4-1 Server Cluster Example Values

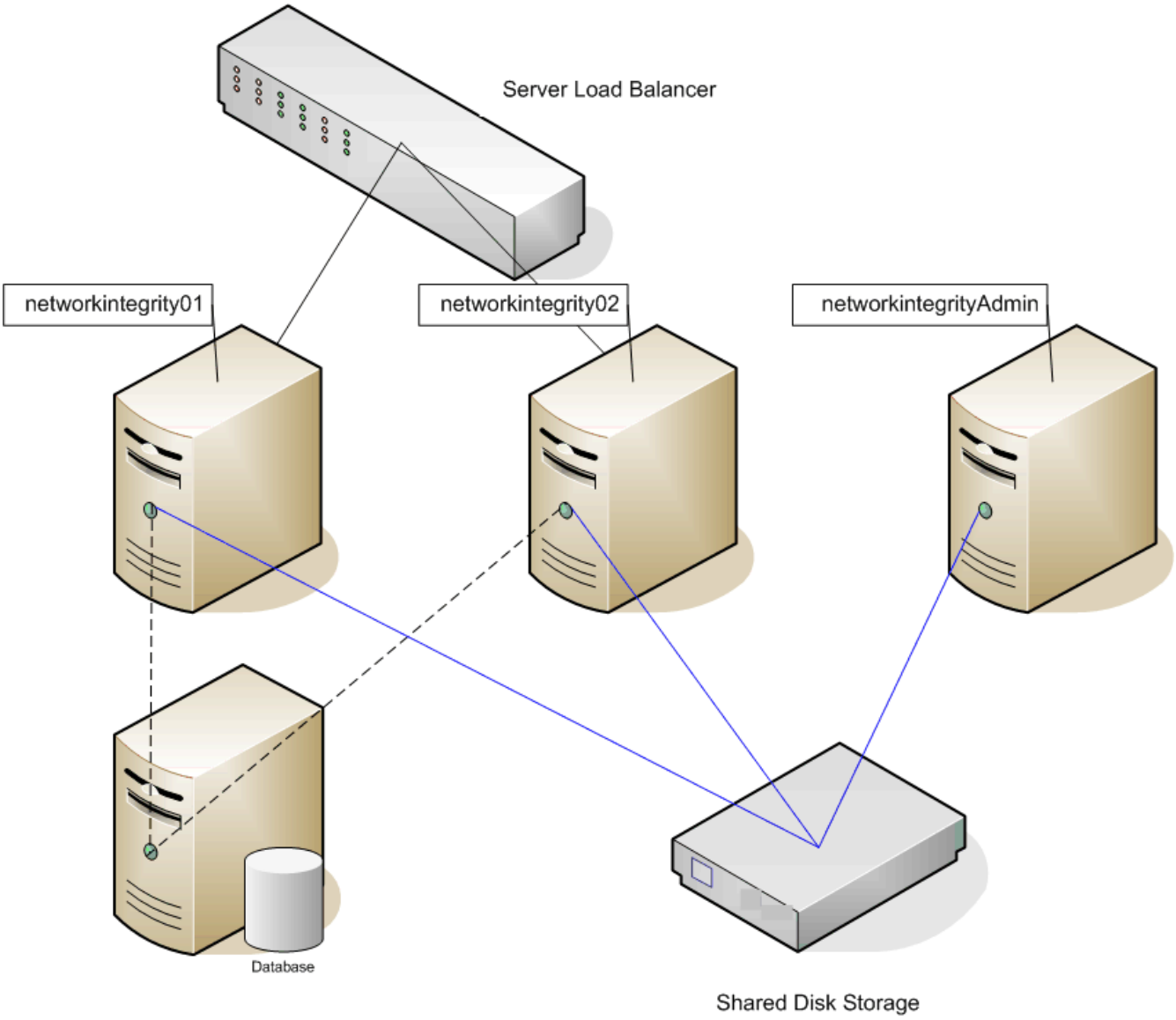
Value	Example
Domain_Home	*WL_Home*/**user_projects/domains/networkintegritycluster**
Domain login	weblogic
Domain password	networkintegritycluster1
Cluster DNS	NetworkIntegrityClusterDNS (It includes the networkintegrity01 and networkintegrity02 listening IP addresses.)

Table 4-2 Servers in a Sample Cluster

Value	Administration Server	Cluster-managed Server #1	Cluster-managed Server #2
WebLogic server	networkintegrityAdmin	networkintegrity01	networkintegrity02
Listening port	*IP_Address*:8063	*IP_Address*:8065	*IP_Address*:8066
Machine	NETINT1	NETINT2	NETINT3

Figure 4-1 shows the servers in a sample server cluster.

Figure 4-1 Servers in a Sample Cluster



Network Integrity Server Cluster Prerequisites

The prerequisites for setting up a Network Integrity server cluster are:

- Oracle WebLogic administration experience.
- A hardware load balancer is required. Refer to the server load balancer configuration for details.
- A DNS entry containing all of the cluster-managed servers' listening addresses serves as the Network Integrity cluster address.
- A system that hosts multiple cluster-managed servers must be multi-homed.
- All cluster-managed servers must reside in the same subnet for multicast traffic.
- Multicast is used for WebLogic cluster heartbeats and JNDI updates.

- Ensure that multicasts do not collide in the same domain and other domains.

Overview of Steps for Setting Up Network Integrity on a Server Cluster

> **Note:**
>
> The figures shown in this section are for reference only. The actual server names that you use may be different from those shown in the figures.

For the considered scenario, installing Network Integrity on an Oracle WebLogic Server cluster arrangement involves:

- Installing Oracle WebLogic Server and Network Integrity software on the shared disk storage.
- Deleting all JMS resources.
- Creating server instances for each WebLogic server in your system, and creating your cluster.
- Deploying the Network Integrity data source and the Network Integrity transaction data source on the cluster.
- Modifying the startup script on the shared disk storage.
- Manually modifying the **config.xml** file.
- Starting up the Administration Server and all cluster-managed servers.
- Logging in to Network Integrity through the server load balancer.

Installing WebLogic Server and Network Integrity in a Clustered Environment

Before creating a WebLogic Server domain, you must have finished installing Oracle Application Development Runtime. See "Installing Application Development Runtime" for more information.

Install WebLogic on the shared disk storage.

After you install WebLogic:

- Create a domain
- Start the WebLogic server
- Install Network Integrity

Creating a Domain

To create a domain:

1. Go to *MW_Home*/**oracle_common/common/bin** and run the WebLogic domain configuration script:

   ```
   ./config.sh
   ```

   The Configuration Type screen of the Fusion Middleware Configuration Wizard appears.

2. Select the **Create a new domain** option and in the **Domain Location** field, enter the full path for the domain or click **Browse** to navigate to the directory in which your domains are located, and then click **Next**.

   The Templates screen appears.

3. Select the **Create Domain Using Product Templates** option and from the provided list, select the following products:

   - **Basic WebLogic Server Domain - 12.2.1.4 [wlserver]** (This product is selected by default and you cannot deselect it.)
   - **Oracle Enterprise Manager - 12.2.1.4 [em]**
   - **Oracle JRF - 12.2.1.4 [oracle_common]**
   - **WebLogic Coherence Cluster Extension - 12.2.1.4 [wlserver]**

   > **Note:**
   >
   > The selection of the **WebLogic Coherence Cluster Extension** template for this step does not imply or require the use of the Oracle Coherence product.

4. Click **Next**.

   The Application Location screen appears.

   The **Domain name** and **Domain location** fields are populated by default.

5. In the **Application location** field, enter the path and directory for the application files. For example, enter the value:

   MW_Home/user_projects/applications/*application_name*

6. Click **Next**.

   The Administrator Account screen appears.

7. In the **Name** field, enter the administrator user name.

8. In the **Password** field, enter the administrator user password. The password must be a minimum of 8 alphanumeric characters, and must contain at least one number or special character.

   In the **Confirm Password** field, reenter your password.

9. Click **Next**.

   The Domain Mode and JDK screen appears.

10. In the Domain Mode section, select the **Production** option.

    In the JDK section, select the required JDK.

11. Click **Next**.

    The Database Configuration Type screen appears.

12. Select the **RCU Data** option and enter the connection information that you specified for the Service Table (STB) schema component in the Repository Creation Utility (RCU):

    a. In the **Vendor** field, select the vendor name for the component schema.

    b. In the **DBMS/Service** field, enter the database management system or service name for the component schema.

    c. In the **Driver** field, select the driver used by the component schema.

d. In the **Host Name** field, enter the host name/IP address for the component schema.

e. In the **Port** field, enter the port number used by the schema component.

f. In the **Schema Owner** field, enter the owner name for the schema component.

> **Note:**
>
> The default schema owner name is *prefix*_**STB**, where *prefix* is the prefix that you defined in RCU for the Service Table schema.

g. In the **Schema Password** field, enter the password for the schema component.

h. Click **Get RCU Configuration**, which retrieves the schema information.

i. After the schema information is retrieved successfully, click **Next**.

The JDBC Component Schema screen appears.

13. Verify the values in the fields and click **Next**.

The Test Component Schema screen appears, which enables you to test the configurations for the schemas.

14. Select the check boxes beside the schemas you want to test and click **Test Selected Connections**.

15. Verify that all the JDBC component connections pass the validation test and click **Next**.

The Advanced Configuration screen appears.

16. Select the services to install in the WebLogic Server domain:

- **Administration Server**
- **Managed Servers, Clusters and Coherence**
- **Deployments and Services**

> **Note:**
>
> Oracle recommends that production environments for Network Integrity use a minimum of an Administration Server and one or more Managed Servers or Clusters. Lab environments can be installed on an Administration Server only, if desired.
>
> If you select only **Administration Server**, the Domain Creation wizard does not display some dialog boxes pertaining to managed servers or clusters.
>
> The selection of the **WebLogic Coherence Cluster Extension** template does not imply or require the use of the Oracle Coherence product.

17. Click **Next**.

The Administration Server screen appears.

18. Do the following:

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

This single server serves as the Network Integrity domain Administration Server.

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

> **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.

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.

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.

g. Click **Next**.

   The Managed Servers screen appears.

19. Do the following:

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

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

> **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.

c. In the **Listen Port** field, enter the number of the port where the managed server listens for incoming messages.

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

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

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. (Optional) Create additional managed servers as required on your Network Integrity deployment by clicking **Add**, and then configure the settings for the new managed servers.

g. Click **Next**.

   The Clusters screen appears.

20. 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.

d. Click **Next**.

The Assign Servers to Clusters screen appears.

21. Assign the servers to the cluster by moving the managed servers in the left pane to the required cluster in the right pane.
22. Click **Next**.

The HTTP Proxy Applications screen appears.

23. (Optional) Select **Create HTTP Proxy** for any proxy servers in the list.

> **Note:**
>
> If you configure an HTTP proxy server to act as a frontend host for the cluster, ensure that you configure the Frontend URL in the Administration Console after the WebLogic domain is created successfully. See "Configuring the Frontend URL in Administration Console" for more information.

24. Click **Next**.

The Coherence Clusters screen appears, displaying the Coherence cluster that is automatically added to the domain.

This screen appears only if you included Coherence in the WebLogic Server installation.

25. Do the following if you included Coherence in the installation:
    a. In the **Name** field, accept the default cluster name or type a new name for the Coherence cluster.
    b. In the **Coherence Listen Port** field, enter the port number to use as the Coherence cluster listen port.
26. Click **Next**.

The Machines screen appears.

Use this screen to change the configuration information for the systems. A computer is the logical expression of the system that hosts one or more WebLogic Server instances. The Administration Server and the Node Manager application use the system definition to start remote servers.

27. (Optional) Add the systems by doing one of the following:
    - Select the **Machine** tab, and do the following:
      a. Click **Add** to create the first system.
      b. In the **Name** field, enter a name for the system.
      c. In the **Node Manager Listen Address** field, enter the host, or IP address of the node manager.
      d. In the **Node Manager Listen Port**, enter the port number for the node manager.
      e. Create further systems as required on your Network Integrity deployment.
      f. Click **Next**.

         The Assign Servers to Machines screen appears.

- Select the **UNIX Machine** tab, and do the following:
  a. Click **Add** to create the first UNIX system.
  b. If required, select the **Enable Post Bind GID** check box. The default state is deselected.
  c. In the **Post Bind GID** field, enter a value or select the default.
  d. If required, select the **Enable Post Bind UID** check box. The default state is deselected.
  e. In the **Post Bind UID** field, enter a value or select the default.
  f. In the **Node Manager Listen Address** field, enter the host, or IP address of the node manager.
  g. In the **Node Manager Listen Port** field, enter the port number of the node manager.
  h. (Optional) Create further systems or UNIX systems as required on your Network Integrity deployment.
  i. Click **Next**.

     The Assign Servers to Machines screen appears.

28. Assign the servers to the machines by moving the servers in the left pane to the required machine in the right pane.
29. Click **Next**.

    The Deployments Targeting screen appears.
30. Under **Targets**, select the Administration Server; under **Deployments**, select the applications; and then click the right arrow, which moves the applications to the Administration Server for deployment.
31. Repeat step 30 to target applications for deployment on the cluster.
32. Click **Next**.

    The Services Targeting screen appears.
33. Under **Targets**, select the Administration Server, under **Services**, select the services; and then click the right arrow, which moves the services to the Administration Server.
34. Repeat step 33 to target services (libraries) to the cluster.
35. Click **Next**.

    The Configuration Summary screen appears.
36. 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.
37. Click **Finish**.

    See Oracle Fusion Middleware documentation for more information.
38. To set memory requirements, see "Setting Memory Requirements for Network Integrity".
39. Continue with the procedures in "Starting the WebLogic Server".

    You can now log in to the Administration console and start the Administration Server manually.

> **Note:**
>
> Create domains for remote system in the same manner, in the respective systems.

Starting the WebLogic Server

To start the WebLogic server:

1. Open a command window.
2. Go to the *Domain_Home*/**bin** and enter the command:

   ```
   ./startWebLogic.sh
   ```

   The script starts the WebLogic server.
3. Verify that the server started by logging in to the WebLogic server administration console or by checking the log files.

   To access the WebLogic server administration console:

   a. Go to:

      ```
      http://Host_Name:Port/console
      ```

      where *Host_Name* is the name of the Administration Server name or IP address and *Port* is the Administration Server port number.

   b. Enter the WebLogic server administration user name and password.

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

      The Summary of Servers screen appears.

   d. View the **State** of the server and see RUNNING.

      If the State is not RUNNING, you may need to wait a short period and refresh the page.
4. Look at the bottom of the Administration Server command window.

   The command window should contain the following lines:

   ```
   Server state changed to RUNNINGServer started in RUNNING mode
   ```

Starting the Cluster Member Servers

> **Note:**
>
> If you have configured the node manager, you can start the Network Integrity cluster member servers using the WebLogic Administration Console.

> **Note:**
>
> If the managed servers are started simultaneously, the *javax.naming.NameNotFoundException* error message is displayed for JMS queues created under JDJMSModule module. To prevent this error message from being displayed, do not start the managed servers simultaneously.

To start the cluster member servers:

1. Log in to the first cluster server system.
2. Go to the *DOMAIN_Home***/bin** directory.
3. Start the cluster server using the following command processed from the system where the managed server is defined:

   ```
   ./startManagedWebLogic.sh cluster_managed_server_name admin_server_URL
   ```

4. Start the second server by using the following command processed from the system where the managed server is defined:

   ```
   ./startManagedWebLogic.sh cluster_managed_server_name admin_server_URL
   ```

5. To view the log file for each of the managed servers to verify that the server is in RUNNING mode, in a command window, enter:

   ```
   tail -f Managed_Server_1.log
   tail -f Managed_Server_2.log
   ```

6. Look at the end of the managed server log files.

   The log files should contain the following lines:

   ```
   Server state changed to RUNNING
   Server started in RUNNING mode
   ```

   If you encounter errors (returned to the terminal, and contained in WebLogic Server domain and server logs) about the *Stuck Thread Max Time*: value being exceeded during these processes, see "Configuring the WebLogic Server StuckThreadMaxTime Value ".

7. Log in to the WebLogic console to check all of the cluster server states.
8. Go to:

   ```
   http://Host_Name:Port/console
   ```

   where *Host_Name* is the name of the Administration Server name or IP address and *Port* is the Administration Server port number.

9. Enter the WebLogic server administration user name and password.
10. Select Servers and verify that the State of all servers is RUNNING. If you encounter

> **Note:**
>
> To configure the Node Manager, see the Oracle WebLogic documentation on the Oracle Help Center:
>
> http://docs.oracle.com

Configuring the WebLogic Server StuckThreadMaxTime Value

During the installation of Oracle WebLogic Server and Network Integrity in a clustered environment, if the execute thread takes more time than the *Stuck Thread Max Time* declared in WebLogic, a *Stuck Thread Max Time* error is displayed.

Stuck Thread Max Time is a property in WebLogic for performance tuning. It is defined as “the number of seconds that a thread must be continually working before this server considers the thread stuck". The minimum value is 0 seconds; the default is 600 seconds.

Consider setting *Stuck Thread Max Time* from its default 600 seconds to a larger value such as 54000 seconds (15 hours).

Use the WebLogic Console to change this value:

1. Log in to the WebLogic Administration console.
2. In the Home page, select **Environment**.
3. Select **Servers**, and then click **Admin Server**.
4. Select **Configuration**, and then click **Tuning**.
5. Increase the value of *Stuck Thread Max Time* to 54000.
6. Restart your domain. Your changes take effect only after a restart.

Configuring Automatic Service Migration (ASM) on the WebLogic Server

WebLogic server's Automatic Service Migration (ASM) framework monitors the health of JMS services and automatically migrates failing services to healthy and available servers. You configure WebLogic server for automatic service migration for failover and high availability.

For information on configuring Automatic Service Migration (ASM) on the WebLogic server, see Roadmap for Configuring Automatic Migration of JMS-related Services.

> **Caution:**
>
> Not configuring ASM on your WebLogic server results in the Network Integrity installer giving the following warning when launched:
>
> **Migration policy for the target is manual. Recommended value is automatic migration. Refer to the JMS recommendations section of the documentation.**
>
> If you choose not to configure ASM, ignore the warning and continue with the installation.

To configure auto migration for JMS service in a WebLogic cluster:

1. Configured Managed Servers and the Node Manager.
2. Configure the Migration Leasing Basis as follows:
   a. Select the cluster where you are planning Auto JMS Service migration and select the **Migration** tab.

b. Add all systems to **Candidate Machines For Migratable Servers**.

c. Select the Migration Basis as **Consensus**.

d. Save the changes and activate.

3. Configure migratable targets as follows:

   a. Select the migratable target and select the **Migration** tab.

   b. Select **Auto-Migrate Exactly-Once Services** as Service Migration Policy.

   c. Add all Constrained Candidate Servers available.

   d. Repeat these steps for each migratable target associated with member servers in the cluster.

4. Continue with installing Network Integrity.

5. Once Network Integrity is installed, you can verify whether the environment is ready for JMS Service Auto Migration by following these steps:

   a. Select servers and navigate to the **Migration** tab.

   b. All member servers are selected in the **JMS Service Candidate Servers** list.

   c. Repeat these steps for all member servers in the cluster.

Verifying WebLogic Administration Server Migration

To ensure that the WebLogic Administration server has migrated:

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

   The Administration Console Home screen appears.

2. Under Environment select **Migratable Targets**.

   The Summary of Migratable Targets screen appears.

3. Select the **Control** tab to display it.

4. If the WebLogic Administration server has migrated, then, in the Migratable Targets table, the name in the Current Hosting Server column equals the corresponding name in the Name column.

5. In case the servers names showing in the two columns are different, do the following:

   a. Select the check box corresponding to the name, and click **Migrate**.

      The Migrate Migratable Targets screen appears.

   b. From the New hosting server list, select the name of the hosting server and click **OK**.

      The server is migrated.

5

Installing and Configuring Additional Software

This chapter describes the process of installing and configuring additional software to enhance Oracle Communications Network Integrity.

Overview of Additional Installation Tasks

Install and configure the following additional software:

- Oracle Internet Directory
- Oracle Analytics Publisher

Installing and Configuring Oracle Internet Directory

The WebLogic Server includes an embedded LDAP store that acts as the default security provider data store for the Default Authentication, Authorization, Credential Mapping, and Role Mapping providers. You manage the embedded LDAP store using the WebLogic console. The Oracle Universal Installer uses this embedded LDAP server by default as the security provider. During installation, you can change the setting to use third party security providers with the Oracle WebLogic server.

See the WebLogic Server documentation for information on the embedded LDAP server.

You also have the option to use an external LDAP store, or security provider, if your requirements are greater and you need more security options than are provided by the embedded LDAP server.

Oracle recommends Oracle Internet Directory as the LDAP store external to the WebLogic server.

You require the following information to install the Oracle Internet Directory:

- A static IP address

  You require a static IP address to install the Oracle Identity Management suite.
- Oracle Database
- WebLogic Server
- Application Development Runtime
- Identity Management
- Fusion Middleware

For information on installing Oracle Internet Directory, see For information on installing and configuring Oracle Internet Directory, see Oracle Fusion Middleware Installing and Configuring Oracle Identity and Access Management.

Configuring the Authentication Provider

To enable the WebLogic Server to work with an external LDAP store, or Oracle Internet Directory:

1. Log in to the Administration console.
2. Under Your Application's Security Settings, click **Security Realms**.

   The **Summary of Security Realms** screen appears.
3. Select the realm *YourRealmName*, for which you must set the Oracle Internet Directory as the external LDAP store.

   The **Settings For** *YourRealmName* screen appears.
4. Click the **Providers** tab, and in the Providers tab, click the **Authentication** tab.
5. Click **New**.

   The **Create a New Authentication Provider** screen appears.
6. In the **Name** field, enter the name of the authenticator, *AuthenticatorName*.
7. From the **Type** list, select **OracleInternetDirectoryAuthenticator**.
8. Click **OK**.

   The **Settings For YourRealmName** screen appears, showing the newly created Authentication Provider, AuthenticatorName, in the Authentication tab.
9. Click the AuthenticatorName.

   The **Settings for AuthenticatorName** screen appears.
10. In the **Control Flag** list, select **SUFFICIENT**.
11. Click **Save**.
12. Click the **Provider Specific** tab.
13. Under the Connection section, in the following fields, enter the relevant values:
    - Host
    - Port
    - Principal
    - Credentials
    - Confirm Credentials
14. Under the Users section, in the following fields, enter the relevant values:
    - User Base DN

      Ensure that you provide the following value:

      ```
      cn=Users,dc=idc,dc=oracle,dc=com
      ```
    - All User Filter
    - User From Name Filter
    - User Search Scope
    - User Name Attribute
    - User Object Class
15. Under the Groups section, in the following fields, enter the relevant values:
    - Group Base DN

      Ensure that you provide the following value:

      ```
      cn=Groups,dc=idc,dc=oracle,dc=com
      ```

- All Groups Filter
- Group From Name Filter
- Group Search Scope
- Group Membership Searching
- Max Group Membership Search Level

16. Click **Save**.
17. Restart the WebLogic server.
18. Log in to the Administration console.
19. Navigate to the **Settings For** *YourRealmName* screen, and click **Reorder**.

    The **Reorder Authentication Providers** screen appears.
20. Use the Up and Down arrows to reorder the listed Authentication Providers, and click **OK**.

Configuring Custom Authentication Providers

You can configure custom authentication providers for your external security provider. In this case, you are required to manually create users and groups before starting Network Integrity installation.

Create the following groups in the new authentication provider store:

- **JDGroup**
- **NetworkIntegrityRole** (this is a member of the **JDGroup**)

Create a user named **NIUSER** in the new authentication provider store as a member of **NetworkIntegrityRole** and **JDGroup**. Ensure that you create the groups and users in the default security realm.

Installing and Configuring Oracle Analytics Publisher

Installing publishing tools is optional. The requirement is based entirely on your individual requirements.

You can use Oracle Analytics Publisher to host and publish Network Integrity scan-related and other reports.

Download Oracle Analytics Publisher from the Oracle Technology Network Web site:

`http://www.oracle.com/technology`

For information on installing and configuring, see Oracle Analytics Publisher documentation.

See "Software Requirements" for information on the required version of Oracle Analytics Publisher.

6
Installing Network Integrity

This chapter describes how to install Oracle Communications Network Integrity. Before installing Network Integrity, read these chapters:

- Network Integrity Installation Overview
- Network Integrity System Requirements
- Installing and Configuring the Oracle Database
- Installing and Configuring Oracle WebLogic Server
- Installing and Configuring Additional Software

Types of Installation

There are two types of Network Integrity installation:

- **Complete installation**. See "Installing Network Integrity by Using Interactive Install".
- **Installation in silent mode**. See "Installing Network Integrity in Silent Mode".

> **Caution:**
>
> If the installation fails for some reason, you must create a new WebLogic domain and a new database user before you begin installation again.
>
> See "Installing and Configuring the Oracle Database" and "Installing and Configuring Oracle WebLogic Server " for more information.

> **Caution:**
>
> The Network Integrity Installer must be launched from the same system as the one hosting the Administration server of your domain.

Installing Network Integrity by Using Interactive Install

To run the Network Integrity installer, the Java Runtime Environment (JRE) must already be installed. See "Required Software" for more information about the required Java version.

To install Network Integrity:

1. Create a directory (*dir*).
2. Download the software for your operating system from the Oracle software delivery website:

   `https://edelivery.oracle.com`

and save it to *dir*:

3. Extract the contents of the software pack to *dir*.
4. Run the Oracle Universal Installer using the following command:

   ```
   /dir/integrity/Disk1/install/runInstaller -jreloc jre_Path
   ```

   where *jre_Path* contains the **jre** folder inside the Java Development Kit (JDK) installation directory.

   The Installer Welcome screen appears.
5. Click **Next**.
6. One of the following screens is displayed:
   - If Network Integrity is the first Oracle product that you are installing on the system, the Specify Inventory directory and credentials screen appears. Enter the full path of the inventory directory, select the Operating System group name, and then click **Next**.

     The Select Installation Type screen appears. Continue with step 7.

     > **Note:**
     >
     > The inventory directory manages all Oracle products installed on your system.

   - If you have installed any Oracle products on the system prior to installing Network Integrity, the Select Installation Type screen appears. Continue with step 7.
7. Select the type of Network Integrity installation you require, and click **Next**.
   - If you select **Complete**, the Specify Home Details screen appears.

     Skip the next step.
   - If you select **Custom**, the Available Product Components screen appears.

     Continue with the next step.
8. In the Available Product Components screen, select the components you want to install, and click **Next**.
9. In the Specify Home Details screen, do the following:
   a. In the **Name** field, enter a name to identify your installation as an Oracle Product in OUI.
   b. In the **Path** field, enter the path to the folder where you want to install Network Integrity.

      > **Note:**
      >
      > You can also select the name for the installation from the list of names the Installer provides or browse to the location.

   c. Click **Next**.

   The WebLogic Administration Server Connection Information screen appears.
10. Do the following:

a. In the **Host Name** field, enter the IP address or the host name of the Administration Server.

b. In the **Port Number** field, enter the Administration Server port number.

c. In the **User Name** field, enter user name with which you connected to the Administration Server.

> **Note:**
>
> This user should belong to the WebLogic Administrator's group.

d. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

e. Select or deselect the **Use SSL** check box based on your business need.

f. In the Keystore field, enter the keystore location if the **Use SSL** check box is selected.

g. Click **Next**.

The WebLogic Server/Cluster Selection screen appears.

11. Select the option for the server, or cluster, where you want to deploy Network Integrity, and click **Next**.

- If you select Administration server, or a managed server, the Database Type Selection screen appears.

  Skip to step 13.

> **Note:**
>
> If you select a managed server, ensure that the managed server and the node manager are running.

- If you select a cluster server, the Cluster Member Server Selection screen appears.

  Continue with the next step.

12. In the Cluster Member Server Selection screen, select a cluster member for Network Integrity adapters installation, and click **Next**.

The Database Type Selection screen appears.

13. In the Database Type Selection screen, do one of the following.

- Select the **Standard Oracle 19c Enterprise Database** option.

  The Database Connection Information screen appears.

  Do the following:

  a. In the **Host Name** field, enter the IP address or the host name of the system where the database server is installed.

  b. In the **Port Number** field, enter the port number with which the installer connects to the database server.

  c. In the **User Name** field, enter the user name for the database server.

> **Caution:**
>
> You must use the same user name and password that you provided when you set up the database schema using the Repository Creation Utility (RCU).
>
> The user must have the following privileges: CATALOG, CONNECT, Create User, Create Session, Grant Any Privilege, Grant Any Role, Select Any Table, Select any Dictionary.
>
> See "Creating the Database (MetaData) Schema for Network Integrity" for more information.

d. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

e. In the **Service name** field, enter the service name that uniquely identifies your database on the system.

f. Click **Next**.

The Network Integrity Schema User Information screen appears.

- Select the **Oracle 12c Real Application Cluster Database** option.

The RAC DB Nodes Connection Information screen appears.

Do the following:

a. In the **RAC Database Connection String** field, enter the connection details to connect to the Oracle RAC database.

For example:

HOST NAME1:PORT1:SERVICE NAME1;HOST NAME2:PORT2:SERVICE NAME2

b. In the **User Name** field, enter the user name for the Oracle RAC database server.

c. In the **Password** field, enter the password for the user name that you provided in the **User Name** field.

d. Click **Next**.

The Network Integrity Schema User Information screen appears.

14. In the Network Integrity Schema User Information screen, do the following:

> **Note:**
>
> Ensure that the schema owner has an associated MetaData Services (MDS) schema.

> **Caution:**
>
> You must use the same user name and password that you created during the MetaData schema creation. See "Creating the Database (MetaData) Schema for Network Integrity" for more information.

a. In the **Schema User Name** field, enter the name for the MDS schema user.

b. In the **Schema User Password** field, enter the password for the MDS schema user to access the schema.

c. Click **Next**.

The Security Provider Selection screen appears.

15. Select the type of security provider you want to use by performing one of the following steps:

- Select the **Default WebLogic Security Provider (Embedded_LDAP**) option, and click **Next**.

  The Network Integrity User Information screen appears.

- If you select **External Security Provider**, the External Security Provider Connection Information screen appears.

  Do the following:

  a. In the **LDAP Server Host Name** field, enter the host name for the external LDAP server.

  b. In the **LDAP Server Port Number** field, enter the port number for the external LDAP server.

  c. In the **LDAP Server User Name** field, enter the user name for the external LDAP server.

  d. In the **LDAP Server Password** field, enter the password for the external LDAP server.

  e. In the **User Base DN** field, enter the user base DN.

  f. In the **Group Base DN** field, enter the group base DN.

  g. Click **Next**.

  The NI Administrator user creation (Optional) screen appears.

- If you select **Other Security Provider**, and click **Next**, the Reporting Tool Connection (Optional) screen appears.

  Skip to step 20.

16. In the NI Administrator user creation (Optional) screen, do the following:

a. In the **User Name** field, enter the user name for the Network Integrity user.

This user accesses and uses Network Integrity.

b. In the **Password** field, define a password for the Network Integrity user.

> **Note:**
>
> The Network Integrity user password can be a maximum of 12 characters long, and should contain at least one digit, one capital letter, and one non alpha-numeric value; For example, Weblogic@123.
>
> Also, the user name must not be part of the password.

In the **Confirm Password** field, enter the password again to confirm it.

c. Click **Next**.

The NI User ni-internal secure credentials screen appears.

17. Do the following:
    a. In the **User Password** field, define a password for the Network Integrity internal user.

       In the **Confirm The User Password** field, enter the password again to confirm it.
    b. Click **Next**.

       The Disable Unsecured Listen Port screen appears.
18. Select whether or not to disable the unsecured listen port by doing one of the following:
    - Select **Yes** if you are configuring Network Integrity to communicate and listen over SSL-enabled ports.
    - Select **No** if you are not configuring Network Integrity to communicate and listen over SSL-enabled ports.
19. Click **Next**.

    The Reporting Tool Connection (Optional) screen appears.
20. Enter the names of, and links to, the reporting tool(s) you have configured, and click **Next**.

> **Note:**
>
> This is an optional screen. If you do not have any reporting tools configured, click **Next** to continue with the installation.

    The Launch Cartridge Deployer (Optional) screen appears.
21. Select whether to launch the Cartridge Deployer and click **Next**.

> **Note:**
>
> This is an optional screen that only appears for systems installed on the Linux or Solaris operating systems. Clicking **Next** takes you to the next screen if you do not want to make this choice now.
>
> Selecting **Yes** launches the Cartridge Deployer Tool after the successful installation of Network Integrity.

    The Summary screen appears.
22. Review the selections you have made in the preceding screens, and click **Install**.

    The Install screen appears.
23. You can view the installation progress.

> **Note:**
>
> During the installation progress, two popup messages will appear.
>
> The first popup message asks for the confirmation to stop the WebLogic Servers, click **OK**.
>
> The second popup message gives the order in which the servers should be restarted manually. Start the servers, in the order listed in the popup message, and click **OK**, only after all the servers are started.

On successful installation of Network Integrity, the End of Installation screen appears.

> **Note:**
>
> Record the URLs that are displayed in the End of Installation screen, to access Network Integrity.

24. Follow any on-screen instructions to complete the installation.

    You can now access the Network Integrity application.

25. Click **Exit** to close the Installation Wizard.

26. For a Cluster Server installation, do the following:

    a. Edit the **startWebLogic.sh** file under *Domain_Home***/bin/** directory.

    ```
    ${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} -Dweblogic.Name=${SERVER_NAME}
    ```

    -Dweblogic.wsee.useRequestHost=true

    ```
    -Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy ${JAVA_OPTIONS}
    ${PROXY_SETTINGS} ${SERVER_CLASS}

    ${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} -Dweblogic.Name=${SERVER_NAME}
    ```

    -Dweblogic.wsee.useRequestHost=true

    ```
    -Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy ${JAVA_OPTIONS}
    ${PROXY_SETTINGS} ${SERVER_CLASS} >"${WLS_REDIRECT_LOG}" 2>&1
    ```

    b. Stop the AdminServer and restart, using the following command:

    ```
    ./startNI.sh
    ```

    c. Stop the managed servers and restart, using the following command:

    ```
    ./startNI.sh cluster_managed_server_name admin_server_URL
    ```

For information on verifying the successful installation of Network Integrity, see "Verifying the Network Integrity Installation".

Installing Network Integrity in Silent Mode

Use silent install mode when you are installing Network Integrity using the same configuration repeatedly. Silent install mode does not use the GUI and it runs in the background.

About the Response File

The Network Integrity installer uses a response file, which contains a pre-defined set of values, such as server connection details. The response file comes in a template form, to install Network Integrity in silent mode.

The following two response file templates come as part of the Network Integrity installation package:

- **oracle.communications.ni.Complete.rsp**

  Use this file template if you are doing a complete installation.

- **oracle.communications.ni.Custom.rsp**

  Use this file template if you are doing a custom installation.

The response file templates contain all the fields that the installer requires values for to connect to various servers during the silent, unattended installation.

When you untar the Network Integrity package, the response file templates are saved in the **Response** folder at the following location:

integrity/Disk1/stage/Response

Populate the response file with the required server and connection values for the installer to use during installation, before you begin the silent installation. The provided response file is a template with pre-defined places where you fill in the required values of the required type. Shown here is sample section of a response file:

```
#Name       : DATABASE_TYPE
 #Datatype   : String
 #Description:
 #Example: DATABASE_TYPE =
 #------------------------------------------------------------------
 DATABASE_TYPE="Non Clustered-DB"
#------------------------------------------------------------------
#Name       : MANAGED_SERVER_NAME
#Datatype   : String
#Description:
#Example: MANAGED_SERVER_NAME =
#------------------------------------------------------------------
MANAGED_SERVER_NAME="Managed_Server_1"
```

In this section of the response file sample, you would provide values for the following:

```
DATABASE_TYPE=
MANAGED_SERVER_NAME=
```

Similarly, provide values for all variables described in the response file.

Populating the Response File

You can populate the response file in the following ways:

- Recording the response file contents during a GUI installation

  To record the response file contents during a GUI installation:

  1. Use the following command to launch the Network Integrity installer and also record all input values you provide during the installation:

     ```
     ./runInstaller -record -destinationFile Path -silent -jreloc jre_Path
     ```

     where *jre_Path* contains the **jre** folder inside the JDK installation directory.

- Manually populating the response file

  To populate the response file manually:

  1. Go to the following location:

     integrity/Disk1/stage/Response

  2. Open the appropriate RSP template and make a copy for your current requirement.
  3. Enter the required input values in the provided locations.

Starting Silent Mode Installation

Before you begin installing Network Integrity in silent mode, ensure that you have provided all required input values in the response file template.

To install Network Integrity in silent mode:

1. Use the following command, where `path` is the response file location, to start the installation:

   ```
   ./runInstaller -responseFile Path -silent -jreloc jre_Path
   ```

   where *jre_Path* contains the **jre** folder inside the JDK installation directory.

   The installation runs silently in the background.

   > **Note:**
   >
   > The installer shuts down all of the servers, including the Administration Server and the Managed Servers, after a silent installation. Start all of the servers manually after the installation is complete. See "Starting the Cluster Member Servers".

2. Open the following file once the installation is complete, to get the URL to access Network Integrity:

   *NI_Home***/install/readme.txt**

   For example: **/opt/integrity/Oraclecommunications/install/readme.txt**

3. Copy the URL and paste it in the browser window's address field and press **Enter** to access Network Integrity.

   You can now access the Network Integrity application.

For information on verifying the successful installation of Network Integrity, see "Verifying the Network Integrity Installation".

7

Network Integrity Post-Installation Tasks

This chapter provides instructions for Oracle Communications Network Integrity post-installation tasks.

Overview of Network Integrity Post-Installation Tasks

Post-installation tasks for Network Integrity include:

- Managing Network Integrity Cartridges
- Configuring Network Integrity for Inventory Management
- Installing Network Integrity Report Templates
- Starting the AgeOut Process
- Enabling HTTP Tunneling
- Setting Up Oracle Internet Directory

> **Note:**
>
> The following post-installation steps need to be manually carried out:
>
> - Before NI startup, add the following Java option to the *startWeblogic.sh* file:
>
> Dorg.apache.logging.log4j.simplelog.StatusLogger.level=OFF
> - In the case of cluster installation, for expanding Network Integrity from weblogic console deployments, it is necessary to add AdminServer to the targets of the following libraries from weblogic console deployments:
> - oracle.communications.platform.cui.webapp
> - oracle.communications.platform.ies
> - oracle.communications.platform.poms
> - oracle.communications.platform.WsFramework

About the Trusted Certificate for Network Integrity

> **Note:**
>
> Network Integrity uses a demo CA certificate provided by the Oracle WebLogic Server. As a result, when you connect to the Network Integrity UI for the first time, the browser displays a warning page with a message indicating that the security certificate presented is not issued by a trusted certificate authority.
>
> This is expected behavior. Accept this untrusted certificate to continue to connect to Network Integrity UI.

The demo CA certificate provided by the Oracle WebLogic Server, automatically configures the SSL settings in your browser. Configure the SSL, according to your individual requirements, if you are using some other certificate.

For information about configuring SSL for Network Integrity, see "Configuring the SSL Policy and SSL Certificate" in *Network Integrity System Administrator's Guide*.

Managing Network Integrity Cartridges

Managing Network Integrity cartridges includes deploying and undeploying cartridges, viewing deployed and available cartridges, and migrating older cartridges to the latest version of Network Integrity.

Deploying Network Integrity Cartridges

You can deploy cartridges into Network Integrity in the following ways:

- From Service Catalog and Design - Design Studio. You can deploy cartridges interactively from Design Studio to test environments. Design Studio enables you to manage cartridges in the test environment consistently, manage common test environment connection parameters across the design team, and compare cartridge version and build numbers in the development environment with those of the cartridges deployed in the test environment. See "Getting Started with Design Studio for Network Integrity (1)" in *SCD Design Studio Modeling Network Integrity* for more information.
- By using the Service Catalog and Design Cartridge Management Tool (CMT). The CMT enables you to automate cartridge deployment. You can use the CMT to deploy cartridges into both test and production environments. You can also use it to deploy cartridges into cluster environments. See "Deploying Cartridges to Environments (1)" in *SCD Developer's Guide* for more information about the CMT.
- By using the Network Integrity Cartridge Deployer Tool (CDT). The Network Integrity CDT is a GUI-based tool that enables you to deploy to Network Integrity run-time environments. The Oracle Universal Installer installs the CDT as part of the Network Integrity installation process. You can use the CDT to deploy cartridges into both test and production environments. You can also use it to deploy cartridges into cluster environments. See "Deploying Cartridges with the Network Integrity Cartridge Deployer Tool" for more information.
- By writing your own custom scripts. See "Managing Cartridges With Custom Scripts" for more information.

Deploying Cartridges with the Network Integrity Cartridge Deployer Tool

The Cartridge Deployer Tool is available as a component of the core Network Integrity application. The Oracle Universal Installer installs the Cartridge Deployer Tool as part of the installation process in the same folder as the Network Integrity application.

The WebLogic Server Administration Console must not be locked for editing for the Cartridge Deployer Tool to successfully manage cartridges. See your WebLogic Server documentation for more information.

> **Note:**
>
> Before deploying or undeploying cartridges, ensure that:
>
> - You are logged out of the WebLogic Server Administration Console.
> - No one else is deploying or undeploying cartridges on the same server.
> - Network Integrity is not running a scan that uses the cartridge.

To deploy cartridges with the Network Integrity Cartridge Deployer Tool:

1. Go to the *NI_Home*/**CartridgeDeployerClients/CartridgeDeployer** folder.
2. Run the Cartridge Deployer Tool executable with the following command:

   ```
   ./runCartridgeDeployer.sh
   ```

   The Cartridge Deployer Welcome screen appears.
3. Select the **Deploy Cartridge** option and click **Next**.

   The Select Cartridge Type screen appears.

   In this screen, you select the cartridge type that is same as the application for which you are deploying the cartridges.
4. Select **Network Integrity** from the Cartridge Type list and click **Next**.

   > **Note:**
   >
   > If you are using a cartridge type other than Network Integrity, then ensure that the cartridge type that you select in this list matches the Cartridge Type attribute in the **manifest.xml** of the cartridge.

   The Cartridge Location screen appears.
5. Click **Browse** to search for and select the required cartridges for the Cartridge Deployer Tool to deploy.

   You can select multiple cartridges from a single directory by holding down the **Ctrl** key.

   Ensure that a cartridge is already deployed, or selected for deployment, if the cartridges you are selecting for deployment are dependent on it.

> **Note:**
>
> The customized file browser shows only predefined cartridge extensions. Network Integrity supports cartridges with IAR and JAR extensions.

6. After selecting the required cartridges, click **Next**.

   The Configure Deployment Queue screen appears.

7. View the details of the selected cartridges, confirm your selection, and click **Next**.

> **Note:**
>
> To add Deploy property or Model property, under **Details** for that cartridge, right-click **Properties** and select the respective options for related menus.

   The WebLogic Connection Information screen appears.

8. Do the following:

   a. In the **Host name or IP address** field, enter the host name or IP address of the WebLogic Administration Server.

   b. In the **Port number** field, enter the port number of the WebLogic Administration Server.

   c. Select whether or not to enable SSL by selecting or deselecting the **Use SSL** check box.

> **Note:**
>
> You must enter the Admin Server SSL Port if the **Use SSL** check box is selected.

   d. In the **Keystore** field, enter the keystore location if the **Use SSL** check box is selected.

   e. In the **CMWS User** field, enter the user name of the CMWS user.

> **Note:**
>
> Use your WebLogic administrator user name and password here, and in the next step.
>
> The cartridge management web service (CMWS) user is a WebLogic server user belonging to the administrators group.

   f. In the **Password** field, enter the password for the CMWS user.

> **Note:**
>
> Use your WebLogic administrator user name and password here.

g. Click **Next**.

The Select WebLogic Target screen appears.

9. In the list, select the Managed Server where CMWS is deployed and click **Next**.

The following message is displayed, if SSL is not configured properly:

```
SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the
bottom of this screen.
```

> **Note:**
>
> The SLL handshake fails when the Cartridge Deployer Tool connects to the CMWS using HTTPS.

10. Click **OK** in the message, and deselect **Use SSL (if enabled) while connecting to Cartridge Management WebService** at the bottom of the screen.

> **Note:**
>
> For information on installing a cartridge with Use SSL enabled, see "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide*.

11. Click **Next**.

The Review Deployment screen appears.

12. Review and confirm your selections, and click **Deploy**.

The Cartridge Deployment screen appears.

> **Note:**
>
> The Cartridge Deployer Tool rejects cartridges whose higher versions already exist. You can view rejected cartridges in the **Cartridges rejected for this deployment session** list.

Logs returned by the adapter are displayed after each cartridge deployment operation irrespective of its success.

> **Note:**
>
> If the system or server goes down during cartridge deployment, the cartridge is recovered after the system is up again, or during the next cartridge deployment session, with the cartridge deployment request showing as “failed".

13. Click **Exit** to close the Cartridge Deployment Tool.

> **Note:**
>
> You must log back into the Network Integrity application (if it is already opened) after cartridge deployment.

Undeploying Cartridges with the Network Integrity Cartridge Deployer Tool

You can use the Cartridge Deployer Tool to undeploy the cartridges.

> **Note:**
>
> When a cartridge is undeployed, all Network Integrity scans that use scan actions associated with the undeployed cartridge are deleted.

To undeploy a cartridge:

1. Go to the *NI_Home*/**CartridgeDeployerClients/CartridgeDeployer** folder.
2. Run the Cartridge Deployer Tool executable by running the following command:

   ```
   ./runCartridgeDeployer.sh
   ```

   The Cartridge Deployer Welcome screen appears.
3. Select **Undeploy Cartridge** and click **Next**.

   The Select Cartridge Type screen appears.
4. From the **Cartridge Type** list, select **NetworkIntegrity** and click **Next**.

   The WebLogic Connection Information screen appears.
5. Do the following:
   a. In the **Host name or IP address** field, enter the host name or IP address of the WebLogic Administration Server.
   b. In the **Port number** field, enter the port number of the WebLogic Administration Server.
   c. In the **CMWS User** field, enter the user name of the CMWS user.

> **Note:**
>
> Use your WebLogic administrator user name and password here, and in the next step.
>
> The CMWS user is a WebLogic server user belonging to the administrators group.

d. In the **Password** field, enter the password for the CMWS user.

> **Note:**
>
> Use your WebLogic administrator user name and password here.

e. Click **Next**.

The Select WebLogic Target screen appears.

6. Select the WebLogic targets where the cartridges you want to undeploy are installed, and click **Next**.

> **Note:**
>
> In some cases, WebLogic targets may be different from where Network Integrity is installed.
>
> The Cartridge Deployer Tool lists all WebLogic targets available in the domain where Network Integrity Cartridge Management Components are installed. Select a target from the list.

The following message appears:

```
SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the
bottom of this screen.
```

> **Note:**
>
> The SLL handshake fails when the Cartridge Deployer Tool connects to the CMWS using HTTPS.

7. Click **OK** in the message, and deselect **Use SSL (if enabled) while connecting to Cartridge Management WebService** at the bottom of the screen.

> **Note:**
>
> For information on installing a cartridge with Use SSL enabled, see "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide*.

8. Click **Next**.

   The Select Cartridges for Undeployment screen appears.

   You can view all of the cartridges that you had selected earlier, deployed in Network Integrity.

9. Click on the cartridge name to select it, then right-click on that cartridge name and select **Select for Undeployment**.

> **Note:**
>
> The cartridge name must be selected before right-clicking.

10. Click **Next**.

> **Note:**
>
> Network Integrity does not use undeployment properties.

   The Review Undeployment screen appears.

11. Review your selection(s) and click **Next**.

   The Cartridge Undeployment screen appears.

   You can view the undeployment progress in this screen. Logs returned by the adapter are displayed after each cartridge operation irrespective of its success.

For more information about managing cartridges and deploying cartridges using Design Studio, see "Getting Started with Design Studio for Network Integrity (1)" in *SCD Design Studio Modeling Network Integrity*.

> **Caution:**
>
> If the server or system goes down during cartridge undeployment, the cartridge is recovered after the system is up again, or during the next cartridge undeployment session, with the cartridge deployment request showing as “deploy".
>
> Ensure that you deploy the recovered cartridge first and then undeploy it.

Deploying and Undeploying Cartridges on a Remote Server

> **Note:**
>
> Oracle recommends that you deploy cartridges, or any Network Integrity adapters on the same server where Network Integrity is deployed.

To deploy cartridges from a remote managed server:

1. Copy the file **NetworkIntegrity.ear** from the administration server to the remote managed server before starting the cartridge deployment/undeployment.

> **Note:**
>
> **NetworkIntegrity.ear** is on the same system where the Administration server is running.

2. In the remote server, deploy, or undeploy, cartridges using steps provided in the sections "Deploying Cartridges with the Network Integrity Cartridge Deployer Tool" and "Undeploying Cartridges with the Network Integrity Cartridge Deployer Tool".
3. Copy the **NetworkIntegrity.ear** file from remote managed server back to the administration server.
4. Update the **NetworkIntegrity.ear** file.

   The cartridges are deployed on, or undeployed from, the remote managed server.

Deploying Cartridges into Cluster Environments That Use Proxy Server

To deploy cartridges into a cluster environment that uses a proxy server as a frontend host:

1. Shut down all the managed servers except the managed server on which the cartridge_management_ws application is deployed. If you do not know the managed server on which the cartridge_management_ws application is deployed, continue with step 2; otherwise, proceed to step 3.
2. (Optional) Locate the cartridge_management_ws application and the corresponding server on which it is deployed by doing the following:
   a. Log in to the WebLogic Server Administration Console.
   b. On the Home page, under **Domain Structure**, click the **Deployments** link.

      The Summary of Deployments page appears.
   c. Under the **Name** column, locate the cartridge_management_ws application; under the **Targets** column, locate the server on which this application is deployed.
3. Deploy the required cartridges.
4. After you have deployed the cartridges, start the Administration Server and all the other managed servers.

> **Note:**
>
> Repeat this procedure for every cartridge deployment life cycle.

Viewing Cartridges with the Network Integrity Cartridge Deployer Tool

To view deployed cartridges:

1. Go to the *NI_Home*/**CartridgeDeployerClients/CartridgeDeployer** folder.
2. Run the Cartridge Deployer Tool executable by running the following command:

```
./runCartridgeDeployer.sh
```

The Cartridge Deployer Welcome screen appears.

3. Select the **View Cartridges** option, and click **Next**.

   The Select Cartridge Type screen appears.

4. Select **Network Integrity** in the Cartridge Type list, and click **Next**.

   The WebLogic Connection Information screen appears.

5. Do the following:

   a. In the **Host name or IP address** field, enter the host name or IP address of the WebLogic Administration Server.

   b. In the **Port number** field, enter the port number of the WebLogic Administration Server.

   c. In the **CMWS User** field, enter the user name of the CMWS user.

   > **Note:**
   >
   > Use your WebLogic administrator user name and password here, and in the next step.
   >
   > The CMWS user is a WebLogic server user belonging to the administrators group.

   d. In the **Password** field, enter the password for the CMWS user.

   > **Note:**
   >
   > Use your WebLogic administrator user name and password here.

   e. Click **Next**.

   The Select WebLogic Target screen appears.

6. Select the WebLogic targets where the CMWS is installed and click **Next**.

   > **Note:**
   >
   > In some cases, the WebLogic targets may be different from where Network Integrity is installed.

   The following message is displayed:

   ```
   SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the bottom of this screen.
   ```

   > **Note:**
   >
   > The SLL handshake fails when the Cartridge Deployer Tool connects to the CMWS using HTTPS.

7. Click **OK** in the message, and deselect the **Use SSL (if enabled) while connecting to Cartridge Management WebService** check box at the bottom of the screen.

> **Note:**
>
> For information about installing a cartridge with Use SSL enabled, see "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide*.

8. Click **Next**.

   The Deployed Cartridges screen appears.

   You can view the deployed cartridges.

For more information about managing cartridges, see "Getting Started with Design Studio for Network Integrity (1)" in *SCD Design Studio Modeling Network Integrity*, which is part of Design Studio Online Help.

For information about deploying cartridges using Design Studio, see "Getting Started with Design Studio for Network Integrity (1)" in *Design Studio Online Help*.

Managing Cartridges With Custom Scripts

Scripted cartridge management allows you to develop custom scripts that deploy, undeploy, list deployed cartridges, and list available cartridges. Scripts can be run manually, or from a command prompt, and can be used to process cartridge operations to secure and non-secure network systems.

To manage cartridges using Java, you must develop a custom Java application. Or, to manage cartridges using ANT tasks, you must develop a custom XML script.

> **Note:**
>
> You can automate cartridge deployment using the Design Studio Cartridge Management Tool (CMT). You can use the CMT to deploy cartridges into both test and production environments. See "Creating, Packaging, and Distributing Plug-in Projects (1)" in *SCD Developer's Guide* for more information about the CMT.

Developing a Custom Java Application

Refer to *NI_Home*/**CartridgeDeployerClients/tools/Sample.java** for an example custom Java application, containing example syntax and sample Java classes.

To develop a custom Java application with which to manage cartridges:

1. Open Oracle Communications Service Catalog and Design - Design Studio or any Java Integrated Development Environment (IDE) in the Java perspective.
2. Create a Java project and a **/lib** directory in the project.
3. Import all the JAR files from the *NI_Home*/**CartridgeDeployerClients/lib/** directory to the **/lib** directory in the project.

4. Download **cartridge-management-client-tools.jar** from the *NI_Home*/**CartridgeDeployerClients/tools** directory to the **/lib** directory in the project.
5. Inside **/lib** directory, create a Java file to develop the Java classes that are required to implement cartridge management operations by doing all of the following:
   a. Import the following files:
      - oracle.communications.platform.cartridgemanagement.client.domain.Cartridge
      - oracle.communications.platform.cartridgemanagement.client.domain.CartridgeOperationResponse
      - oracle.communications.platform.cartridgemanagement.client.core.CartridgeManager
   b. To deploy cartridges, create an oracle.communications.platform.cartridgemanagement.client.domain.Cartridge object with the following class attributes:
      - name
      - version
      - buildId
      - type
      - deploy properties
   c. Call the deployCartridge() operation on the cartridge manager object with the following arguments:
      - webServiceUrl
      - keystore_location
      - cmwsUserName
      - password
      - cartridge_object
      - pollwait
      - pollcount
   d. To undeploy cartridges, create an oracle.communications.platform.cartridgemanagement.client.domain.Cartridge object with the following class attributes:
      - name
      - version
      - type
      - undeploy properties
   e. Call the unDeployCartridge() operation on the cartridge manager object with the following arguments:
      - webServiceUrl
      - keystore_location
      - cmwsUserName
      - password
      - cartridge_object

- pollwait
- pollcount

f. To list cartridges of a specific type, call the getInstalledCartridges() operation on the cartridge manager object with the following arguments:
   - webServiceUrl
   - keystore_location
   - cmwsUserName
   - password
   - cartridgeType

g. To list existing cartridges of a specific type, create an oracle.communications.platform.cartridgemanagement.client.domain.Cartridge object with the following class attributes:
   - name
   - version
   - type

h. Call the cartridgeExist() operation on the cartridge manager object with the following arguments:
   - webServiceUrl
   - keystore_location
   - cmwsUserName
   - password
   - cartridge_object
   - comparisonOperator

i. To get the environment, call the getEnvironmentVersion() operation on the cartridge manager object with the following arguments:
   - webServiceUrl
   - keystore_location
   - cmwsUserName
   - password
   - cartridgeType

Developing Custom ANT Tasks

Refer to *NI_Home*/**CartridgeDeployerClients/tools/sample-build.xml** for an example custom ANT script, containing example syntax and sample operations. Refer to *NI_Home*/**CartridgeDeployerClients/tools/sample-build.properties** for an example custom Java application, containing example syntax and sample operations.

To develop custom ANT tasks with which to manage cartridges:

1. Open Design Studio or any Java Integrated Development Environment (IDE) in the XML perspective.
2. Create a Java project and a **/lib** directory in the project.

3. Import all the JAR files from the *NI_Home*/**CartridgeDeployerClients/lib/** directory to the **/lib** directory in the project.
4. Download **cartridge-management-client-tools.jar** from the *NI_Home*/**CartridgeDeployerClients/tools** directory to the **/lib** directory in the project.
5. Inside the **lib/** directory, create an XML file with the following cartridge management operations:

```
<taskdef name="deploy"
classname="oracle.communications.sce.cartridgemanagement.ws.tools.DeployCartridge"
classpathref="class.path"/>

<taskdef name="undeploy"
classname="oracle.communications.sce.cartridgemanagement.ws.tools.UndeployCartridge"
classpathref="class.path"/>

<taskdef name="list"
classname="oracle.communications.sce.cartridgemanagement.ws.tools.ListCartridge"
classpathref="class.path"/>

<taskdef name="exist"
classname="oracle.communications.sce.cartridgemanagement.ws.tools.CartridgeExist"
classpathref="class.path"/>

<taskdef name="environment"
classname="oracle.communications.sce.cartridgemanagement.ws.tools.GetEnvironment
Version" classpathref="class.path"/>
```

6. Add the valid attributes for each ANT task:
   - For the deploy task:

```
<target name="deploy">
  <echo message="Deploying cartridge..."/>
  <deploy host="${host}" port="${port}" username="${username}" password="$
{password}" adminServerKeyStore="${adminServerKeyStore}" sslKeyStore="$
{sslKeyStore}" fileLocation="${fileLocation}" cartridgeType="${cartridgeType}"
target="${target}" property="deployresponse"/>
  <echo message="Message from cartridge deploy task : ${deployresponse}"/>
</target>
```

   - For the list task:

```
<target name="list">
  <echo message="Listing cartridge..."/>
  <list host="${host}" port="${port}" username="${username}" password="$
{password}" adminServerKeyStore="${adminServerKeyStore}" sslKeyStore="$
{sslKeyStore}" target="${target}" cartridgeType="${cartridgeType}"
property="listval"/>
  <echo message="Message from cartridge list task : ${listval}"/>
</target>
```

   - For the undeploy task:

```
<target name="undeploy">
  <echo message="Undeploying cartridge ${cartridgeName}
${cartridgeVersion}..."/>
  <undeploy host="${host}" port="${port}" username="${username}" password="$
{password}" adminServerKeyStore="${adminServerKeyStore}" sslKeyStore="$
{sslKeyStore}" target="${target}" cartridgeName="${cartridgeName}"
cartridgeVersion="${cartridgeVersion}" cartridgeType="${cartridgeType}"
property="undeployresponse"/>
  <echo message="Message from cartridge undeploy task : ${undeployresponse}"/>
</target>
```

- For the exist task:

```
<target name="exist">
  <echo message="Checking existance of cartridge ${cartridgeName} $
{cartridgeVersion}..."/>
  <exist host="${host}" port="${port}" username="${username}" password="$
{password}" adminServerKeyStore="${adminServerKeyStore}" sslKeyStore="$
{sslKeyStore}" target="${target}" cartridgeName="${cartridgeName}"
cartridgeVersion="${cartridgeVersion}" cartridgeType="${cartridgeType}"
property="existval"/>
  <echo message="Message from cartridge exist task : ${existval}"/>
</target>
```

- For the environment task:

```
<target name="env">
  <echo message="Fetching environment version..."/>
  <environment host="${host}" port="${port}" username="${username}" password="$
{password}" adminServerKeyStore="${adminServerKeyStore}" adminServerKeyStore="$
{adminServerKeyStore}" sslKeyStore="${sslKeyStore}" target="${target}"
cartridgeType="${cartridgeType}" property="envval"/>
  <echo message="Message from env task : ${envval}"/>
</target>
```

7. Inside the **lib/** directory, create an XML properties file to automate the ANT tasks:

```
ant -lib ..lib/ -f sample-build.xml deploy
ant -lib ..lib/ -f sample-build.xml list
ant -lib ..lib/ -f sample-build.xml undeploy
ant -lib ..lib/ -f sample-build.xml exist
ant -lib ..lib/ -f sample-build.xml env
```

Where *lib/* refers to the location where the dependent libraries are stored.

Running Cartridge Operations From a Command-Line

To use a command-line interface to run cartridge operations:

1. Open a system console command-line or connect to the Network Integrity server using a remote client.
2. Set the Java path, as it is explained in your Java documentation.
3. Enter commands at the command-line.

From the command-line interface, you can:

- Deploy one or more cartridges.
- Undeploy one or more cartridges.
- List all deployed cartridges.
- List all available, undeployed cartridges.
- Show the help message.

Table 7-1 lists all the arguments used at the command-line for managing cartridge operations.

Table 7-1 Valid Arguments for Command-Line Cartridge Management

Valid Argument	Description
-host	The admin host name where the cartridge manager web service (CMWS) is deployed.

Table 7-1 (Cont.) Valid Arguments for Command-Line Cartridge Management

Valid Argument	Description
-port	A valid port number to the admin server.
-user	A CMWS user.
-password	The CMWS password for the specified user. If -password is omitted from the command, you are prompted to enter the password at the command prompt.
-keystore	A valid keystore location for SSL connection.
-adminkeystore	A valid keystore location for the admin server if the SSL connection is used.
-type	The cartridge type. When deploying multiple cartridges, -type must be set to `NetworkIntegrity`.
-operation	The cartridge operation to be performed. Possible values are: `deploy`, `undeploy`, `list`, and `exist`.
-location	A path to a single cartridge, or a comma separated list of paths to multiple cartridges.
-target	The target server, where CMWS is deployed.
-name	A single cartridge name, or a comma-delimited list of cartridge names for multiple cartridges. Only the undeploy operation can accept multiple names.
-version	A single five-digit cartridge version, or a comma-delimited list of cartridge versions for multiple cartridges. Only the undeploy operation can accept multiple versions.
-help	Display the help message.

Table 7-2 lists the commands for managing cartridge operations, with their mandatory and valid arguments.

Table 7-2 Valid Arguments for Each Cartridge Command

Command	Description
deploy	Mandatory Arguments: -host, -port, -username, -password, -target, -keystore (if command is run on an SSL-enabled network system) Valid Arguments: -type, -location, -target
undeploy	Mandatory Arguments: -host, -port, -username, -password, -target, -keystore (if command is being run on an SSL-enabled network system) Valid Arguments: -type, -target, -name, -version
list	Mandatory Arguments: -host, -port, -username, -password, -target, -keystore (if command is being run on an SSL-enabled network system) Valid Arguments: -type, -target
exist	Mandatory Arguments: -host, -port, -username, -password, -target, -keystore (if command is being run on an SSL-enabled network system) Valid Arguments: -type, -name, -version, -target

To display instruction messages, enter a command similar to the example below:

```
java -jar cartridge-management-client-tools.jar -help
```

To deploy a cartridge, enter a command similar to the example below:

```
java -Djava.util.logging.config.file=logger.conf -jar cartridge-management-client-
tools.jar -operation deploy -host admin_host -port admin_port -user cmws_user -password
```

```
cmws_password -target target_name_where_cmws_deployed -location cartridge_path -type
cartridge_type -property
model.modelname=modelvalue,deploy.deployname1=deployvalue1,deploy.deployname2=deployvalue
2
```

To list deployed cartridges, enter a command similar to the example below:

```
java -Djava.util.logging.config.file=logger.conf -jar cartridge-management-client-
tools.jar -operation list -host admin_host -port admin_port -user cmws_user -password
cmws_password -type cartridge_type -target target_name_where_cmws_deployed
```

To undeploy a cartridge, enter a command similar to the example below:

```
java -Djava.util.logging.config.file=logger.conf -jar cartridge-management-client-
tools.jar -operation undeploy -host admin_host -port admin_port -user cmws_user -
password cmws_password -type cartridge_type -target target_name_where_cmws_deployed -
name cartridge_name -version cartridge_version
```

To check if a cartridge exists, enter a command similar to the example below:

```
java -Djava.util.logging.config.file=logger.conf -jar cartridge-management-client-
tools.jar -operation exist -host admin_host -port admin_port -user cmws_user -password
cmws_password -type cartridge_type -target target_name_where_cmws_deployed -name
name_of_cartridge -version version_of_cartridge
```

To fetch environment properties, enter a command similar to the example below:

```
java -Djava.util.logging.config.file=logger.conf -jar cartridge-management-client-
tools.jar -operation env -host admin_host -port admin_port -user cmws_user -password
cmws_password -type cartridge_type -target target_name_where_cmws_deployed
```

Configuring Network Integrity for Inventory Management

After installing Network Integrity, you can use it to discover devices on your network. To compare the discovered device data with an existing inventory model, and to detect and resolve discrepancies between the two, you must configure or extend Network Integrity to communicate with your inventory management system. You may also need to configure or extend your inventory system.

You can license and download components to simplify the task of configuring and extending Network Integrity to communicate with Unified Inventory Management (UIM).

You can license and download components to simplify the task of configuring and extending Network Integrity to communicate with MetaSolv Solution (MSS).

For information on Network Integrity cartridges or UIM technology packs that enable communication between Network Integrity and UIM, see "Overview" in *UIM Integration Cartridge* documentation.

Installing Network Integrity Report Templates

Network Integrity comes with pre-defined report templates that you can use. A folder, **integrityreports**, is created during installation, in the folder where Network Integrity is deployed. The **integrityreports** folder contains the following report templates:

- Scan_History_Report
- Discrepancy_Corrective_Action_Report
- Device_Discrepancy_Detection_Summary_Report

- Device_Discrepancy_Detection_Detailed_Report
- Device_Discovery_Summary_Report

> **Note:**
>
> The **integrityreports** folder should be on the system where Oracle Analytics Publisher is installed. If Oracle Analytics Publisher is installed on a system separate from the system where Network Integrity is deployed, move the **integrityreports** folder to the location where Oracle Analytics Publisher is installed and provide the correct connection information as shown in "Installing Network Integrity Report Templates".

To deploy the report templates to Oracle Analytics Publisher:

1. Open the Oracle Analytics Publisher application, click on **New** and select **Data Model** from the dropdown menu.
2. Within the **Diagram** tab, click on the '+' symbol and select **SQL Query**.

   The New Data Set - SQL Query window appears.
3. Open the .xdo file and copy the SQL from the file.
4. Paste the copied SQL into the **SQL Query** field on the window.
5. Provide the name of the Data Model and click **OK**.
6. The Add Parameter window appears. In this window, select all of the parameters and click on **OK**.
7. Click on **View Data** in the Data Model screen.
8. From the **Data** tab, click on **View** and click **Table View** to view the data in table format.
9. Click on the **Save as Sample Data** icon.
10. Check the .xdo file for any available valueSet values.

    If there are any values then:

    a. Click on **List of Values** on the left side of the Data Model screen.

    b. Click on '+' to add values.

    c. Provide the name and copy the SQL query from the .xdo file. Paste this code into the **deviceTypes: Type: SQL Query** field.
11. Click on **Save** icon.

    The **Save As** window appears. Here, select the Data Model folder, provide the data model name and save it.
12. Click on **New** and select **Report** from the dropdown menu.

    The **Create Report** window appears.
13. Click on the **Search** icon next to the **Data Model** field.

    The Select Data Model window opens.
14. Select the corresponding data model for the report from the window and click **Open**.

    Click **Next** on the Create Report window.
15. Under Layout options, select **Table** and click **Next**.

16. Select **View Report** and Click on **Finish**.
17. Select OAPubReports folder and provide the name of the report.
18. Click on **Save** to save your report.

Starting the AgeOut Process

The AgeOut process in Network Integrity cleans up the database by deleting old scan results. Although running the AgeOut process is an optional component, doing so improves Network Integrity performance and is recommended.

See "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide* for information about starting the AgeOut Process.

Enabling HTTP Tunneling

For Network Integrity to transfer large amounts of data between the server and client, the WebLogic server must be configured for http tunneling. This will help the server to make a dedicated connection with the client, for the given timeout and within this time, the data can be transferred without giving any errors.

> **Note:**
>
> HTTP tunneling should be enabled on the server where Network Integrity is deployed. If Network Integrity is deployed in a single managed server installation, then the parameters need to be changed on the WebLogic administration server. If Network Integrity is deployed in a clustered server installation, then the parameters need to be changed on the WebLogic administration server and all the managed servers.

To enable http tunneling, perform the following:

1. Log in to the Administration console using the administrator user name and password.
2. Click **Lock and edit**.
3. Click **Servers** in the left panel.
4. Select the server name and click **Protocols**.
5. In the **Enable tunneling** field, select the check box.
6. In the **Tunneling client ping** field, enter **80** seconds.
7. In the **Tunneling client timeout** field, enter **900** seconds.
8. Click **Activate Changes**.
9. Repeat the same procedure for any managed servers.

Setting Up Oracle Internet Directory

If you choose to use Oracle Internet Directory as your lightweight directory access protocol (LDAP) provider, you must set it up to run with Network Integrity.

1. Navigate to *Domain_Home***/config/fmwconfig**.

2. Edit the file **jps-config.xml**.
3. Find the following serviceInstance parameter:

```
<serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
```

4. Add the following bold entries to the file:

```
<serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
    <description>LDAP Identity Store Service Instance</description>
    <property name="idstore.config.provider"
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"/>
    <property name="CONNECTION_POOL_CLASS"
value="oracle.security.idm.providers.stdldap.JNDIPool"/>
    <property name="virtualize" value="true"/>
    <serviceInstanceRef ref="NetworkIntegrityAuthenticationProvider"/>
</serviceInstance>
<serviceInstance name="NetworkIntegrityAuthenticationProvider"
provider="idstore.ldap.provider">
    <property name="idstore.type" value="ACTIVE_DIRECTORY" />
</serviceInstance>
```

5. Save and close the file.

8
Verifying the Network Integrity Installation

This chapter describes how to verify that Oracle Communications Network Integrity is installed correctly.

Checking the State of all Installed Components

You can verify that Network Integrity is installed by checking the state of all installed components.

To check the state of all installed components:

1. Log in to the WebLogic Administration Server.
2. Ensure that all of the managed servers are running.
3. In the left panel, in the Domain Structure section, click **Deployments**.

   The Summary of Deployments page appears.
4. If Network Integrity is installed successfully, the following deployments appear in the **Active** state:
   - JobDispatcher
   - NetworkIntegrity
   - NICMWSAdapter
   - snmpAdapter
   - FileTransferJCA
   - cartridge_management_ws

Logging In to Network Integrity

You can verify that Network Integrity is installed by logging in to Network Integrity.

To log in to Network Integrity:

1. Open a browser window. Refer to Table 2-2 for supported web browsers.
2. Enter the URL as provided by the Installer after the installation.
3. Click **Go**, or press the **Enter** key.

   The Network Integrity login page appears.
4. Do the following:
   a. In the **User Name** field, enter the Network Integrity user name.
   b. In the **Password** field, enter the password for the Network Integrity user name.

   The Network Integrity home page appears, verifying that Network Integrity is installed successfully.

9
Upgrading Network Integrity

This chapter explains how to upgrade your existing system to the latest release of Oracle Communications Network Integrity.

This chapter explains how to recover your system after an upgrade failure. See "About Rolling Back Network Integrity" for more information.

About Upgrading Network Integrity

Upgrading to a new release of Network Integrity consists of the following tasks:

- Planning the upgrade. See "Planning Your Upgrade" for more information.
- Reviewing the upgrade impacts. See "Upgrade Impacts" for more information.
- Performing the pre-upgrade tasks.
- Upgrading Network Integrity.
- Performing the post-upgrade tasks.

  See "Upgrading Network Integrity" for more information.

Before upgrading a production environment, you should first test the upgrade in a test environment. See "Testing the Upgrade in a Test Environment" for more information.

In this chapter, the release you are upgrading from is called the *old* release, the release you are upgrading to is called the *new* release.

Supported Upgrade Paths

This release of Network Integrity supports the direct upgrade path from release 7.3.6.4 to release 7.5 and release 7.4 to release 7.5.

See "Upgrading Network Integrity" for more information.

Planning Your Upgrade

Depending on the components affected by the upgrade, your upgrade team may include the following:

- A database administrator, to manage the database upgrade and tune the database.
- A system integrator, to handle new and existing customizations.
- A system administrator, to manage the Oracle WebLogic Server and Network Integrity software upgrade.
- A UNIX administrator, to manage accounts, network setup, and IP configurations.

Identify who might be affected by the upgrade. For example:

- You might need to give your system administrators and Network Integrity users notice of any system downtime.

- Tell your system administrators in advance about any changes to the system architecture (for example, Oracle database, client, or WebLogic Server upgrades).
- Train your administrators, users, cartridge developers, or system integrators on new functionality introduced by the upgrade that has an impact on their role.

You might need to make changes to your system after the upgrade is complete to accommodate new or modified features or functionality. For example, if the new release provides new security functionality, additional system configuration steps may be required. See "Upgrade Impacts" for more information.

The best way to estimate the duration of an upgrade is to perform the upgrade procedure on a test system with a copy of the production data. See "Testing the Upgrade in a Test Environment" for more information.

It is not necessary to shut down Network Integrity or the Network Integrity WebLogic Server domain before an upgrade. However, you must ensure that Network Integrity is not running any operations, such as scans or blackouts.

Oracle recommends scheduling your upgrade during non-peak hours to minimize the disruption to your operations.

Testing the Upgrade in a Test Environment

Oracle recommends running the upgrade procedure on a test system with a copy of your production data before upgrading your production system. Test the upgrade by doing the following:

- Successfully completing all the pre-upgrade, upgrade, and post-upgrade tasks.
- Comparing the default behavior between the old and the new releases.
- Recreating any custom configurations and extensions.
- Confirming that all new behavior and functionality works.
- Ensuring that the database tables are properly installed.
- Ensuring that the database data is correct.
- Starting the WebLogic Server domain.
- Ensuring that users and user permissions are correct.
- Ensuring that productized and custom cartridges build and deploy properly.
- Logging into Network Integrity and verifying the version number of installed components.

Upgrade Impacts

This section explains any important system changes introduced by an upgrade. Upgrading to this version of Network Integrity requires the following system changes:

- Fusion Middleware Changes
- Java Development Kit Changes
- WebLogic Server Changes
- Database Software Changes
- Database Schema Changes
- Application Component Changes

- Design Studio Changes
- Cartridge Changes

New features and new functionality are described in *Network Integrity Release Notes*.

Fusion Middleware Changes

You must upgrade your version of Application Development Runtime and apply applicable patches, and install Repository Creation Utility.

See "Software Requirements" for more information.

Java Development Kit Changes

The new version of Network Integrity requires an updated version of the Java Development Kit (JDK) on the Network Integrity application server. See "Software Requirements" for more information.

During the upgrade, you will need to update the Network Integrity domain to point to the new JDK.

WebLogic Server Changes

You must upgrade your version of WebLogic Server and apply applicable patches.

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

Database Software Changes

You must import and export the upgraded Network Integrity schema into Oracle Database 19.22.

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

Database Schema Changes

The new version of Network Integrity requires an updated database schema.

Application Component Changes

The Oracle Universal Installer updates all the Network Integrity components.

Design Studio Changes

This version of Network Integrity requires an updated version of Oracle Communications Service Catalog and Design - Design Studio. See "Network Integrity System Requirements " for more information.

Design Studio can be set up before or after you upgrade Network Integrity. See "Design Studio Installation Overview (1)" in Design Studio installation documentation for more information. Rather than upgrading Design Studio, install the new version and keep the old version until after you have finished upgrading Network Integrity.

Cartridge Changes

You must undeploy cartridges that you do not want to migrate to the new release before beginning the upgrade.

After the upgrade is complete, cartridges must be migrated to the new release of Network Integrity using the Design Studio Cartridge Migration Tool. It is possible that migrated cartridges contain minor compilation errors that prevent them from building and deploying. If a cartridge fails to build, open it in Design Studio and correct any compilation errors.

Upgrading Network Integrity

To upgrade Network Integrity, do the following tasks:

- Pre-Upgrade Tasks
- Upgrading Network Integrity
- Post-Upgrade Tasks

Pre-Upgrade Tasks

This section details the procedures to upgrade Network Integrity from release 7.3.6.4 to release 7.5 and release 7.4 to release 7.5. Pre-upgrade tasks must be performed while the WebLogic server is inactive.

Perform and complete all the following pre-upgrade tasks before upgrading Network Integrity:

1. Back up the Network Integrity and MDS databases. See "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide* for more information.
2. Back up the Network Integrity WebLogic Server domain. See the WebLogic Server documentation for more information.

   > **Note:**
   >
   > Verify that the file/folder being backed up meets the file size or path name length requirements for the backup utility being used. For example, the maximum path name length for the tar application is 256 characters.

3. Upgrade the Fusion Middleware Application Development Runtime and apply any required patches.

   See "Software Requirements" for version information regarding Fusion Middleware Application Development Runtime and any applicable patches.

4. Upgrade the MDS and OPSS schemas:
   a. Navigate to *MW_HOME*/**oracle_common/upgrade/bin/ua**

      where *MW_HOME* is the directory in which Oracle Fusion Middleware is installed.

      This directory contains the Upgrade Assistant (UA) tool, which you use to upgrade the schema.

   b. Launch the UA tool to upgrade the schema.

The Welcome screen appears.

c. Click **Next**.

The All Schemas screen appears.

d. Select **Schemas** and click **Next**.

The Available Components List screen appears showing the Components to be upgraded and select these check boxes, and click **Next**:

```
Common Infrastructure Services
Oracle Metadata Services
Audit Services
Audit Services Append
Audit Service Viewer
Oracle Platform Security Services
```

e. Create a new Weblogic Services (WLS) schema using the rcu tool for existing prefix.

f. In the Direction field, select the Weblogic domain directory for the upgrade. click **Next**.

The Prerequisites screen appears.

g. Confirm that the database backup is complete by selecting the **All affected data is backed up**, **Database version is certified by Oracle for Fusion Middleware upgrade**, and **Certification and system requirements have been met** check boxes, and click **Next**.

The OPSS Schema screen appears.

h. From the **Database Type** list, select the database type.

i. In **Database Connect String**, enter the *hostname:portnumber/SID* string.

> **Note:**
>
> For a clustered environment, the *hostname:portnumber/SID* must specify the primary Oracle RAC node.

j. In **DBA User Name**, enter the database administrator user name.

k. In **DBA Password**, enter the password for the administrator user.

l. Click **Connect**.

If the provided details are valid, the **Schema User Name** and **Schema Password** fields become enabled.

m. From the **Schema User Name** list, select the OPSS schema.

n. In **Schema Password** field, enter the database password, and click **Next**.

The MDS Schema screen appears.

o. From the **Database Type** list, select the database type.

p. In **Database Connect String**, enter the *hostname:portnumber/SID* string.

> **Note:**
>
> For a clustered environment, the *hostname:portnumber/SID* must specify the primary Oracle RAC node.

q. In **DBA User Name**, enter the database administrator user name.

r. In **DBA Password**, enter the password for the administrator user.

s. Click **Connect**.

If the provided details are valid, the **Schema User Name** and **Schema Password** fields become enabled.

t. From the **Schema User Name** list, select the MDS schema.

u. In **Schema Password** field, enter the database password, and click **Next**.

The Examine screen appears.

v. Click **Next**.

The Upgrade Summary screen appears.

w. Verify the details of the OPSS and MDS schema to be upgraded and click **Upgrade**.

The Upgrading Components screen appears. You can monitor the progress of the upgrade from this screen.

x. After the upgrade completes, click **Next**.

The Upgrade Success screen appears.

y. Verify that the upgrade was successful and click **Close**.

See Oracle Fusion Middleware documentation for more information.

5. Reconfigure the WebLogic domain configurations using the Fusion Middleware Reconfiguration Wizard, which you open using the following command:

```
./MW_Home/oracle_common/common/bin/reconfig.sh
```

a. On the Select Domain screen, from the **Existing Domain Location** list, select the domain that you want to upgrade and click **Next**.

The Reconfiguration Setup Progress screen appears, displaying the progress of the reconfiguration setup process.

b. Click **Next**.

The Domain Mode and JDK screen appears.

The domain mode cannot be changed during reconfiguration. It is inherited from the original domain.

c. Select the **JDK** option and browse to the folder (JAVA_HOME) where the JDK is installed and click **Next**.

Ensure that you have installed the correct version of the JDK. See "Software Requirements" for more information.

The Database Configuration Type screen appears.

d. Select the **RCU Data** option, complete the required fields, and then click **Get RCU Configuration**, which retrieves the schema information.

You select the **RCU Data** option to connect to the database to retrieve schema information for all schemas that are included in the domain.

e. Click **Next**.

f. Navigate through the different screens by clicking **Next** on each screen and specify your settings as necessary.

g. On the Node Manager screen, under the **Node Manager Type** area, select **Manual Node Manager Setup** and click **Next**.

The Advanced Configuration screen appears.

h. Select the categories for which you want to perform advanced configuration and click **Next**.

For each category you select, the appropriate configuration screen is displayed to allow you to perform advanced configuration.

i. Navigate through the different screens by clicking **Next** on each screen and specify your settings as necessary.

j. On the Deployments Targeting screen, under **Targets**, select the **Network Integrity.ear** application and then click the left arrow, which moves the application to the **Deployments** section.

k. On the Deployments Targeting screen, under **Deployments**, select **Library**, and then under **Targets**, select the server or cluster, and then click the right arrow, which moves all the libraries to the targeted server or cluster for deployment.

> **Note:**
>
> When targeting applications for deployment on a cluster, ensure that NICMWSAdapter and cartridge_management_ws are selected for only the first managed server of the cluster.

l. Click **Next**.

The Services Targeting screen appears.

m. Under **Services**, select all the services, and then under **Targets**, select the server or cluster, and then click the right arrow, which moves the services to the targeted server or cluster for deployment.

> **Note:**
>
> When targeting services to a cluster, ensure that CMWSPersistentDS, CMWSPersistentJDBCStore, and CMWSJMSModule are targeted to only the first managed server of the cluster.

n. Click **Next** until the Configuration Summary screen appears.

o. Review the detailed configuration settings of the domain and click **Reconfig**.

The Reconfiguration Progress screen appears, which displays the progress of the reconfiguration process.

After the reconfiguration process completes, the Reconfiguration Success screen appears.

p. Click **Finish**.

See Oracle Fusion Middleware documentation for more information.

6. Upgrade the WebLogic domain configurations by doing the following:

a. Navigate to the *MW_Home***/oracle_common/upgrade/bin/ua** directory.

This directory contains the Fusion Middleware Upgrade Assistant, which you use to upgrade the WebLogic domain configurations.

b. Launch the Fusion Middleware Upgrade Assistant.

The Welcome screen appears.

c. Click **Next**.

d. Select **WebLogic Component Configurations**, and in the **Domain Directory** field, select the WebLogic domain directory you want to upgrade, and then click **Next**.

The Prerequisites screen appears.

e. Navigate through the different screens by clicking **Next** on each screen and specifying your settings as necessary.

f. On the Upgrade Success screen, verify that the upgrade was successful and click **Close**.

See Oracle Fusion Middleware documentation for more information.

7. After the upgrade of the WebLogic domain, you perform this step before starting the WebLogic Administration server.

If Network Integrity is installed in a WebLogic cluster domain, open the *WL_DOMAIN*/**config/config.xml** file and change the JD persistent store and the NI persistent store targets to managed server migratables.

See Installing and Configuring Oracle WebLogic Server for more information.

8. Start the Network Integrity Administration server. If this is a clustered server environment, start the cluster member servers.

> **Note:**
>
> If there are any JNDI issues and if managed server status goes to “Admin" state, then delete **NetworkIntegrity.ear** and **NICMWSAdapter.ear** from deployments and start the managed server.

9. Ensure that all the deployed applications are active, otherwise you will need to manually update each application and then make each application active.

10. Undeploy all cartridges that you do not want migrated to the new version of Network Integrity. See "Migrating Cartridges" for more information.

For example, you should undeploy cartridges that you are no longer licensed to use, or cartridges that provide functionality you no longer want to use.

> **WARNING:**
>
> It is not possible to undeploy a non-migrated cartridge after upgrading Network Integrity. Failure to undeploy cartridges that cannot or are not migrated causes Network Integrity to not function.

See "Problem: Inability To Run Scans or Resolve Discrepancies After Upgrading" for more information.

Upgrading Network Integrity

This section assumes that you have completed the steps in "Pre-Upgrade Tasks" before proceeding with the upgrade of Network Integrity.

> **Note:**
>
> The following tasks need to be carried out manually before proceeding with normal upgrade. These tasks apply if your version of Network Integrity is version 7.3.6.3 or below.
>
> 1. Stop all managed servers, except admin server.
> 2. Undeploy snmpAdapter from the console.
> 3. Start all managed servers.

To upgrade Network Integrity:

1. Create a directory (*dir*) for a temporary installation directory.
2. Download the software for your operating system from the Oracle software delivery web site:

   `https://edelivery.oracle.com`

   and save it to *dir*:
3. Extract the contents of the software pack to *dir*.

   The extracted software pack has the following structure:

   integrity/Disk1/install/
4. (IBM AIX only) Stop and restart the WebLogic Server domain for Network Integrity.
5. Run the following command:

   ```
   ./dir/integrity/Disk1/install/runInstaller -paramFile ../oraparam.ini -jreloc
   jre_Path
   ```

   where *jre_Path* contains **jre** folder inside the JDK installation directory.

   The Installer Welcome screen appears.
6. Click **Next**.

   The Select Installation Type screen appears.
7. Select **Complete** and click **Next**.

The Available Product Components screen appears.

8. Select **Network Integrity** and click **Next**.

   The Specify Home Details screen appears.

9. Do all of the following:

   a. In the **Name** field, enter, browse to, or confirm the name of the folder that contains the installation files for the old version of Network Integrity.

   b. In the **Path** field, enter, browse to, or confirm the directory where the folder specified in the **Name** field is located.

   c. Click **Next**.

   The Installer scans the specified directory and folder. The Installer displays a pop-up message if it detects a pre-existing installation of Network Integrity.

10. (Optional) Confirm that you want to override your pre-existing installation.

    The Installer retrieves information about your old Network Integrity installation, such as connection details and user names.

    The Available Product Components screen appears displaying installation information about the installed Network Integrity components.

    The Installer automatically detects the Network Integrity components that can be upgraded.

11. Review the list of components to be upgraded and click **Next**.

    The WebLogic Administration Server Connection Information screen appears displaying the current connection information.

12. Verify the WebLogic Administration Server connection information, enter the WebLogic Server password, and click **Next**.

    The WebLogic Server / Cluster Selection screen appears.

> **Note:**
>
> The Installer does not proceed from the WebLogic Administration Server Connection Information screen if the fields contain errors.

13. Select the same target WebLogic server or cluster of servers belonging to the WebLogic Server domain to upgrade and click **Next**.

    If you are upgrading a cluster of servers, the Cluster Member Server Selection screen appears, where you can select a cluster member for Network Integrity adapters to install or upgrade.

    The Database Type Selection screen appears.

14. Select the same database type that is used by your old Network Integrity installation:

    - If your old installation is connected to a standalone database, select **Standard Oracle 12c Enterprise Database** and click **Next**.

      The Database Connection Information screen appears.

      Do the following:

      a. Verify that the retrieved field values are correct and click **Next**.

b. In the **Password** field, enter the database server password for the user specified in the **User Name** field.

c. Click **Next**.

- If your old installation is connected to an Oracle Real Application Clusters (RAC) database, select **Oracle 12c Real Application Cluster Database** and click **Next**.

  The RAC DB Nodes Connection Information screen appears.

  Do the following:

  a. Verify that the retrieved field values are correct and click **Next**.

  b. In the **Password** field, enter the database server password for the user specified in the **User Name** field.

  c. Click **Next**.

  The Network Integrity Schema User Information screen appears.

> **Note:**
>
> The Installer does not proceed from either the Database Connection Information or RAC DB Nodes Connection Information screen if the fields on these screens contain errors.

15. Do the following:

    a. Verify that the retrieved value in the **Schema User Name** field is correct.

    b. In the **Schema User Password** field, enter the schema user password for the user specified in the **Schema User Name** field.

    c. Click **Next**.

    The NI User ni-internal secure credentials screen appears.

16. Do the following:

    a. In the **User Password** field, define a password for the Network Integrity internal user.

    b. In the **Confirm The User Password** field, enter the password again to confirm it.

    c. Click **Next**.

    The Summary screen appears.

17. Review the Summary screen and click **Install**.

    The Summary screen lists the products and components that are being upgraded. The **Already Installed** list includes products and components that are already up to date and are not being upgraded.

18. Click the **Install** button.

    The Install screen appears, showing the status of the upgrade installation. The Install screen also explains where the upgrade log files are saved (*NI_Home***/oraInventory/logs/installAction***Date_Time***.log**).

    When the Installer completes the upgrade, the End of Installation screen appears displaying the success of the upgrade. This screen also provides the URLs for accessing the new release of Network Integrity. Make a note of the URLs.

19. Click **Installed Products** and verify that the installed version for Network Integrity is correct.

20. In the Installer, click **Exit**.

Post-Upgrade Tasks

After upgrading Network Integrity, do the following, if necessary:

1. Restart the Weblogic Server and log in to the WebLogic console.
2. Go to **Summary of Deployments** and click **CMWSJMSModule**.
3. In the **Configuration** tab, except **NICMWSAdapterQueue**, select and delete all other resources from the Summary of Resources table.
4. Verify that the Network Integrity software upgrade was completed successfully. See "Verifying the Network Integrity Installation" for more information.
5. If you configured an Inventory System in the old version of Network Integrity and specified a password, you need to re-enter the password.
   a. In the new version of Network Integrity, click **Manage Import System**.
   b. Click **Edit**.
   c. Enter the password and click **Save and Close**.
6. Migrate your cartridges to the new version of Network Integrity. See "Migrating Cartridges" for more information.
7. Re-deploy your cartridges. See "Deploying Network Integrity Cartridges" for more information.

Migrating Cartridges

If you developed or extended cartridges for the old version of Network Integrity, you must migrate them to the new version of Network Integrity to continue to use them.

It is not possible to migrate scan instances or scan data. Scan instances have to be manually re-created in Network Integrity. Scan data is re-created when you run a scan.

Production cartridges (those with binaries supplied by Oracle) are already compatible with and can be deployed to the new version of Network Integrity.

Migrate your old custom cartridges to be compatible with the new version of Network Integrity using the Design Studio Cartridge Migration Tool. See "Getting Started with Design Studio for Network Integrity (1)" in *Design Studio Platform Online Help* for more information.

The procedure for migrating cartridges assumes you have two Design Studio environments: one for the old version of Network Integrity, and one for the new version of Network Integrity.

Ensure the imported project is not read-only. The cartridge migration will fail if the project is read-only.

It is important to make sure that all the dependent projects exist in the workspace before importing a Network Integrity project. The migration tool will automatically set the dependencies when migrating Network Integrity projects, if the dependent projects exist in the workspace. If multiple projects are imported into Design Studio at the same time, move the dependent project to the top of the order in the cartridge upgrade dialog, so that the dependent project will be migrated first.

To migrate a custom cartridge (a cartridge with binaries not supplied by Oracle):

1. Using the old Design Studio environment for Network Integrity, do the following:

a. Select the Design Studio perspective.
b. Select the Studio Projects view.
c. Select the cartridge project and, from the **Project** menu, deselect **Build Automatically**.
d. From the **Project** menu, select **Clean**.
e. Select the **Navigation** view.
f. Right-click the cartridge project folder and select **Close Project**.

2. Using the new installation of Design Studio for Network Integrity, do the following:
   a. Select the Design Studio perspective.
   b. Select the Studio Projects view.
   c. Right-click anywhere in the Studio Projects view and select **Import**.

      The Import Project dialog box appears.
   d. Verify that the imported project is not “read-only."
   e. Locate the cartridge project and import it.
   f. Double-click the cartridge project folder.

      The cartridge properties appear.
   g. Verify that the **Target Version** field value matches the Network Integrity version.

      > **Note:**
      >
      > If the Target Version field is not editable, it may mean that the cartridge is sealed, read-only, or under source control.

   h. Perform all necessary pre-build steps particular to your cartridge.
   i. From the **Project** menu, enable **Build Automatically**.
   j. From the **Project** menu, select **Clean**.

      The cartridge project is automatically built. The binary file is produced and written to the **cartridgeBin** directory.

About Rolling Back Network Integrity

If the Installer fails to successfully upgrade Network Integrity, you must manually restore the WebLogic server domain, the database schema, and the database domain. See "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide* for more information about restoring the database. See your WebLogic Server documentation for more information about restoring the WebLogic Server domain.

10

Setting Up Network Integrity for Single Sign-On Authentication

This chapter provides instructions for setting up Oracle Communications Network Integrity for single sign-on (SSO) authentication.

Network Integrity implements the single sign-on (SSO) authentication solution using Oracle Access Manager, which enables you to seamlessly access multiple applications without being prompted to authenticate for each application separately. You can also use SAML 2.0 to enable Single Sign-On (SSO) and Single Log-Out (SLO) in Network Integrity which allows you to access applications with a single username and password combination. For more information on security concepts and definitions, see “Security Assertion Markup Language (SAML)” section of the *Understanding Security for Oracle WebLogic Server Guide*. The main advantage of SSO is that you are authenticated only once, when you log in to the first application; you are not required to authenticate again when you subsequently access different applications with the same (or lower) authentication level (as the first application) within the same web browser session.

Network Integrity also supports the single logout (SLO) feature. If you access multiple applications using SSO within the same web browser session, and then if you log out of any one of the applications, you are logged out of all the applications.

This solution supports SSO authentication between Network Integrity and Oracle Communications Unified Inventory Management (UIM) applications.

For more information, see *Fusion Middleware Administrator's Guide for Oracle Access Management*.

Setting up Network Integrity for SSO authentication includes the following tasks:

Using Oracle Access Manager:

- Installing Required Software
- Configuring Network Integrity to Enable SSO Authentication

Using SAML 2.0 and IDP:

- Installing Required Software
- Configuring Network Integrity to Enable Authentication using SSO/SLO and IDP using SAML

Installing Required Software

Install and configure the following software that Network Integrity requires for implementing SSO authentication:

- External Lightweight Directory Access Protocol (LDAP) Server. Oracle recommends Oracle Internet Directory (OID) as the LDAP store external to the WebLogic server.
- Oracle Access Manager (OAM), included with Oracle Identity and Access Management
- Oracle WebLogic Server

- Oracle HTTP Server (OHS)
- Oracle HTTP Server WebGate for OAM

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

To install the required software, do the following:

1. Install WebLogic Server and create the Oracle Middleware Home directory (*MW_Home*). This is the directory in which the Oracle Fusion Middleware products are installed.

   For more information, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Install Oracle Access Manager (OAM) in the same Oracle Middleware Home directory that you created when you installed Oracle WebLogic Server.

   For more information, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3. Install and configure Oracle HTTP Server, which is a Web server that acts as the front end to the Oracle WebLogic Server.

   For more information, *Oracle Fusion Middleware Installing and Configuring Oracle HTTP Server*.

4. Install and configure Oracle HTTP Server WebGate for OAM.

   A WebGate is a web-server plug-in for Oracle Access Manager (OAM) that intercepts HTTP requests and forwards them to the Access Server for authentication and authorization. For more information, see *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager.*.

5. Install an external LDAP server. For example, Oracle Internet Directory (OID). Oracle recommends Oracle Internet Directory as the LDAP store external to the WebLogic Server. See the following for more information.

   - Installing and Configuring Oracle Internet Directory
   - Setting Up Oracle Internet Directory

   For information on installing and configuring Oracle Internet Directory, see *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

6. Configure the external LDAP as the user identity store in OAM.

   For more information, see *Fusion Middleware Administrator's Guide for Oracle Access Management*.

7. Register the Oracle HTTP Server WebGate instance with OAM by using the Oracle Access Manager Administration Console.

   For more information, see the chapter on “Registering Partners (Agents and Applications) by Using the Console" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

8. Install Oracle WebLogic Server 12c. See "Installing and Configuring Oracle WebLogic Server " for more information.

9. Continue with the steps in "Configuring Network Integrity to Enable SSO Authentication".

Configuring Network Integrity to Enable SSO Authentication

Configuring Network Integrity to enable SSO authentication involves the following tasks:

- Installing and Deploying Network Integrity Specifying the External LDAP Provider

- Configuring the Frontend URL in Administration Console
- Creating and Configuring Authentication Providers for OAM SSO
- Configuring web.xml for the OAM Identity Asserter
- Configuring the mod_wl_ohs Plug-In for Oracle HTTP Server
- Protecting Resources For SSO Authentication
- Excluding Resources From SSO Authentication

Installing and Deploying Network Integrity Specifying the External LDAP Provider

To install and deploy Network Integrity specifying the external LDAP security provider:

1. Configure authentication providers for your external security provider. See "Configuring Custom Authentication Providers" for more information.

   Oracle recommends Oracle Internet Directory as the LDAP store external to the WebLogic server. See "Installing and Configuring Oracle Internet Directory" for more information.

2. Install and deploy Network Integrity specifying the external LDAP provider.

   When installing Network Integrity, in the Security Provider Selection screen, select the **External Security Provider** option, and then enter the required information in the External Security Provider Connection Information screen. Follow the instructions provided in "Installing Network Integrity by Using Interactive Install".

Configuring the Frontend URL in Administration Console

Set the front-end host and port so that all requests to access the applications (Network Integrity) deployed in the WebLogic administration server go through the Oracle HTTP server:

To configure the Frontend URL:

1. Log in to the Oracle WebLogic Server administration console.
2. In the **Domain Structure** tree, expand **Environment**, and do one of the following:
   - Select **Clusters** (if the server instances to which you want to proxy requests from Oracle HTTP Server are in a cluster)
   - Select **Servers**.

     The Summary of Servers page appears.
3. Select the server or cluster to which you want to proxy requests from Oracle HTTP Server.
4. Click the **Configuration** tab.
5. On the **General** tab, in the Advanced section, select the **WebLogic Plug-In Enabled** check box.
6. If you selected Servers in step 2, repeat steps 3 through 5 for the other servers to which you want to proxy requests from Oracle HTTP Servers.
7. Click **Save**.
8. Restart the WebLogic server.
9. Log in to the Oracle WebLogic Server administration console.
10. In the **Domain Structure** tree, expand **Environment**, and click **Servers**.

The Summary of Servers screen appears.

11. Click the server where Network Integrity is deployed.

    The settings screen for the server appears.

12. Click the **Protocols** tab.
13. On the **HTTP** tab, do the following:
14. In the **Frontend Host** field, enter the name of the Oracle HTTP Server host machine.

    WebLogic Server uses this value instead of the one in the host header. All HTTP URLs are redirected to this HTTP host.

15. In the **Frontend HTTP Port** field, enter the Oracle HTTP Server port number.

    All HTTP URLs are redirected to this HTTP port.

16. In the **Frontend HTTPS Port** field, enter the Oracle HTTP Server SSL port number.

    All HTTPS URLs are redirected to this HTTPS port.

17. Click **Save**.
18. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

Creating and Configuring Authentication Providers for OAM SSO

You must create a new OAMIdentityAsserter provider for OAM SSO in WebLogic Server Administration Console.

To create the OAMIdentityAsserter provider:

1. Log in to the WebLogic Server Administration Console.
2. Under Your Application's Security Settings, click **Security Realms**.

   The Summary of Security Realms screen appears.

3. Select the realm *YourRealmName*, for which you need to configure the OAM identity asserter.

   The Settings For *YourRealmName* screen appears.

4. Click the **Providers** tab, and then click the **Authentication** tab.
5. Click **New**.

   The Create a New Authentication Provider screen appears.

6. In the **Name** field, enter a name for the new provider; for example, **OAM ID Asserter**.
7. From the **Type** list, select **OAMIdentityAsserter**.
8. Click **OK**.

   The Settings For *YourRealmName* screen appears, showing the newly created authentication name in the **Authentication** tab.

9. Click the link for *AuthenticatorName* (For example, OAM ID Asserter).

   The Settings for *AuthenticatorName* screen appears.

10. On the **Common** tab, from the **Control Flag** list, select **REQUIRED**.
11. Under **Active Types**, use the directional arrow buttons to move **OAM_REMOTE_USER** from the **Available** column to the **Chosen** column.

Ensure that **OAMAuthnCookie** and **OAM_IDENTITY_ASSERTION** are present in the **Chosen** column.

12. Click **Save**.
13. Click the **Providers** tab, and then click the **Authentication** tab.
14. Click the link for DefaultAuthenticator and ensure that the default authenticator's control flag is set to **SUFFICIENT**.
15. Click the link for OID/OUD Authenticator (for example, OracleInternetDirectoryAuthenticator) and ensure that the OID/OUD authenticator's control flag is set to **SUFFICIENT**.

    See "Configuring the Authentication Provider" for more information.
16. On the **Authentication** tab, click **Reorder**.

    The Reorder Authentication Providers screen appears
17. Use the up and down arrows to reorder the listed authentication providers as follows:
    - OAMIdentityAsserter (REQUIRED)
    - OracleInternetDirectoryAuthenticator (SUFFICIENT)
    - DefaultAuthenticator (SUFFICIENT)
18. Click **OK**.

Configuring web.xml for the OAM Identity Asserter

You configure the **web.xml** file for the OAM Identity Asserter by updating the deployment plan. You use deployment plans to change an application's WebLogic Server configuration for a specific environment without modifying existing deployment descriptors.

To update the web.xml file:

1. For using Oracle Access Manager Identity Asserter, you must specify the authentication method as CLIENT-CERT in the **web.xml** file for the appropriate realm by editing the deployment plan. The **web.xml** file is located at *NI_Home***/app/NetworkIntegrity.ear/NetworkIntegrityApp_NetworkIntegrityUI_webapp1.war/WEB-INF/**, where *NI_Home* is the directory in which the Network Integrity software is installed.
   - Depending on your deployment configuration, do one of the following:
     - If Network Integrity is installed in a single server environment, navigate to and open the *NI_Home***/app/plan/Plan.xml** file.
     - If Network Integrity is installed in a clustered server environment, navigate to and open the *NI_Home***/app/plan/ClusterPlan.xml** file.
   - Update the variable-definition and variable-assignment elements; specifically, add CLIENT-CERT as follows:

```
<variable-definition>
 <variable>
     <name>ClientCertAuthMethod</name>
     <value>CLIENT-CERT</value>
 </variable>
 <variable>
     <name>RealmName</name>
     <value>myrealm</value>
 </variable>
</variable-definition>
<module-override>
```

```
   <module-name>NetworkIntegrityApp_NetworkIntegrityUI_webapp1.war</module-name>
   <module-type>war</module-type> <module-descriptor external="false">
     <root-element>web-app</root-element>
     <uri>WEB-INF/web.xml</uri>
 <variable-assignment>
     <name>ClientCertAuthMethod</name>
     <xpath>/web-app/login-config/auth-method</xpath>
     <operation>replace</operation>
 </variable-assignment>
 <variable-assignment>
     <name>RealmName</name>
     <xpath>/web-app/login-config/realm-name</xpath>
     <operation>add</operation>
  </variable-assignment>
    </module-descriptor>
</module-override>
```

- Save and close the **Plan.xml/ClusterPlan.xml** file.

2. Update the deployment plan for the currently-deployed Network Integrity application:
   a. Log in to the WebLogic Server Administration Console.
   b. In the **Domain Structure** tree, expand **Environment**, and click **Deployments**.

      The Summary of Deployments screen appears.
   c. Select the check box beside NetworkIntegrity.
   d. Click **Update**.

      The Update Application Assistant page appears.
   e. Select **Update this application in place with new deployment plan changes** and click **Next**.
   f. (Optional) Click **Change Path** beside the **Deployment Plan Path** field and browse to the location of the **Plan.xml/ClusterPlan.xml** file.

      The Summary page appears.
   g. Click **Finish**.
   h. In the Change Center of the Administration Console, click **Activate Changes**, which activates these changes.

Configuring the mod_wl_ohs Plug-In for Oracle HTTP Server

You can configure mod_wl_ohs plug-in by specifying directives in the **mod_wl_ohs.conf** file to enable the Oracle HTTP Server instances to forward requests to the applications deployed on the Oracle WebLogic server or clusters.

For more information, see Oracle Fusion Middleware Using Web Server Plug-Ins with Oracle WebLogic Server.

To configure the mod_wls_ohs plug-in:

1. Open the **mod_wl_ohs.conf** file from the following location:

   *Domain_Home***/config/fmwconfig/components/OHS/ohs1/**

   where:

   Domain_Home is the directory containing the configuration for the domain into which Oracle HTTP Server is installed.

2. Add directives within the <IfModule weblogic_module> element in the configuration file as follows:

   - To forward requests to the Network Integrity application running on a single Oracle WebLogic Server instance, specify **/NetworkIntegrity** within the <location> element as follows:

     ```
     <IfModule weblogic_module>
     <Location /NetworkIntegrity>
     SetHandler weblogic-handler
     WebLogicHost host
     WebLogicPort port
     </Location>
     </IfModule>
     ```

     where:

     – *host* is the name of the WebLogic Administration server machine

     – *port* is the port of the server on which Network Integrity is installed

   - To forward requests to the Network Integrity application running on a cluster of Oracle WebLogic Server instances, specify **/NetworkIntegrity** within a new <location> element as follows:

     ```
     <IfModule weblogic_module>
     <Location /NetworkIntegrity>
     SetHandler weblogic-handler
     WebLogicCluster host1:port1,host2:port2
     </Location>
     </IfModule>
     ```

     where:

     – *host1* and *host 2* are host names of the managed servers

     – *port1* and *port2* are ports of the managed servers

   - To forward requests to the Network Integrity Web services running on a single Oracle WebLogic Server instance, specify **/NetworkIntegrityApp-NetworkIntegrityControlWebService-context-root** within the <location> element as follows:

     ```
     <IfModule weblogic_module>
     <Location /NetworkIntegrityApp-NetworkIntegrityControlWebService-context-root>
     SetHandler weblogic-handler
     WebLogicHost host
     WebLogicPort port
     </Location>
     </IfModule>
     ```

     where:

     – *host* is the name of the WebLogic Administration server machine

     – *port* is the port of the server on which Network Integrity is installed

   - To forward requests to the Network Integrity Web services running on a cluster of Oracle WebLogic Server instances, specify **/NetworkIntegrityApp-NetworkIntegrityControlWebService-context-root** within a new <location> element as follows:

     ```
     <IfModule weblogic_module>
     <Location /NetworkIntegrityApp-NetworkIntegrityControlWebService-context-root>
     SetHandler weblogic-handler
     ```

```
WebLogicCluster host1:port1,host2:port2
</Location>
</IfModule>
```

where:

- *host1* and *host 2* are host names of the managed servers
- *port1* and *port2* are ports of the managed servers

- To forward requests to the Network Integrity application running on a single Oracle WebLogic Server instance to support integration with UIM, specify **/NI_Uim** within the <location> element as follows:

```
<IfModule weblogic_module>
<Location /NI_Uim>
SetHandler weblogic-handler
WebLogicHost host
WebLogicPort port
</Location>
</IfModule>
```

where:

- *host* is the name of the WebLogic Administration server machine
- *port* is the port of the server on which Network Integrity is installed

- To forward requests to the Network Integrity application running on a cluster of Oracle WebLogic Server instances to support integration with UIM, specify **/NI_Uim** within a new <location> element as follows:

```
<IfModule weblogic_module>
<Location /NI_Uim>
SetHandler weblogic-handler
WebLogicCluster host1:port1,host2:port2
</Location>
</IfModule>
```

where:

- *host1* and *host 2* are host names of the managed servers
- *port1* and *port2* are ports of the managed servers

- To forward requests to the Network Integrity application running on a single Oracle WebLogic Server instance into which you want to deploy cartridges, specify **/cartridge** within the <location> element as follows:

```
<IfModule weblogic_module>
<Location /cartridge>
SetHandler weblogic-handler
WebLogicHost host
WebLogicPort port
</Location>
</IfModule>
```

where:

- *host* is the name of the WebLogic Administration server machine
- *port* is the port of the server on which Network Integrity is installed

- To forward requests to the Network Integrity application running on a cluster of Oracle WebLogic Server instances into which you want to deploy cartridges, specify **/cartridge** within a new <location> element as follows:

```
<IfModule weblogic_module>
<Location /cartridge>
SetHandler weblogic-handler
WebLogicHost host
WebLogicPort ms_port
</Location>
</IfModule>
```

where:

- *host* is the machine where the managed server is running
- *ms_port* is the port of the managed server running on the host specified in the *host* variable above

For example, if a managed server **networkintegrity01** with listen port **8065** is running on the machine **NETINT1**, you must specify the following:

```
<IfModule weblogic_module>
<Location /cartridge>
SetHandler weblogic-handler
WebLogicHost NETINT1
WebLogicPort 8065
</Location>
</IfModule>
```

Protecting Resources For SSO Authentication

You must protect resources (for example, the Network Integrity application) in Oracle Access Manager for SSO authentication. For more information, see *Fusion Middleware Administrator's Guide for Oracle Access Management*.

To protect resources for SSO authentication:

1. Open the Oracle Access Management Console.
2. On the **Policy Configuration** tab, expand the **Application Domains** node.
3. Expand the node for the application domain.
4. Within the application domain, expand the **Resources** node.
5. Click the **Resources** tab, and then click the **New Resource** button in the upper-right corner of the Search page.

   The Resource Definition page appears.
6. Do the following to configure the Network Integrity application as a protected resource for SSO authentication:
   - From the **Type** list, select **HTTP**.
   - In the **Resource URL** field, enter **/NetworkIntegrity/.../***.
   - From the **Protection Level** list, select **Protected**.
7. Click **Apply**.

Excluding Resources From SSO Authentication

You can exclude HTTP resources that do not require SSO authentication. For example, when accessing a Web Services Description Language (WSDL) document for Web services. The excluded resources are public and do not require an OAM Server check for authentication.

When allowing access to excluded resources, WebGate does not contact the OAM Server. Excluded resources cannot be added to any user-defined policy in the console. For more information, see *Fusion Middleware Administrator's Guide for Oracle Access Management*.

To exclude resources from SSO authentication:

1. Open the Oracle Access Management Console.
2. On the **Policy Configuration** tab, expand the **Application Domains** node.
3. Expand the node for the application domain.
4. Within the application domain, expand the **Resources** node.
5. Click the **Resources** tab, and then click the **New Resource** button in the upper-right corner of the Search page.

   The Resource Definition page appears.
6. Do the following to exclude Network Integrity Web services from SSO authentication:
   - From the **Type** list, select **HTTP**.
   - In the **Resource URL** field, enter the following to exclude Network Integrity Web services from SSO authentication:

     /NetworkIntegrityApp-NetworkIntegrityControlWebService-context-root/.../*
   - From the **Protection Level** list, select **Excluded**.
7. Click **Apply**.
8. Click the **New Resource** button.

   The Resource Definition page appears.
9. Do the following to exclude the Network Integrity cartridge deployment process from SSO authentication:
   - From the **Type** list, select **HTTP**.
   - In the **Resource URL** field, enter **/cartridge/.../***.
   - From the **Protection Level** list, select **Excluded**.
10. Click **Apply**.
11. Click the **New Resource** button.

    The Resource Definition page appears.
12. Do the following to exclude the Network Integrity and UIM integration process from SSO authentication:
    - From the **Type** list, select **HTTP**.
    - In the **Resource URL** field, enter **/NI_Uim/.../***.
    - From the **Protection Level** list, select **Excluded**.
13. Click **Apply**.

Installing Required Software

Install and configure the following software that Network Integrity requires for implementing for SSO authentication using SAML 2.0:

- Oracle WebLogic Server

There is no need to install a separate instance of WebLogic server since the instance being used for running Network Integrity will be sufficient.

- Identity Provider (IDP)

> **Note:**
>
> In the procedure to configure SAML 2.0 for NI, Oracle IDCS is used as IDP. To use Oracle IDCS as your IDP, you will require a license. You can choose to use any IDP that supports SAML 2.0. Refer the documentation of the corresponding IDP to configure it with the application.

Configuring Network Integrity to Enable Authentication using SSO/SLO and IDP using SAML

Configuring Network Integrity to enable SSO authentication and IDP using SAML involves the following tasks:

1. Creating SAML Assertion Provider and SAML Authenticator
2. Specifying General Information
3. Configuring the SAML Service Provider
4. Updating the deployment Plan of Network Integrity
5. Registering the NI Application in Identity Cloud Service or any other IDP
6. Registering IDP in WebLogic
7. Verifying SAML Configuration

Creating SAML Assertion Provider and SAML Authenticator

To create SAML Assertion Provider and SAML Authenticator, do the following:

1. Access the WebLogic Server Console as administrator (for example, weblogic).
2. Click **Lock & Edit**.
3. Click **Security Realm**.
4. Click **myrealm**.
5. Click **Providers**, and then click **New**.
6. Enter *SAML2IdentityAsserter* as **Name**, select ***SAML2IdentityAsserter*** as **Type**, and then click **OK**.

   The *SAML2IdentityAsserter* is displayed under the Authentication Providers table.
7. On the **Providers** page, click **New**.
8. Enter *SAMLAuthenticator* as **Name**, select ***SAMLAuthenticator*** as **Type**, and then click **OK**.

   The *SAMLAuthenticator* is displayed under the Authentication Providers table.
9. Click **Reorder**.
10. Select and reorder the providers in the following order:

a. *SAML2IdentityAsserter*
b. *SAMLAuthenticator*
c. DefaultAuthenticator
d. DefaultIdentityAsserter

11. Click **OK**.
12. Click **SAMLAuthenticator**.
13. Select *SUFFICIENT* as **Control Flag** and then click **Save**.
14. Return to the Providers page.
15. Click **DefaultAuthenticator**.
16. Select *SUFFICIENT* as **Control Flag** and then click **Save**.
17. Click **Activate Changes**.
18. Restart the server.

Specifying General Information

1. Access the WebLogic Server Console as administrator.
2. Click **Lock & Edit**.
3. Click **Environment** > **Servers**.
4. Click the manager server (in this case, AdminServer) that is hosting the Inventory application (for example, **ms1**).

> **Note:**
>
> In a clustered environment, the below steps need to be performed on each managed server that is hosting the Inventory application (not 'proxy' and 'admin server').

5. Click **Federation Services** > **SAML 2.0 General**.

> **Tip:**
>
> **Tip:** You can use this page to define the Site Information and additional settings for the SAML assertion, plus generate the service provider metadata file.

6. Modify the General settings as follows to enter information accordingly.

Attribute	Sample Value
Published Site URL	*https://<HostName>:<NIPort>/saml2*

Attribute	Sample Value
Entity ID	samlNI **Tip:** You can enter any identification value, as long it's unique in Identity Cloud Service and in your WebLogic Domain.
Recipient Check Enabled	Deselected

7. Click **Save**.

Configuring the SAML Service Provider

1. Access the WebLogic Server Console as administrator.
2. Click **Lock & Edit**.
3. Click **Environment** and **Servers**.
4. Select the manager server (in our case AdminServer) that is hosting Inventory application (for example, **ms1**).

> **Note:**
> In a clustered environment, the below steps need to be performed on each managed server that is hosting the Inventory application. (not 'proxy' and 'admin server').

5. Select **Configuration**, then **Federation Services** and then select **SAML 2.0 Service Provider**.
6. Select **Enabled**.
7. Select **Single Logout Enabled** (*).
8. Select **Assertion Subject Timeout Check** (*).
9. Optionally provide the list of **Allowed redirect URIs** to be used but Service Provide for after logout redirections. (*).
10. Select POST as **Preferred Binding**.
11. Enter *https://<HostName>:<NIPort>/NetworkIntegrity/faces/login.jspx* as the **Default URL**, and then click **Save**.
12. Click **Activate Changes**.

Updating the deployment Plan of Network Integrity

Changes have to be made on top of your Plan.xml (Standalone) or ClusterPlan.xml (Cluster) depending on your environment, for the authentication to happen. The file will be present inside your domain_home/ni/plan folder .

Modify the logout URL to *https://<MachineIP>:<Port>/saml2/sp/slo/init*. Replace the port and machine IP as per your NI machine.

Registering the NI Application in Identity Cloud Service or any other IDP

In this section, you register Network Integrity as a SAML application in Oracle Identity Cloud Service.

1. Access the Identity Cloud Service console and log in as administrator.
2. Navigate to the **Domains** and select the domain (in our case *Default domain*) to add NI as SAML application.
3. Click **Add application** button to register Inventory as SAML application.
    a. Choose **SAML Application** and click the **Launch app catalog** button.
    b. Enter*NI Application*as **Name** and *NI Application as SAML application*as **Description**.
    c. Click **Next** button at the bottom of the page.
    d. Enter *samlNI* as **Entity ID**. (This should be same as the value provided in above section i.e., ***Configure the SAML Service Provider Settings*** under **Federation Services** > **SAML 2.0 General**.)
    e. Enter *https://<Hostname>:<NIPORT>/saml2/sp/acs/post*as **Assertion consumer URL**.
    f. Choose *Unspecified* as **Name ID format**.
    g. Choose *Username* as **Name ID value**.
    h. Upload the **Signing certificate** of your application. This is needed for SLO to work.
4. You can download the certificate from the browser, from the NI login page
    a. check **Enable single logout** checkbox.
    b. Enter *https://Hostname:NIPORT/saml2/sp/slo as* ***Single Logout URL and Logout Response URL****.*
    c. Set ***Require Encrypted Assertion : NO***
    d. Click **+ Additional attribute** at the right bottom corner of the page.
        i. Enter *Groups* as **Name**.
        ii. Choose *User attribute* as **Type**.
        iii. Choose *Group* membership as **Type value**.
        iv. Choose *All groups* as **Condition**.
    e. Click **Finish**.
5. Click the **Activate** button for the create application within NI.
    a. Click **Activate application** button in the pop-up window.
6. Click the **Download identity provider metadata** button for downloading the IDP's metadata xml (for example, IDCSMetadata.xml).
7. Click the **Users** on the left side pane to assign users.
    a. Click the **Assign users** for adding the domain users to the registered application.
    b. Choose the desired users from the pop-up window and click **Assign**.

c. Click Groups on the left side pane to assign groups (ensure '*NetworkIntegrityGroup, NetworkIntegrityRole and JDGroup*' group is created/added to your domain prior to this step).

d. Click **Assign groups** for adding the domain groups to the registered application.

e. Choose the 3 groups mentioned in Step 7c from the pop-up window and click **Assign**.

Registering IDP in WebLogic

In this section, you register Oracle Identity Cloud Service as a SAML Identity Provider in WebLogic.

1. Upload the IDCSMetadata.xml obtained from the IDP to the server hosting WebLogic (for example, under <Domain_Home>/NI/IDCSMetadata.xml).
2. Access the WebLogic Administration Server Console as administrator.
3. Click **Security Realm**.
4. Click **myrealm**.
5. Click **Providers**, and then click **SAML2IdentityAsserter**.
6. Click **Management**, and then click on **New** and then **New Web Single Sign-On Identity Provider Partner**.

   The Create a Web Single Sign-On Identity Provider Partner page appears.
7. In the **Name** field, enter WebSSO-IdP-Partner-1.
8. In the **Path** field, enter the path to the XML file that contains the identity provider's metadata.
9. Click **OK**.
10. Click WebSSO-IdP-Partner-1 link.
11. Ensure that the identity provider details are displayed in the **Site Info** and **Single Sign-On Signing Certificate** tabs.
12. In the **General** tab, select the **Enabled**, **Virtual User**, and **Process Attributes** check box. This is required for allowing IDP users with UIM group to be allowed access to NI UI. See "Configuring the SAML Authentication Provider" in *Fusion Middleware Administering Security for Oracle WebLogic Server 12.1.3* for more information.
13. In the **Redirect URIs** field, enter */NetworkIntegrity/**.
14. Click on **Save**.

    The WebLogic server displays a confirmation message.
15. Sign-out of the WebLogic Server and close your browser.

Verifying SAML Configuration

1. Go to the URL http://<Hostname>:<NIPort>/NetworkIntegrity

   The login page of the identity provider is displayed.
2. Enter the login credentials.

   The NI home page appears.
3. Once logged in, user can logout by clicking the Logout option from the top right corner of the page.

Based on the configurations in Identity Provider, either the login page is displayed or a successful logged message is shown. Close the browser or tab.

4. To verify SLO register multiple applications in the same domain in IDCS. When you hit logout button for one application, it should log you out of other applications also.

11

Installing Patches

This chapter describes how to install patches on Oracle Communications Network Integrity.

See the patch ReadMe file, included in the patch download, for information about the contents of a patch.

About Patching Network Integrity

Network Integrity patches are posted on the My Oracle Support Web site:

https://support.oracle.com

Most Network Integrity patches are installed using the Oracle Universal Installer. If the Installer fails to install the patch, you must restore your database schema and domain, and your WebLogic Server domain.

The patch ReadMe file specifies whether to use the Installer to install a patch or whether to follow other installation instructions.

> **Caution:**
>
> Always read the patch ReadMe file in its entirety before installing a patch.

Install all patches for a release of Network Integrity to benefit from the contents of each patch. For example, if Network Integrity 7.5 has three available patches, install each patch. The patch with the latest date does not contain the content from the previous two patches.

Some patches contain fixes and functionality that may not be of any interest to you or may apply to features that you have not installed or purchased. Read the patch ReadMe file to determine if you must install the patch.

Some patches are password protected. To request the password to download a protected patch, open a Service Request on the My Oracle Support Web site.

Planning Your Patch Installation

Before installing a patch, verify your version of Network Integrity and ensure the patch is not already installed.

Oracle recommends scheduling your patch installation during non-peak hours to minimize the disruption to your operations.

Ensure that Network Integrity is not running any operations, such as scans or blackouts.

As a precaution against a failed patch installation, Oracle recommends that you back up your database schema for Network Integrity, database domain for Network integrity, and your WebLogic Server domain for Network Integrity. See "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide* for more information about

backing up the database. See your WebLogic Server documentation for more information about backing up your WebLogic Server domain. See "About Rolling Back Network Integrity" for more information about restoring Network Integrity after a failed patch installation.

Oracle recommends installing a patch on a test system with a copy of your production data before installing the patch on your production system. Test the patch by logging into Network Integrity and verifying the version number of installed components

Installing a Patch

To install a patch on Network Integrity:

1. Create a directory (*dir*).
2. Download the patch for your operating system from the My Oracle Support Web site:

   `https://support.oracle.com`

   and save it to *dir*:
3. Extract the contents of the software pack to *dir*.

   The extracted software pack has the following structure:

   NI-*version*/Disk1/install/
4. (IBM AIX systems only) Stop and restart the WebLogic Server domain for Network Integrity.
5. Run the following command:

   ```
   . /dir/integrity/Disk1/install/runInstaller -jreloc jre_Path
   ```

   where *jre_Path* contains the **jre** folder inside the Java Development Kit (JDK) installation directory.

   The Installer Welcome screen appears.
6. Click **Next**.

   The Specify Home Details screen appears.
7. Do the following:
   a. In the **Name** field, enter, browse to, or confirm the name of the folder that contains the installation files for Network Integrity.
   b. In the **Path** field, enter, browse to, or confirm the directory where the folder specified in the **Name** field is located.
   c. Click **Next**.

   The Installer scans the specified directory and folder and retrieves information about your Network Integrity installation, such as connection details and user names.

   The WebLogic Administration Server Connection Information screen appears, displaying the current connection information.
8. Verify the WebLogic Administration Server connection information, enter the WebLogic Server password, and click **Next**.

   The WebLogic Server/Cluster Selection screen appears.

> **Note:**
>
> The Installer does not proceed from the WebLogic Administration Server Connection Information screen if any field contains errors.

9. Select the same target WebLogic server or cluster of servers belonging to the WebLogic Server domain and click **Next**.

   If you are installing a patch on a cluster of servers, the Cluster Member Server Selection screen appears, where you can select a cluster member for Network Integrity adapters to patch.

   The Database Type Selection screen appears.

10. Select the same database type that is used by your old Network Integrity installation:

    - If your old installation is connected to a standalone database, select **Standard Oracle 12c Enterprise Database** and click **Next**.

      The Database Connection Information screen appears.

      Do the following:

      a. Verify that the retrieved field values are correct and click **Next**.

      b. In the **Password** field, enter the database server password for the user specified in the **User Name** field.

      c. Click **Next**.

      The Network Integrity Schema User Information screen appears.

    - If your old installation is connected to an Oracle Real Application Cluster (RAC) database, select **Oracle 12c Real Application Cluster Database** and click **Next**.

      The RAC DB Nodes Connection Information screen appears.

      Do the following:

      a. Verify that the retrieved field values are correct and click **Next**.

      b. In the **Password** field, enter the database server password for the user specified in the **User Name** field.

      c. Click **Next**.

      The Network Integrity Schema User Information screen appears.

      > **Note:**
      >
      > The Installer does not proceed from either the Database Connection Information screen or the RAC DB Nodes Connection Information screen if any field on these screens contains errors.

11. Do the following:

    a. Verify that the retrieved value in the **Schema User Name** field is correct.

    b. In the **Schema User Password** field, enter the schema user password for the user specified in the **Schema User Name** field.

    c. Click **Next**.

The Summary screen appears.

12. Review the Summary screen and click **Install**.

    The Install screen appears, showing the status of the installation.

    Installation log files for Linux and Solaris are saved to *NI_Home*/**oraInventory/logs/installAction***Date_Time*.**log**.

    Installation log files for IBM AIX are saved to **export/home/oracle/oraInventory/logs/installAction***Date_Time*.**log**.

    When the Installer completes the installation, the End of Installation screen appears. This screen provides the URLs for accessing the new release of Network Integrity. Make a note of the URLs.

13. Click **Installed Products** and verify that the patch is listed.

14. Click **Exit**.

12

Uninstalling Network Integrity

This chapter describes how to uninstall Oracle Communications Network Integrity.

About Uninstalling Network Integrity

You use the Oracle Universal Installer to uninstall Network Integrity. You can also uninstall other components of the Network Integrity product using the Oracle Universal Installer.

Uninstalling Network Integrity or Network Integrity Components

To uninstall Network Integrity, or a component belonging to the Network Integrity product:

1. Go to the location of the **install** folder into which you have untarred the original Network Integrity installation file. The folder structure should look something like the folder structure shown here:

   ```
   integrity/Disk1/install
   ```

2. In the **install** folder, run the OUI executable file **runInstaller** by using the following command syntax:

   ```
   ./runInstaller
   ```

   The Oracle Universal Installer installation wizard starts.

   The Welcome screen appears.

3. Click **Deinstall Products**.

   The Inventory screen appears.

4. Select the item(s) you want to uninstall.

5. Click **Remove**.

   > **Note:**
   >
   > Selecting **Show Empty Homes** displays any previously created Oracle product homes. Select displayed homes, or folders, to remove them.

   The User Input screen appears.

6. In the **WebLogic User Password** field, enter your WebLogic user password, and click **OK**.

   The Confirmation screen appears.

7. View and confirm your selection, and click **Next**.

   You can see the remove progress as the selected components are uninstalled.

   The installer removes Network Integrity files and directories, except the logs. If required, delete the log files manually. The logs can be found at the following location:

*CentralInventorylocation***/logs/**

> **Note:**
>
> Some files and directories will not be removed from the Network Integrity home directory during uninstallation. Verify that these remaining files and directories do not contain any customized information that may be necessary for upgrades, and if required, remove the files manually.
>
> The Network Integrity schema, Network Integrity user, Cartridge Deployer Client and CMWS user will not be removed during uninstallation. The database schema and application users can be used by other applications, so they should not be deleted.

8. Remove the MDS schema user. Refer to *Oracle Fusion Middleware Repository Creation Utility User's Guide* for details on removing/dropping the schema.

Uninstalling Network Integrity Using the Silent Mode

Use the following command to uninstall Network Integrity:

```
./runInstaller -responseFile path -silent -deinstall
```

Where *path* is the location of the response file that was created during silent mode installation of Network Integrity.

After a successful uninstall, you get a message indicating that Network Integrity has been uninstalled successfully.

13

Troubleshooting the Network Integrity Installation

This chapter describes how to troubleshoot the Oracle Communications Network Integrity installation. For more information on troubleshooting Network Integrity, see "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide*. To verify that the installation was successful, see "Verifying the Network Integrity Installation".

Common Problems and Their Solutions

This section describes the following installation problems, and how to resolve them:

- Problem: Installer Fails to Update Application KEYSTORE Table
- Problem: Installer Fails to Update Application INFORMATION Table
- Problem: Inability To Run Scans or Resolve Discrepancies After Upgrading
- Problem: Unable to Load Performance Pack
- Problem: Application Server Takes a Long Time to Start

Problem: Installer Fails to Update Application KEYSTORE Table

If the installer fails to update the application KEYSTORE table, the installer is interrupted and the following error message appears:

```
Unable to update application key store 'AppKeyStore', please check log files for more
details. Refer to Network Integrity documentation for executing this step manually.
```

Solution

Click the **Continue** button to complete the installation. Manually update the application KEYSTORE table when the installation is complete.

To manually update the application KEYSTORE table:

1. Navigate to *NI_Home*/**POMSClient**.
2. Run the following command:

   ```
   jre_Path/bin/java -javaagent:lib/eclipselink.jar -cp POMSClient.jar
   oui.j2ee.poms.client.UpdateAppKeyStore DB_HostName DB_Port DB_ServiceName
   NI_Schema_UserName NI_Schema_Password default aes 128
   ```

   where:

   - *jre_Path* contains the **jre** folder inside the Java Development Kit (JDK) installation directory
   - *DB_HostName* is the database host name
   - *DB_Port* is the database port number
   - *DB_ServiceName* is the database service name or system ID

- *NI_Schema_UserName* is a valid Network Integrity database user name for the schema
- *NI_Schema_Password* is the password for the Network Integrity schema user name

3. Connect to the application KEYSTORE table and verify the following:
   - That the COMPONENT column has a value of **`default`**.
   - That the ENCRYPTALGORITHM column has a value of **`aes`**.
   - That the KEYLENGTH column has a value of **`128`**.
4. Restart Network Integrity for the changes to take effect, as explained in *Network Integrity System Administrator's Guide*.

Problem: Installer Fails to Update Application INFORMATION Table

If the installer fails to update the application INFORMATION table, the installer is interrupted and the following error message appears:

```
Unable to update application details 'ApplicationInfo', please check log files for more details. Refer to Network Integrity documentation for executing this step manually.
```

Solution

Click the **Continue** button to complete the installation. Manually update the application INFORMATION table when the installation is complete.

To manually update the application INFORMATION table:

1. Navigate to *NI_Home*/**POMSClient**.
2. Run the following command:

   ```
   jre_Path/bin/java -javaagent:lib/eclipselink.jar -cp POMSClient.jar
   oui.j2ee.poms.client.UpdateAppInfoTable DB_HostName DB_Port DB_ServiceName
   NI_Schema_UserName NI_Schema_Password "Network Integrity" NI_Version SUCCESS
   ```

   where:

   - *jre_Path* contains the **jre** folder inside the JDK installation directory
   - *DB_HostName* is the database host name
   - *DB_Port* is the database port number
   - *DB_ServiceName* is the database service name or system ID
   - *NI_Schema_UserName* is a valid Network Integrity database user name for the schema
   - *NI_Schema_Password* is the password for the Network Integrity schema user name
   - *NI_Version* is the version of Network Integrity being installed
3. Connect to the application INFORMATION table and verify the following:
   - That the NAME column has a value of **`Network Integrity`**.
   - That the VERSION column has the correct version of Network Integrity.
   - That the STATUS column has a value of **`SUCCESS`**.

Problem: Inability To Run Scans or Resolve Discrepancies After Upgrading

After upgrading Network Integrity, you may be unable to run scans or resolve discrepancies using cartridges if you have unmigrated cartridges still deployed to your system.

To confirm that you are experiencing this issue, verify the following:

- Network Integrity displays the following error messages when you try to run a scan:

  ```
  Unable to start scan, as cartridge is in the process of getting deployed or
  undeployed.
  ```

- Network Integrity displays the following error messages when you try to resolve discrepancies:

  ```
  All Plugins are not ready. Cartridge deploy or undeploy is in progress.
  ```

- The DisPlugin database table has the value **0** set for the pluginready attribute for some cartridges.

Solution

Resolve this issue by doing the following:

- Migrate all deployed, unmigrated cartridges that you are licensed and permitted to migrate.
- Run the **Troubleshoot_delete_unused_plugins_post_upgrade.sql** script to delete the remaining unmigrated cartridges from your system:
  1. In Network Integrity, delete all scan configurations related to unmigrated cartridges.
  2. From the command prompt, go to the *NI_Home***/integrity/upgrade/migration** directory.
  3. Enter the following command, to run the script as the Network Integrity MDS DB schema user, using sqlplus:

     ```
     Troubleshoot_delete_unused_plugins_post_upgrade.sql
     ```

  4. Follow the command-line prompts.

     The script deletes all cartridges from the system that have a pluginready value of **0** in the DisPlugin database table.

  5. Restart Network Integrity.
  6. Run a test scan to confirm that the issue is resolved.

Problem: Unable to Load Performance Pack

This procedure is only applicable if you are running WebLogic Server 10.3.6 on a Solaris platform with a 64-bit JVM.

There is a known issue that is encountered when starting the WebLogic server. Specifically, the 64-bit native libraries are not loaded correctly. To confirm that you have this issue, search the standard output log for the following error:

```
Unable to load performance pack
```

Solution

If you have this issue, do the following:

1. Back up and edit the *Domain_Home***/bin/setDomainEnv.sh** file.
2. Add the following lines to the end of the file:

```
LD_LIBRARY_PATH_64=${BEA_HOME}/wlserver_10.3/server/native/solaris/sparc64
export LD_LIBRARY_PATH_64
```

3. Save and close the file.

Problem: Application Server Takes a Long Time to Start

If the Network Integrity environment has McAfee AntiVirus software installed, the Application server takes a long time to start.

Solution

Add the *NI_Home*, *MW_Home*, and *WL_Home***/server/lib/***Java_Home* directories to the McAfee exclusion list so that these directories are excluded from being scanned.

where:

- *NI_Home* is the directory in which the Network Integrity software is installed.
- *MW_Home* is the directory in which the Oracle Fusion Middleware products, files, and folders are installed.
- *WL_Home* is the directory in which WebLogic Server is installed. *WL_Home* is located in *MW_Home*.
- *Java_Home* is the JDK installation directory.

Reporting Problems

Before calling Oracle Global Support, read the description of preparing to call Global Support in the Troubleshooting chapter in *Network Integrity System Administrator's Guide*.