Oracle® Communications Network Integrity

Installation Guide

Release 8.0
G34177-01
October 2025

Oracle Communications Network Integrity Installation Guide, Release 8.0

G34177-01

Contents

4 Installing and Configuring Oracle WebLogic Server

5 Installing and Configuring Additional Software

6 Installing Network Integrity

7 Network Integrity Post-Installation Tasks

About This Content

This guide provides instructions for installing Oracle Communications Network Integrity.

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.

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.

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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 NextGen Installer. The Installer installs the core application and configures connections with the components, according to the connection details you provide during installation.

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. 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 Fusion Middleware Infrastructure	14*c* (14.1.2.0.0)
Oracle Java SE Development Kit (JDK) for Linux	Java 21 with latest critical patch update

Table 2-2 (Cont.) Required Server-Side Software

Product	Version
Oracle Database Enterprise Edition	19*c* (19.25) or 23ai
Oracle Access Manager (OAM), included with Oracle Identity and Access Management	14*c* (14.1.2.0.0)

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 21 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	14*c* (14.1.2.0.0)

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" 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	8.2 Oracle Analytics Publisher is required to use the reporting templates included with Network Integrity.
Oracle Communications Unified Inventory Management (UIM)	NA
Oracle Communications MetaSolv Solution (MSS)	NA
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.

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)

Table 2-10 (Cont.) Network Integrity Hardware Planning Guideline

Product Cartridge	Network Domain	Protocol	NI Actions benchmarked	Network Resources
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)
Netconf_Network_Discovery_Cartridge	NETCONF	NETCONF	Discovery, Discrepancy Detection, Reconciliation, Import	Physical Network Resources (Node, Equipment, Slot, Card, Port and Interface)
Restconf_Network_Discovery_Cartridge	RESTCONF	RESTCONF	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
NETCONF	10k Devices	NI 4*4 OCPU and 128 GB RAM (4 MS each with 4 OCPUs and 32 GB RAM)	4 * VM.Standard3.Flex
RESTCONF	10k 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. • **Scenario 4:**Two scan for 10k chunk size for NETCONF domain covering 20k device. • **Scenario 5:**Two scan for 10k chunk size for RESTCONF domain covering 20k device. 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. • **Scenario 4:** Two scans for a 10k chunk size for NETCONF domain spanning 20k devices. • **Scenario 5:** Two scans for a 10k chunk size for RESTCONF domain spanning 20k devices.

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. • **Scenario 4:** Five scans for a 10k chunk size for NETCONF domain spanning 50k devices. • **Scenario 5:** Five scans for a 10k chunk size for RESTCONF domain spanning 50k 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. • **Scenario 4:** Seven scans for a 10k chunk size for NETCONF domain spanning 70k devices and one scan for a 5k chunk size of Optical domain spanning 5k devices. • **Scenario 5:** Seven scans for a 10k chunk size for RESTCONF domain spanning 70k devices and one scan for 5k chunk size of Optical domain spanning 5k 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. • **Scenario 4:** Twenty scans for a 10k chunk size for NETCONF domain covering 200k devices. • **Scenario 5:** Twenty scans for a 10k chunk size for RESTCONF domain covering 200k 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 Schema. 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:

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

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

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.
> - The Database server and the Application server must be in the same time zone.

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 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 the **Create Repository** option. Under this, choose **System Load and Product Load**, then click **Next**.

5. Do the following:

   a. From the **DatabaseType** list,select **Oracle Database enabled for edition-based redefinition**.

   b. For **Connection String Format**, select **Connection Parameters**.

   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**, **Common Infrastructure Services**, **Weblogic Services** 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**.

4

Installing and Configuring Oracle WebLogic Server

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

Installation and configuration tasks include:

About Java Requirements

Oracle WebLogic Server is a Java application and needs a Java environment 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 Oracle Fusion Middleware Infrastructure

Download Oracle Fusion Middleware Infrastructure from the Network Integrity software on the Oracle software delivery website:

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

For more information about installing Oracle Fusion Middleware Infrastructure, see the Oracle Fusion Middleware Infrastructure documentation.

Installing Patches for Oracle Fusion Middleware

After you install Oracle Fusion Middleware Infrastructure, you must install any applicable patches. See Required Software for information about patches for Oracle Fusion Middleware. Download the required patches from the My Oracle Support Web site: https://support.oracle.com

You need to apply patches using the OPatch tool. For more information about downloading and applying patches, see *Oracle Fusion Middleware Install, Patch and Upgrade* see the document:

https://docs.oracle.com/en/middleware/fusion-middleware/14.1.2/install-patch-tasks.html

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

https://docs.oracle.com/en/middleware/fusion-middleware/14.1.2/opatc/patching-opatch.pdf

Option 1: Creating a Standalone WebLogic Domain For Application Deployment

To create a standalone WebLogic domain:

> **Note**
>
> Oracle recommends using a cluster setup for production environments, as detailed in Option 2: Creating a Clustered WebLogic Domain For Application Deployment. You may use the following procedure for installing lab environments on standalone domain as per your preference.

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 - 14.1.2.0.0 [wlserver]** (This product is selected by default and you cannot deselect it.)
   - **Oracle Enterprise Manager - 14.1.2.0.0 [em]**
   - **Oracle JRF - 14.1.2.0.0 [oracle_common]**
   - **WebLogic Coherence Cluster Extension - 14.1.2.0.0 [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.

> **Note**
>
> The user name cannot contain spaces, commas, tabs, or any of the following special characters: <, >, #, ?, |, &, (,), {, or }.

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, re-enter your password.

9. Click **Next**.

   The Domain Mode and JDK screen appears.

10. In the Domain Mode section, select the **Production** option and uncheck **Disable Secure Mode**.

11. In **Enable or Disable Default Ports for Your Domain** section,

    - Select **Enable Listen Ports (non-SSL Ports)** and **Enable SSL Listen Ports** checkboxes.
    - Deselect **Enable Administration Port (SSL Port)** checkbox.

> **Note**
>
> While it is not mandatory, Oracle recommends enabling the SSL Listen Ports.

12. In the **JDK** section, click **Browse** and select the required JDK Version. See Required Software for information about JDK version requirements

13. Click **Next**.

    The Database Configuration Type screen appears.

14. 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 **Driver** field, selectthe driver used by the component schema.

    c. Select the **connection Parameters** option

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

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

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

    g. 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.

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

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

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

The Component Datasources screen appears.

15. Perform either one of the following steps:

a. **For single-instance database (Standard DB):** Verify the values in the fields and click **Next**.

The JDBC Test screen appears.

Continue with step 16.

b. **For Oracle Real Application Clusters (RAC) database:** Select the **Convert to RAC multi data source** option and click **Next**.
The Oracle RAC Multi Data Source Component Schema screen appears.

i. From the list of drivers, select the driver used by the component schema.

ii. In the **Service Name** field, enter the service name for the RAC database.

iii. In the **Host Name** field, enter the host name/IP address of the machine configured for RAC database.

iv. In the **Instance Name** field, enter the SID of the host.

v. In the **Port** field, enter the configured port of the host.

vi. Add additional hosts by clicking **Add Host** and repeat steps **iii** to **v** for each new RAC node instance to be added.

vii. Click **Next**.
The JDBC Test screen appears.

Continue with step 16.

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

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

The Advanced Configuration screen appears. For RAC, a connection result log appears.

18. Select the **Administration Server** services to install in the WebLogic Server domain.

19. Click **Next**.

The Administration Server screen appears.

20. 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.
>
> It is recommended to use DNS host name instead of the IP address during installation.

c. Select **Enable Listen Port** checkbox if you want to enable non-SSL Ports.

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

   This field is enabled only if you have selected the **Enable Listen Port** checkbox.

e. Select the **Enable SSL Listen Port** checkbox if you want to enable SSL Ports. It is recommended to enable SSL Ports.

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

   This field is enabled only if you have selected the **Enable SSL Listen Port** checkbox.

g. Leave the **Server Groups** list set to its default value, **Unspecified**.

h. Click **Next**.

   The Configuration Summary screen appears.

21. 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.

22. Click **Finish**.

    See Oracle Fusion Middleware documentation for more information.

23. Continue with the procedures in Starting the WebLogic Server.

Option 2: Creating a Clustered WebLogic Domain For Application Deployment

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.

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.

Example Server Cluster Details

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

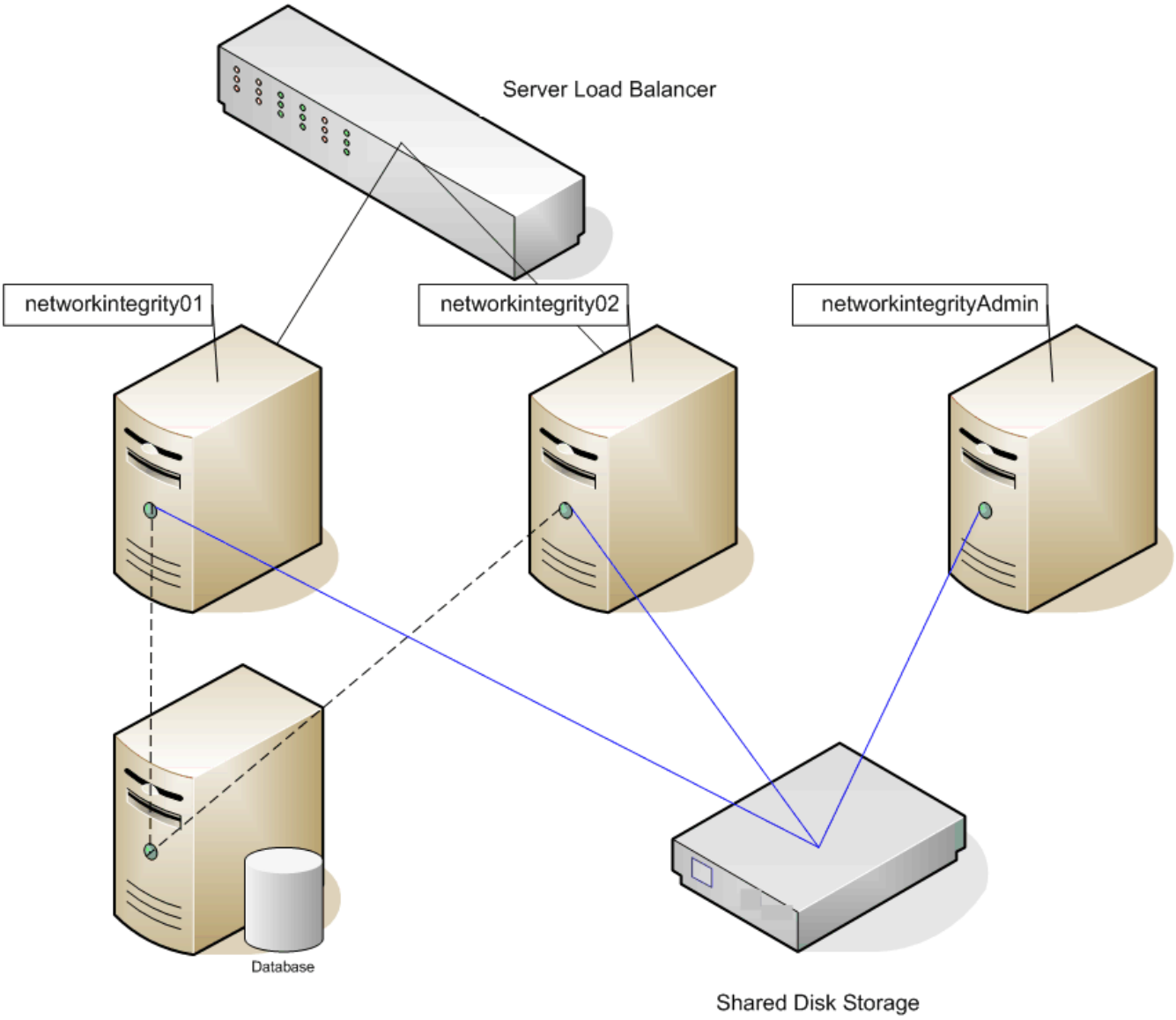
Value	Example
Domain_Home	*MW_Home*/**user_projects/domains/networkintegritycluster**
Domain login	weblogic
Domain password	networkintegritycluster1
Cluster DNS	NetworkIntegrityClusterDNS (It includes the networkintegrity01 and networkintegrity02 listening DNS_Hostname/IPAddress)

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	*DNS_Host1*/*IP1*:8063	*DNS_Host2*/*IP2*:8065	*DNS_Host3*/*IP3*:8066
Machine	NETINT1	NETINT2	NETINT3

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

Figure 4-1 Server Architecture Diagram



Network Integrity Server Cluster Prerequisites

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

- Oracle WebLogic administration experience.
- 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 Fusion Middleware Infrastructure on the shared disk storage.
- Creating Database (Metadata) Schema for Network Integrity
- Creating an instance of WebLogic server domain, and creating your cluster.
- Starting up the Administration Server and all cluster-managed servers.
- Installing and Configuring Additional Software (Optional)
- Installing Network Integrity on the cluster setup
- Performing post Installation Action Steps
- Configuring Load balancer to cluster setup
- Accessing Network Integrity through server load balancer URL

Creating a Clustered Domain

To create a clustered 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 - 14.1.2.0.0 [wlserver]** (This product is selected by default and you cannot deselect it.)
   - **Oracle Enterprise Manager - 14.1.2.0.0 [em]**
   - **Oracle JRF - 14.1.2.0.0 [oracle_common]**
   - **WebLogic Coherence Cluster Extension - 14.1.2.0.0 [wlserver]**
   - **Oracle WSM Policy Manager - 14.1.2 [oracle_common]**

> **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.

    Select the **Production** option and uncheck **Disable Secure Mode**.

11. In Enable or Disable Default Ports for Your Domain section,

    - Select the **Enable Listen Ports (non-SSL Ports)** and **Enable SSL Listen Ports** checkboxes.
    - Deselect the **Enable Administration Port (SSL Port)** checkbox.

    > **Note**
    >
    > While it is not mandatory, Oracle recommends enabling the SSL Listen Ports.

12. In the JDK section, select the required JDK Version. See Required Software for more information about the JDK version requirements

13. Click **Next**.

    The Database Configuration Type screen appears.

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

    c. Select **connection Parameters** option

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

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

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

g. 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.

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

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

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

The Component Datasource screen appears.

15. Perform any one of the following steps:

- **For single-instance database (Standard DB):** Verify the values in the fields and click **Next**.
  The JDBC Test screen appears.

  Continue with step 16.

- **For Oracle Real Application Clusters (RAC) database:** Select the **Convert to RAC multi data source** option and click **Next**.
  The Oracle RAC Multi Data Source Component Schema screen appears.

  a. From the list of drivers, select the driver used by the component schema.

  b. In the **Service Name** field, enter the service name for the RAC database.

  c. In the **Host Name** field, enter the host name/IP address of the machine configured for RAC database.

  d. In the **Instance Name** field, enter the SID of the host.

  e. In the **Port** field, enter the configured port of the host.

  f. Add additional RAC database nodes by clicking **Add Host** and repeat steps from **c** to **e** for each new RAC node instance to be added.

  g. Click **Next**.
  The JDBC Test screen appears.

  Continue with step 16.

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

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

The Advanced Configuration screen appears.

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

- **Administration Server**
- **Topology**
- **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, if desired.

19. Click **Next**.

    The Administration Server screen appears.

20. 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**
       >
       > It is recommended to use the DNS host name instead of the IP address during installation.

    c. Select **Enable Listen Port** checkbox to enable non-SSL Ports.

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

       This field is enabled only if you selected the **Enable Listen Port** checkbox.

    e. Select the **Enable SSL Listen Port** checkbox if you want to enable SSL.

       It is recommended to enable SSL Listen Ports.

    f. 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** checkbox.

    g. Click **Next**.

       The Managed Servers screen appears.

21. 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** checkbox if you want to enable SSL.

       It is recommended to use SSL ports.

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.

22. 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 Server Templates screen appears.

23. Accept the default settings, then click **Next**.

    The Dynamic Servers screen appears.

24. Accept the default settings, then click **Next**.

    The Assign Servers to Clusters screen appears.

25. Assign the servers to the cluster by moving the managed servers in the left pane to the required cluster in the right pane.

26. 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.

27. 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.

28. Click **Next**.

    The Machines screen appears.

29. Accept the default settings, then click **Next**.

    The Deployments Targeting screen appears.

30. Click **Next**.

    The Services Targeting screen appears.

31. Under **Targets**, select **AppDeployment** and **wsm-pm**, then move them to the right side under AppDeployment under AdminServer.

32. Under **Targets**, select **Library**, then move them to the cluster node on the right side.

33. Click Next.

The Services Targeting screen appears.

Under services, select **JDBCSystemResource**, **ShutdownClass**, **StartupClass** and **WLDFSystemResource**, then move them to the cluster node on right side.

34. Click **Next**.

    The Configuration Summary screen appears.

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

> **Note**
>
> The warning message that appears (CFGFWK-40318) can be ignored.

    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.

36. Click **Finish**.

    See Oracle Fusion Middleware documentation for more information.

37. Continue with the procedures in Starting the WebLogic Server.

38. Continue with the procedures in Starting the Cluster Member Servers.

    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 Admin server.

3. 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
```

4. Alternately, verify that the server has started by logging in to the WebLogic Remote console or checking the log files.

   a. **To access the WebLogic server administration console:** Use WebLogic Remote Console application. For WebLogic Remote Console Installation and Usage, see this website: https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-remote-console/

> **Note**
>
> Starting with Oracle Fusion Middleware 14*c*, direct access to the Oracle WebLogic Server Administration Console via the traditional console URL is no longer supported. Instead, administrators should use the WebLogic Remote Console to manage and administer Oracle WebLogic Server.

b. Once connected with theWebLogic server administration console using WebLogic Remote Console application, in the Edit tree, expand **Environment**, and click **Servers**. The Summary of Servers screen appears.

5. Check if the server's **State** displays RUNNING. If it is not in RUNNING, you may need to wait for a short period and refresh the page.

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 managed 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. Look at the bottom of the managed Server command window. The command window should contain the following lines:

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

5. Alternately, verify that the server has started by logging in to the WebLogic Remote console or by checking the log files.

   a. To access the WebLogic server administration console: Use WebLogic Remote Console application. For more information on the WebLogic Remote Console installation and usage, see this website: https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-remote-console/

> **Note**
>
> For Oracle Fusion Middleware 14*c*, direct access to the Oracle WebLogic Server Administration Console via the traditional console URL is no longer supported. Instead, administrators should use the WebLogic Remote Console to manage and administer Oracle WebLogic Server.

b. Once connected with theWebLogic server administration console using WebLogic Remote Console application, in the Edit tree, expand **Environment**, and click on **Servers**.
The Summary of Servers screen appears.

c. Check if the server's **State** displays RUNNING. If the **State** is not in RUNNING, you may need to wait for a short period and refresh the page.

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 8.0. 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

Methods to Install Network Integrity

Network Integrity installation can be performed in two ways:

- **Installation in Interactive Mode**. See "Installing Network Integrity Using Interactive Install" for more information.
- **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 schema 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 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 Network Integrity Installer software from the Oracle software delivery website:

   `https://edelivery.oracle.com`

and save it to *dir*:

3. Export JDK Home by running one of the following command. See Software Requirements for JDK version information.

   ```
   export JAVA_HOME=$JDK_HOME
   ```

4. Run the Oracle Nextgen Network Integrity Installer using the following command:

   ```
   java -jar NetworkIntegrityInstaller_{release}.jar
   ```

   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 Installation Location Screen appears appears. Continue with step 7.

7. In **NI_Home** field, enter or browse the path to the folder where you want to install Network Integrity and click **Next**.

   The Installation Type Screen appears.

8. Select **Complete** and click **Next**.

   The WebLogic Administration Server Connection Information screen appears.

9. 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** checkbox based on your business need.

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

> **Note**
>
> You can configure an SSL certificate based on any specific requirements. If necessary, you can create a custom certificate and apply it to your domain before installing Network Integrity. For more information, see "Configuring the SSL Policy and SSL Certificate" section in *Network Integrity System Administrator's Guide*.

g. Click **Next**.

The Target Selection screen appears.

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

The DB Type Selection Page appears.

> **Note**
>
> If you select a managed server, ensure that all the managed servers are running.

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

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

  The Standard DB Connection 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 of the database **SYSDBA** User.

  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 Intgrity Schema Table Creation screen appears.

- Select the **Oracle 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 **SYSDBA** user.

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

d. Click **Next**.

The NI Schema Table Creation screen appears.

12. Select **Yes** Option and click Next.
The MDS Schema User Connection screen appears.

13. In MDS Schema User Connection, 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.

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

- If you select **Embedded_LDAP** option,the Admin User Creation screenappears.

  Do the following (Optional):

  a. In the **UserName** 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 password requirements for the Network Integrity user is as follows:
>
> – Password length must be between 8 to 12 characters.
> – It should contain at least one uppercase letter, one lowercase letter, one number and one special character.
> – It must not contain the username either directly or in reverse
> – You may use a character 3 times in a row maximum, but not more than 4 times in total.

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

c. Click **Next**.

The Internal user Creation 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 Internal user Creation screen appears.

- If you select **Other Security Provider**, and click **Next**.

  The Disable unsecured Port screen appears.

  Skip to step 16.

15. In the Internal user Creation, do the following:

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

> **Note**
>
> The password requirements for the Network Integrity internal user is as follows:
>
> - Password length must be between 8 to 12 characters.
> - It should contain at least one uppercase letter, one lowercase letter, one number and one special character.
> - It must not contain the username either directly or in reverse
> - You may use a character 3 times in a row maximum, but not more than 4 times in total.

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

b. Click **Next**.

The Disable Unsecured Listen Port screen appears.

16. Select whether 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 only by disabling Non-SSL Ports.
    - Select **No** if you are not configuring Network Integrity to communicate and listen over both SSL and Non-SSL ports.
17. Click **Next**.

    The Java Home Location screen appears.
18. Accept the default settings, then click **Next**.

    The Installation Summary screen appears.
19. Review the content in the summary and click **Next**.

    The Installation Progress Screen appears.
20. 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.

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

21. Click **Exit** to close the Installation Wizard.
22. 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**
23. To start the server, do the following:

a. To start the AdminServer, use the following command:

```
./startNI.sh
```

b. To startt the managed servers, use 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".

After verifying the successful installation, perform the required post-installation actions. See Network Integrity Post-Installation Tasks for more information.

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 **oracle.communications.integrity.rsp** response file template comes as part of the Network Integrity installation package.

The response file templates contain all the fields that the installer requires performing installation in silent mode.

When you extract the installer JAR file, the response file templates are saved in the Response directory at the following location: **Disk1/storage/Response**.

Table 6-1 presents the Network Integrity response file template properties, along with the values that should be specified for a complete installation scenario.

> **Note**
>
> Before using the response file, ensure that any optional properties or values not required by the installer are left empty.

Table 6-1 Network Integrity Response File Template Properties

Response File Template Name	Property Name	Description (with Default Values)
Installation Location Details (Required)	ORACLE_HOME	Directory path where the NI application will be installed.
Installation Type Details (Required)	INSTALLATION_TYPE	Type of installation (Allowed values: **Complete** or **Upgrade**). Set to "**Complete**" for a fresh installation.
WebLogic Admin Server Connection Details (Required)	APP_ADMIN_HOST	Host name or IP address of the WebLogic Admin Server.

Table 6-1 (Cont.) Network Integrity Response File Template Properties

Response File Template Name	Property Name	Description (with Default Values)
WebLogic Admin Server Connection Details (Required)	APP_ADMIN_PORT	Port number for the WebLogic Admin Server (values provided must be enclosed in double quotes). For SSL-based deployment, provide the SSL port value and specify the keystore file location in the APP_SERVER_KEYSTORE property.
WebLogic Admin Server Connection Details (Required)	APP_SERVER_USER	Username for the WebLogic Admin Server.
WebLogic Admin Server Connection Details (Required)	APP_SERVER_PASSWD	Password for the WebLogic Admin Server.
WebLogic Admin Server Connection Details (Required)	APP_SERVER_KEYSTORE	Path to the keystore file required for SSL-based deployment. Example:, certs/Keystore.jks
Target Selection Details (Required)	APP_TARGET_NAME	Name of the target (such as AdminServer or CL1) where the NI application will be installed.
Database Selection Details (Required)	DATABASE_TYPE	Type of database used. Accepted values: **Standard Oracle Enterprise Database** or **Oracle Real Application Cluster Database**
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_HOST_NAME	Host name of the standard Oracle database.
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_HOST_PORT	Port number of the standard Oracle database (enclose in double quotes).
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_USER_NAME	Username with SYSDBA privileges for the standard Oracle database.
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_PASSWORD	Password for the SYSDBA user of the standard Oracle database.
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_SERVER_SERVICE	Service name of the standard Oracle database.
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_CONNECTION_STRING	Connection string details for Oracle RAC in the format: HostName1:Port1:Service1,Host Name2:Port2:Service2

Table 6-1 (Cont.) Network Integrity Response File Template Properties

Response File Template Name	Property Name	Description (with Default Values)
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_SERVER_USER	Username for connecting to the Oracle RAC database
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_SERVER_PASSWORD	Password for the Oracle RAC database server.
NI Schema Table Creation (Required only if INSTALLATION_TYPE=Complete)	DB_SCHEMA	Flag to indicate whether to create the app schema table Allowed values: “**true**” or “**false**”). For fresh installation, provide “**true**”.
MDS Schema Information Details (Required)	SCHEMA_OWNER_NAME	Username for the MDS (Metadata Services) schema created using RCU utility.
MDS Schema Information Details (Required)	SCHEMA_OWNER_PASSWD	Password for the MDS (Metadata Services) schema user.
Security Provider Selection Details	SECURITY_PROVIDER_NAME	Type of security provider to select. Allowed values: **Embedded_LDAP** or **External_LDAP**
Embedded LDAP Details (User creation is optional; values can be left empty even if SECURITY_PROVIDER_NAME is set to Embedded LDAP)	LDAP_USER_NAME	Username to be created in the embedded LDAP directory.
Embedded LDAP Details (User creation is optional; values can be left empty even if SECURITY_PROVIDER_NAME is set to Embedded LDAP)	LDAP_PASSWD	Password for the newly embedded LDAP user. **Note:** The password requirements are as follows. • Password length must be between 8 to 12 characters. • It should contain at least one uppercase letter, one lowercase letter, one number and one special character. • It must not contain username directly or in reverse. • You may use a character 3 times in a row maximum, but not more than 4 times in total.
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_HOST	Host name of the external LDAP server.
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_PORT	Port number of the external LDAP server.

Table 6-1 (Cont.) Network Integrity Response File Template Properties

Response File Template Name	Property Name	Description (with Default Values)
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_USER	Username for connecting to the external LDAP server.
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_PASSWORD	Password for the external LDAP server user.
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_USER_BASE_DN	User BASE DN information of external LDAP server.
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_GROUP_BASE_DN	Group BASE DN information of external LDAP server.
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_KEYSTORE	Path to the keystore file for the external LDAP server (e.g., certs/externalLDAPKeystore.jks).
NI Internal user Details (Required)	LDAP_DEF_USER_PASSWD	Password for the NI internal user. **Note:** The password requirements are as follows. • Password length must be between 8 to 12 characters. • It should contain at least one uppercase letter, one lowercase letter, one number and one special character. • It must not contain username directly or in reverse. • You may use a character 3 times in a row maximum, but not more than 4 times in total.
Disable Non-SSL Port Option (Required)	DISABLE_NONSSLPORT	Option to disable the non-SSL port (Allowed Values: set to "**true**" to disable, or "**false**" to keep enabled).

Note

- Before using the response file, ensure that any optional properties or values not required by the installer are left empty.
- You can configure an SSL certificate based on any specific requirements. If necessary, you can create a custom certificate and apply it to your domain before installing Network Integrity. For more information, see "Configuring the SSL Policy and SSL Certificate" section in *Network Integrity System Administrator's Guide*.

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. Export JDK Home by running one of the following command, See Software Requirements for JDK version information:

   ```
   export JAVA_HOME=$JDK_HOME
   ```

2. Use the following command to start the silent installer,here absolute_*path* is the fully qualified response file location:

   ```
   java -jar NetworkIntegrityInstaller_{release}.jar -responseFile
   {absolute_path}
   ```

   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.

3. At the end of the installation, the command window displays the location of the installer log files. Users can review these logs located at **oraInventory/logs** to verify that the installation was successful.
4. Start the AdminServer, using the following command:

   ```
   ./startNI.sh
   ```

5. Start the managed servers, using the following command:

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

6. 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**

7. 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".

After verifying a successful installation, perform the required post-installation actions. See Network Integrity Post-Installation Tasks for more information.

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:

- Configuring Proxy Server
- Managing Network Integrity Cartridges
- Configuring Network Integrity for Inventory Management
- Installing Network Integrity Report Templates
- Enabling HTTP Tunneling
- Setting Up Oracle Internet Directory
- Configuring the WebLogic Server StuckThreadMaxTime Value
- Setting Memory Requirements for Network Integrity

Configuring Proxy Server

You may select and configure a proxy server according to your specific requirements. By default, Network Integrity supports Oracle HTTP Server (OHS). For more information on setting up OHS as a proxy server, see Configuring Oracle HTTP Server as Proxy.

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**.

   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.
6. Enable **Ignore dependency check failures for all Cartridges**.

> **Note**
>
> Before deploying the selected cartridge, ensure that all dependent cartridges have been successfully deployed to the environment. If the dependent cartridges are not deployed, the selected cartridge deployment may fail.

7. Verify the default selections and click **Next**.

> **Note**
>
> On the WebLogic Connection Information screen, if the **Use SSL** checkbox is selected and the "SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the bottom of this screen" error message appears, it indicates that SSL is not properly configured for the environment.
> To proceed without SSL:
>
> a. Click **OK** on the error message dialog.
>
> b. Deselect the **Use SSL** checkbox at the bottom of the screen.

8. 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.

9. 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.

10. Verify the default selections and click **Next**.

> **Note**
>
> On the WebLogic Connection Information screen, if the **Use SSL** checkbox is selected and the "SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the bottom of this screen" error message appears, it indicates that SSL is not properly configured for the environment.
> To proceed without SSL:
>
> a. Click **OK** on the error message dialog.
>
> b. Deselect the **Use SSL** checkbox at the bottom of the screen.

11. Click **Next**.

The Review Deployment screen appears.

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

The Cartridge Deployment screen appears that shows the deployment progress. A message appears upon successful deployment.

> **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. Verify the default selections and click **Next**.

> **Note**
>
> On the **WebLogic Connection Information** screen, if the **Use SSL** checkbox is selected and you receive the error message `SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the bottom of this screen.`, it means that SSL is not properly set up in the environment.

7. (Optional) To proceed without SSL:
   a. Click **OK** on the error message dialog.
   b. Clear the **Use SSL** checkbox at the bottom of the screen.
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 and a message after the cartridge is undeployed. 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 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 3; otherwise, proceed to step 4.
2. For proxy server:
   a. Log in to the WebLogic console and go to **Edit Tree**.
   b. Select the required cluster from **Clusters** under **Environments**.
   c. Go to **HTTP Tab** and remove the front-end host and port details.
   d. Restart the servers.
3. (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.
4. Deploy the required cartridges.
5. After you have deployed the cartridges, configure the front-end host and port details for the cluster in the console.
6. Restart all 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. Verify the default selections and click **Next**.

> **Note**
>
> On the **WebLogic Connection Information** screen, if the **Use SSL** checkbox is selected and you receive the error message `SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the bottom of this screen.`, it means that SSL is not properly set up in the environment.

7. (Optional) To proceed without SSL:
   a. Click **OK** on the error message dialog.
   b. Clear the **Use SSL** checkbox at the bottom of the screen.
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.
-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.

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

To set up Oracle Internet Directory:

> **Note**
>
> If you want to use Oracle Internet Directory, you must first complete all prerequisite steps outlined in the Installing and Configuring Additional Software. After doing so, you can proceed with the following post-installation steps.

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.

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.

Setting Memory Requirements for Network Integrity

To ensure that Network Integrity scans run successfully, you must configure appropriate memory settings in the WebLogic Server. Network Integrity may require different JVM heap sizes depending on the production volume processed by each scan.

To do so:

1. In the WebLogic domain’s bin directory, open the **startNI.sh** file.
2. Set the JVM memory arguments as required. For example,

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

   This configures the JVM to use 20 GB of memory as both the minimum and maximum heap size.

> **Note**
>
> See "Hardware Sizing Considerations" to determine the appropriate memory allocation for your JVM based on your specific requirements.

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
   - 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 2-3 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 direct upgrades to version 8.0 from releases 7.3.6.3, 7.3.6.4, 7.4, and 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 Oracle Fusion Middleware and apply applicable patches.

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

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 NextGen 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

Network Integrity supports two upgrade approaches from release 8.0:

- In-Place Upgrade
- Blue Green Upgrade

In-Place Upgrade

This section describes the procedures to upgrade Network Integrity to release 8.0 from the following versions:

- Release 7.3.6.3
- Release 7.3.6.4
- Release 7.4
- Release 7.5

The In-Place upgrade involves the following tasks:

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

> **Note**
>
> If you are using **Fusion Middleware Infrastructure 12.2.1.3**, you must first upgrade to **12.2.1.4** before proceeding with these steps.
>
> See Oracle Fusion Middleware documentation for more information.
>
> In addition, ensure that your database is on Oracle Database 19c (19.26) or Oracle Database 23ai.
>
> See Software Requirements for more information on software versions.

Pre-Upgrade Tasks

This section provides the pre-upgrade tasks to be performed for the In-Place upgrade method.

Perform all the following 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. For more information, see the WebLogic Server documentation.

> **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. 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 longer want to use.

> **Warning**
>
> After you upgrade Network Integrity, you cannot undeploy a non-migrated cartridge. If you do not undeploy cartridges that cannot be migrated or are not migrated, Network Integrity does not function.

   For more information, see Problem: Inability To Run Scans or Resolve Discrepancies After Upgrading.
4. Undeploy the cartridges to avoid any old scan names after the upgrade. Perform this step only if you are upgrading from an environment earlier than 7.4.0.
5. If your version of Network Integrity is 7.3.6.3 or below, perform the following steps before starting the upgrade.
   a. Stop all managed servers except the Administration Server.
   b. Undeploy **snmpAdapter** from the WebLogic Administration Console
   c. Restart all managed servers.
6. Install the Fusion Middleware Infrastructure and apply any required patches.
   See Software Requirements for version information regarding Fusion Middleware Infrastructure and any applicable patches.
7. Before upgrading the WebLogic domain, Update the existing **WLSSchemaDataSource** as follows:

> **Note**
>
> Perform this step only if you are upgrading your WebLogic domain from version 12*c* to 14*c*. If your WebLogic domain is already running on 14*c*, proceed directly to step 8.

   a. Log in to the WebLogic Administration Console.
   b. In the left navigation pane, expand **Services** and click **Data Sources**.
   c. On the Data Sources page, proceed based on your database type:
      i. **Standard database:** Select WLSSchemaDataSource and continue with step d.
      ii. **RAC database:** Select each WLSSchemaDataSource RAC node individually, such as WLSSchemaDataSource-rac0, WLSSchemaDataSource-rac1 and perform steps d and e for each node.

d. On the Configuration tab, select the Connection Pool sub-tab.

e. In the Properties section, update the User value from <PREFIX>_WLS_RUNTIME to <PREFIX>_WLS.

8. Shutdown all WebLogic servers before performing the following pre-upgrade steps.

9. Upgrade the database schemas:

a. Navigate to *MW_HOME*/**oracle_common/upgrade/bin/ua**
where*MW_HOME* is the directory in which Oracle Fusion Middleware 14c 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 Upgrade Type screen appears.

d. On the **Upgrade Type** screen, select **Individually Selected Schemas**, and click **Next**.

e. The **Available Components** screen appears which lists the available components that can be upgraded.

f. Select the below components and click **Next**.

```
Common Infrastructure Services
Oracle Audit Services
Oracle Metadata Services
Oracle Platform Security Services
Oracle WebLogic Server
```

The Domain Directory screen appears.

g. Select the existing WebLogic domain directory that needs to be upgraded and click **Next.**

The Prerequisites screen appears.

h. Confirm that the database backup is complete by selecting the following checkboxes:

- **All affected servers are down**
- **All affected data is backed up**
- **Database version is certified by Oracle for Fusion Middleware upgrade**
- **Certification and system requirements have been met**

i. Click **Next**.

The OPSS Schema screen appears.

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

k. In the **Database Connect String** field, enter the *hostname:portnumber/ServiceName* string.

> **Note**
>
> For a RAC database, provide RAC Server DB Information, in the following format: *hostname*:*portnumber/ServiceName*

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

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

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

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

p. In **Schema Password** field, enter the schema password, and click **Next**.

q. Repeat the same procedure for all remaining schemas (for example, MDS, IAU, STB, WLS, etc.) until all schema credentials are provided and click **Next.**
The Examine screen appears.

r. Verify that all listed schemas show the status as **ready for upgrade**, and then click **Next.**
The Upgrade Summary screen appears.

s. Verify the details of the schemas to be upgraded and click **Upgrade**.
The Upgrading Progress screen appears. You can monitor the progress of the upgrade from this screen.

t. After the upgrade completes, click **Next**.
The Upgrade Success screen appears.

u. Verify that the upgrade was successful and click **Close**.
For more information on upgrading schemas (using the Upgrade Assistant), see Oracle Fusion Middleware documentation.

10. Reconfigure the WebLogic domain configurations using the Fusion Middleware Reconfiguration Wizard.

a. Run the `reconfig.sh` script located in: *MW_HOME***/oracle_common/common/bin/reconfig.sh**, where *MW_HOME* is the directory in which Oracle Fusion Middleware 14c is installed.

b. 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.

c. Click **Next**.
The Reconfig Summary screen appears.

d. Click **Next.**
The Domain Mode and JDK screen appears. The domain mode cannot be changed during reconfiguration. It is inherited from the existing WebLogic domain that is being upgraded.

e. Select the **JDK** option and select the folder (*JAVA_HOME*) where the JDK is installed. Then, click **Next**.
Ensure that you have installed the correct version of the JDK. See Software Requirements for more information.

f. The JDBC Data Sources screen appears. Click **Next.**

g. The JDBC Data Sources Test screen appears. Click **Next.**

h. The Database Configuration Type screen appears.
Details are automatically retrieved from the existing WebLogic domain being upgraded.

Verify the information, click **Get RCU Configuration** to confirm, and then click **Next**.

i. The JDBC Component Schema screen appears.

i. For single-instance database (Standard DB): Verify the values in the fields and click Next, the JDBC Test screen appears. Continue with step j.

ii. For Oracle Real Application Clusters (RAC) database:

   i. Select the check box left to Component Schema.

   ii. Select the **Convert to RAC multi data source** option.

   iii. Click **Next.**
   The Oracle RAC Multi Data Source Component Schema screen appears.

   iv. Verify the details retrieved.

   v. In the **Host Name** field, enter the host name/IP address of the RAC database node.

   vi. In the **Instance Name** field, enter the instance name of the RAC database node.

   vii. In the **Port** field, enter the listener port of the RAC database node.

   viii. Add additional RAC database nodes by clicking **Add Host** and providing their details.

   ix. Click **Next**.
   The JDBC Test screen appears. Continue with step j.

j. Verify that all the JDBC component connections pass the validation test and click **Next**.
The Advanced Configuration screen appears.

k. On the **Advanced Configuration** screen:

   i. If upgrading a standalone environment, select **Administration Server** only.

   ii. If upgrading a clustered environment, select the following options.

   - **Administration Server**
   - **Topology**
   - **Deployments and Services**

l. Click **Next**.
The Administration Server screen appears.

m. The details are automatically fetched from the existing WebLogic domain that is being upgraded, Review the values, and click **Next.**
If upgrading a standalone environment continue with q.

n. Continue navigating through the subsequent screens, reviewing the details on each. Click **Next** to proceed, updating settings only if necessary.

o. On the Deployments Targeting screen, the existing configuration is displayed.

> **Note**
>
> In a clustered environment, ensure that NICMWSAdapter, cartridge_management_ws are present only on the first managed server.

Review the details and click **Next**.

p. The Services Targeting screen appears. The existing configuration is displayed. Review the details and click **Next**.

q. The Configuration Summary screen appears.

r. 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 is completed, click **Next.**

s. The End of Configuration screen appears. Click**Finish**.
For more information on reconfiguring the domain, see Oracle Fusion Middleware documentation.

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

a. Navigate to the *MW_Home***/oracle_common/upgrade/bin/ua**directory.
where *MW_Home* is the directory in which Oracle Fusion Middleware 14c is installed.

This directory contains the Fusion Middleware Upgrade Assistant which is used to upgrade the WebLogic domain configurations.

b. Launch the Fusion Middleware Upgrade Assistant.
The Welcome screen appears.

c. Click **Next**.
The Upgrade Type screen appears.

d. Select **All Configurations used by a domain**.
In the **Domain Directory** field, select the WebLogic domain directory you want to upgrade, and then click **Next**.

e. The Component List screen appears, click **Next**.
The Prerequisites screen appears.

f. Select all the checkboxes, click **Next.**

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

h. On the Upgrade Success screen, verify that the upgrade was successful and click **Close**.
For more information on upgrading domain component configurations, see Oracle Fusion Middleware documentation.

12. 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.

Upgrading Network Integrity

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

In-Place Upgrade Using Interactive Install

To upgrade Network Integrity using the In-Place upgrade method:

1. Create a directory (*dir*)for a temporary installation directory.
2. Download the Network Integrity Installer software from the Oracle software delivery website: https://edelivery.oracle.com
   and save it to *dir*:
3. Export JDK Home by running the following command, See Software Requirements for JDK version information:

   ```
   export JAVA_HOME=$JDK_HOME
   ```

4. Run the Oracle Nextgen Network Integrity Installer using the following command:

   ```
   java -jar NetworkIntegrityInstaller_{release}.jar
   ```

   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 Installation Location 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 Installation Location Screen appears. Continue with step 7.
7. In **NI_Home** field, enter or browse the path to the folder where you previously installed the old release of Network Integrity. And click Next.
8. The Installation Type Screen appears. Select **upgrade**, click **Next**.
   The WebLogic admin server connection screen appears.
9. The Installer retrieves information about your old Network Integrity installation, such as connection details and usernames.
10. Verify the WebLogic Administration Server connection information, enter the **WebLogic Server password**, and click **Next**.
    The Target Selection screen appears.
11. Select the target WebLogic server or cluster where you want to upgrade Network Integrity and click **Next.**
    The DB Type Selection screen appears.
12. 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 Enterprise Database,** and click **Next**.
      The Standard DB Connection 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 Real Application Cluster Database**, and click **Next**.
  The RAC DB Connection 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 MDS Schema User Connection screen appears.

13. 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 Disable Unsecured Port screen appears.
14. Select whether 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 only, by disabling Non-SSL Ports.
    - Select **No** if you are configuring Network Integrity to communicate and listen over both SSL and Non-SSL ports.
15. The Java Home Location Screen appears, Verify the java home path and click Next.
    The Installation Summary screen appears.
16. Review the details and click **Install**.
17. The Install Progress screen appears, showing the status of the upgrade installation. When the installer completes the upgrade, click **Next**.
18. The Installation Complete 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. In the Installer, click **Finish**.

In-Place Upgrade Using Silent Mode

You can use the silent install mode when you are upgrading Network Integrity using the same configuration repeatedly. The silent install mode does not use the GUI and 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 upgrade Network Integrity in silent mode.

The following response file templates come as part of the Network Integrity installation package: **oracle.communications.integrity.rsp**

The response file templates contain all the fields that the installer requires to perform upgrade in silent mode

When you extract the installer JAR file, the response file templates are saved in the **Response** directory at the following location: **Disk1/stage/Response**.

describes the Network Integrity response file template properties, along with the values that should be specified for a complete upgrade scenario.

Table 9-1 Network Integrity Response File Template Properties

Response File Template Name	Property Name	Description (with Default Values)
Installation Location Details (Required)	ORACLE_HOME	Directory path where the NI application will be installed.
Installation Type Details (Required)	INSTALLATION_TYPE	Type of installation (Allowed values: **Complete** or **Upgrade**). Set to "**Upgrade**" for an In-Place upgrade.
WebLogic Admin Server Connection Details (Required)	APP_ADMIN_HOST	Host name or IP address of the WebLogic Admin Server.
WebLogic Admin Server Connection Details (Required)	APP_ADMIN_PORT	Port number for the WebLogic Admin Server (values provided must be enclosed in double quotes). For SSL-based deployment, provide the SSL port value and specify the keystore file location in the APP_SERVER_KEYSTORE property.
WebLogic Admin Server Connection Details (Required)	APP_SERVER_USER	Username for the WebLogic Admin Server.
WebLogic Admin Server Connection Details (Required)	APP_SERVER_PASSWD	Password for the WebLogic Admin Server.
WebLogic Admin Server Connection Details (Required)	APP_SERVER_KEYSTORE	Path to the keystore file required for SSL-based deployment. Example:, certs/Keystore.jks
Target Selection Details (Required)	APP_TARGET_NAME	Name of the target (such as AdminServer or CL1) where the NI application was previously installed and will be upgraded.
Database Selection Details (Required)	DATABASE_TYPE	Type of database used. Accepted values: **Standard Oracle Enterprise Database** or **Oracle Real Application Cluster Database** Use the same type that you used in the production environment.
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_HOST_NAME	Host name of the standard Oracle database.
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_HOST_PORT	Port number of the standard Oracle database (enclose in double quotes).

Table 9-1 (Cont.) Network Integrity Response File Template Properties

Response File Template Name	Property Name	Description (with Default Values)
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_USER_NAME	Username with SYSDBA privileges for the standard Oracle database.
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_PASSWORD	Password for the SYSDBA user of the standard Oracle database.
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_SERVER_SERVICE	Service name of the standard Oracle database.
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_CONNECTION_STRING	Connection string details for Oracle RAC in the format: HostName1:Port1:Service1,Host Name2:Port2:Service2
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_SERVER_USER	Username for connecting to the Oracle RAC database
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_SERVER_PASSWORD	Password for the Oracle RAC database server.
NI Schema Table Creation (Not Required). For the In-Place upgrade, do not enter any value.	DB_SCHEMA	Flag to indicate whether to create the app schema table Allowed values: “**true**” or “**false**”).
MDS Schema Information Details (Required)	SCHEMA_OWNER_NAME	Username for the MDS (Metadata Services) schema user. **Note**: These details are related to the upgraded MDS schema.
MDS Schema Information Details (Required)	SCHEMA_OWNER_PASSWD	Password for the MDS (Metadata Services) schema user. **Note**: These details are related to the upgraded MDS schema.
Security Provider Selection Details (Not Required). For the In-Place upgrade, do not enter any value.	SECURITY_PROVIDER_NAME	Type of security provider to select. Allowed values: **Embedded_LDAP** or **External_LDAP**
Embedded LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_USER_NAME	Username to be created in the embedded LDAP directory.

Table 9-1 (Cont.) Network Integrity Response File Template Properties

Response File Template Name	Property Name	Description (with Default Values)
Embedded LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_PASSWD	Password for the newly embedded LDAP user. **Note:** The password requirements are as follows. • Password length must be between 8 to 12 characters. • It should contain at least one uppercase letter, one lowercase letter, one number and one special character. • It must not contain username directly or in reverse. • You may use a character 3 times in a row maximum, but not more than 4 times in total.
External LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_SERVER_HOST	Host name of the external LDAP server.
External LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_SERVER_PORT	Port number of the external LDAP server.
External LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_SERVER_USER	Username for connecting to the external LDAP server.
External LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_SERVER_PASSWORD	Password for the external LDAP server user.
External LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_USER_BASE_DN	User BASE DN information of external LDAP server.
External LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_GROUP_BASE_DN	Group BASE DN information of external LDAP server.
External LDAP Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_SERVER_KEYSTORE	Path to the keystore file for the external LDAP server (for example, certs/externalLDAPKeystore.jks).

Table 9-1 (Cont.) Network Integrity Response File Template Properties

Response File Template Name	Property Name	Description (with Default Values)
NI Internal user Details (Not Required). For the In-Place upgrade, do not enter any value.	LDAP_DEF_USER_PASSWD	Password for the NI internal user. **Note:** The password requirements are as follows. • Password length must be between 8 to 12 characters. • It should contain at least one uppercase letter, one lowercase letter, one number and one special character. • It must not contain username directly or in reverse. • You may use a character 3 times in a row maximum, but not more than 4 times in total.
Disable Non-SSL Port Option (Required)	DISABLE_NONSSLPORT	Option to disable the non-SSL port (Allowed Values: set to "**true**" to disable, or "**false**" to keep enabled).

Before using the response file, ensure that any optional properties or values that are not required by the installer are left empty.

Starting Silent Mode Installation

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

To upgrade Network Integrity in silent mode using In-Place Upgrade:

1. Export JDK Home by running one of the following command, See Software Requirements for JDK version information:

   ```
   export JAVA_HOME=$JDK_HOME
   ```

2. Use the following command to start the silent installer,here absolute_*path* is the fully qualified response file location:

   ```
   java -jar NetworkIntegrityInstaller_{release}.jar -responseFile
   {absolute_path}
   ```

   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.

3. At the end of the installation, the command window displays the location of the installer log files. Users can review these logs files to verify that the installation was successful.
4. Start the AdminServer, using the following command:

   ```
   ./startNI.sh
   ```

5. If you use a Cluster environment, start the managed servers, using the following command:

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

6. 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**

7. 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 upgrade of Network Integrity, see "Verifying the Network Integrity Installation".

After verifying a successful upgrade, perform the required post-installation actions. See Network Integrity Post-Installation Tasks for more information.

Post-Upgrade Tasks

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

1. Verify that the Network Integrity software upgrade was completed successfully. See "Verifying the Network Integrity Installation" for more information.
2. 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**.
3. Migrate your cartridges to the new version of Network Integrity. See "Migrating Cartridges" for more information.
4. Re-deploy your cartridges. See "Deploying Network Integrity Cartridges" for more information.

Blue Green Upgrade

The Blue Green Upgrade is designed to minimize downtime and risk by creating a backup environment and thoroughly testing the new version before replacing the production system.

This section uses the following terms to explain the Blue Green upgrade method:

- **Blue environment:** This refers to the current (running) production environment that is active.
- **Green environment:** This refers to the staging environment where the backed-up MDS schema (secured and synchronized using Data Guard) is upgraded and validated by the uploading to the new version (8.0 release). All upgrade and testing operations are

performed in the Green environment, ensuring no disruption to the Blue environment. Once the validation is completed, the Green environment is promoted as the new production environment.

The Blue Green upgrade method involves three phases:

- **Phase 1:** Staging and ValidationStaging and Validation
- **Phase 2:** Staging Update and Production SwitchoverStaging Update and Production Switchover
- **Phase 3:** Upgrading the Blue EnvironmentUpgrading the Blue Environment

Prerequisites for Blue Green Upgrade

The prerequisites for upgrading Network Integrity using Blue Green upgrade is as following:

- Primary production environment (Blue environment): The environment running with the older version of Network Integrity. It is also the production environment of Network Integrity.
- Secondary container database (CDB) (Green environment): You must provision a new Oracle CDB with the same CDB as the Blue environment.

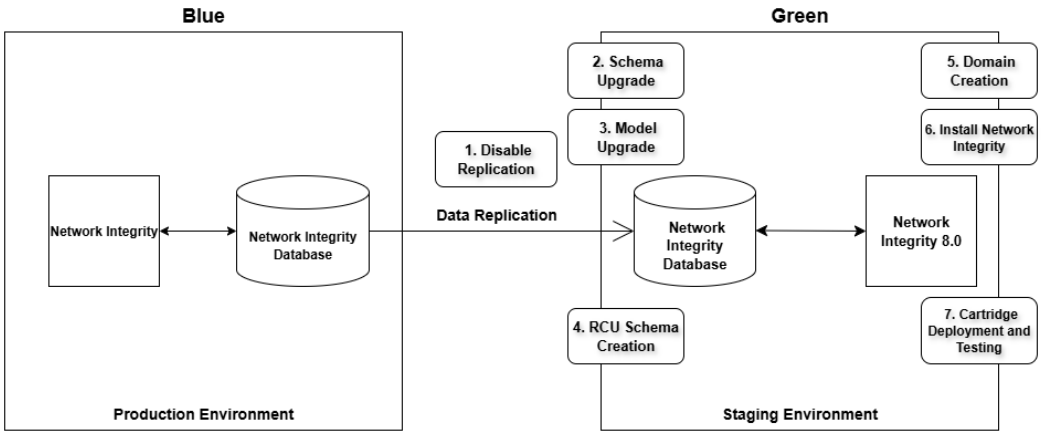
> **Note**
>
> PDB-level data replication using Data Guard is supported only in Oracle Database 23ai. For more information, see Oracle Data Guard documentation.

- Establish Data Guard Configuration: You must implement Oracle Data Guard for real-time data replication between the Blue and Green environments to ensure that the MDS schema from production is replicated.

Staging and Validation

Figure 9-1 depicts the first phase of the Blue Green upgrade method.

Figure 9-1 Phase 1: Staging and Validation



To carry out the first phase of Blue Green Upgrade:

> **Note**
>
> The Blue environment is the live production instance and remains online throughout the staging and validation phase. The Green environment will be configured and upgraded separately for staging and validation with the latest application version.

1. Temporarily disable Data Guard replication between the Blue and Green CDBs.
2. Perform the upgrade on the Green CDB to a database version compatible with NI 8.0.0.0 application version.
3. Create the RCU schema using Oracle Fusion Middleware 14c RCU utility by following the steps outlined in Installing and Configuring the Oracle Database.

   > **Note**
   >
   a. Create the RCU schema in the same PDB as the MDS-replicated data in the designated staging CDB.
   b. Use an RCU schema prefix that differs from the production environment prefix.

4. Perform domain creation using the Oracle Fusion Middleware 14c Domain Creation Utility by following the steps in Installing and Configuring Oracle WebLogic Server .

   > **Note**
   >
   a. Ensure that the domain configuration matches that of the production environment.
   b. During the domain creation process, use the newly created RCU schema from the previous step and associate it with the domain.

5. Upgrade the replicated MDS schema (the production schema replicated to the staging CDB using Data Guard) by using the Oracle Fusion Middleware 14c Schema Upgrade Utility:
   a. Navigate to *MW_HOME*`/oracle_common/upgrade/bin/ua` where ***MW_HOME*** is the directory in which Oracle Fusion Middleware 14C is installed.
   b. Launch the UA tool to upgrade the schema.
      The Welcome screen appears.
   c. Click **Next**.
      The Upgrade Type screen appears.
   d. Select **Individually Selected Schemas**, and click **Next**.
      The Available Components screen appears. It lists the available components that can be upgraded.
   e. Select the **Oracle Metadata Section** component and click **Next**.
      The Domain Directory screen appears.
   f. Select the newly created WebLogic domain directory and click **Next.**
      The Prerequisites screen appears.

g. Confirm that the database backup is complete by selecting the following checkboxes and click **Next**:

- **All affected servers are down**
- **All affected data is backed up**
- **Database version is certified by Oracle for Fusion Middleware upgrade**
- **Certification and system requirements have been met**

The MDS Schema screen appears.

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

i. In the **Database Connect String** field, enter the value in *hostname*:*portnumber*/*ServiceName* format.

> **Note**
>
> For a RAC database, provide RAC Server DB Information in the following format: *hostname*:*portnumber*/*ServiceName*.

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

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

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 replicated MDS Schema.

n. In the **Schema Password** field, enter the replicated MDS Schema password, and click **Next**.
The Examine screen appears.

o. Verify that all listed schemas show the status as **ready for upgrade**, and then click **Next**.
The Upgrade Summary screen appears.

p. Verify the details of the schemas to be upgraded and click **Upgrade**.
The Upgrading Progress screen appears. You can monitor the progress of the upgrade from this screen.

q. After the upgrade completes, click **Next**.
The Upgrade Success screen appears.

r. Verify successful upgrade and click **Close**.

6. Perform Model Upgrade on **Replicated MDS Schema** using **NIDBTools.jar** file.

a. Extract the **jar** file to a temporary directory (e.g., **temp**).

b. Run the **NIDBTools.jar** file using the following command and provide the following details when prompted:

```
java -jar NIDBTOOLS.jar
```

i. In the **Enter Database Hostname** field: Enter the hostname of the staging database.

ii. In the **Enter Database Port Number** field: Enter the port number of the staging database.

iii. In the **Enter Database Service Name** field: Enter the service name of the staging database.

iv. In the **Enter MDS Schema Username** field: Enter the replicated MDS schema name (e.g, **NISchema_MDS**).

v. In the **Enter MDS Schema Password** field: Enter the password for the replicated MDS schema.

vi. In the **Enter DB Version to Upgrade** field: Select the target version from the allowed values (**7.3.6.3.0**, **7.3.6.4.0**, **7.4.0.0.0**, **7.5.0.0.0**, **7.5.0.1.0**, **8.0.0.0.0**). Provide **8.0.0.0.0** as the target version.

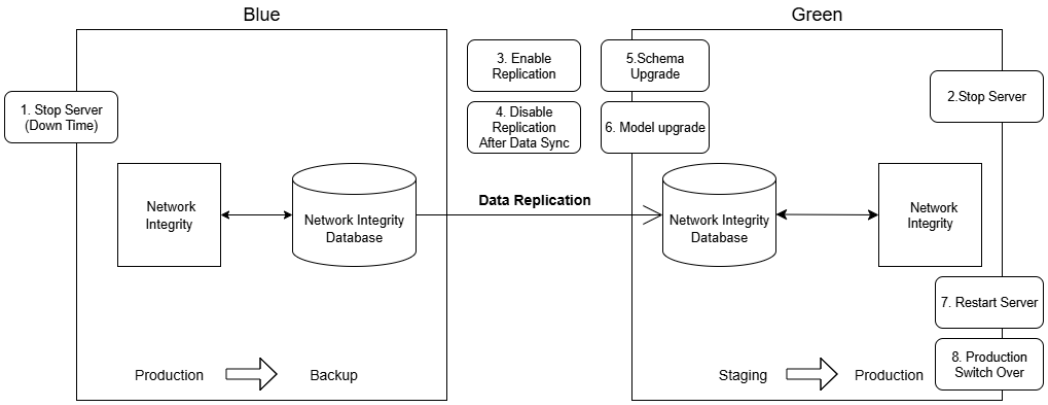
vii. In the **Enter NIDBTools Extracted Location** field: Provide the path to the temporary directory (**temp**) where the **NIDBTools.jar** file was extracted.

7. Install Network Integrity 8.0 by following the instructions in Upgrading Network Integrity Using Blue Green Upgrade.

Staging Update and Production Switchover

Figure 9-2 depicts the second phase of the Blue Green upgrade method.

Figure 9-2 Phase 2: Staging Update and Production Switchover



> **Note**
>
> Upon completion of the staging and validation phase, the Blue environment must be taken offline, resulting in a scheduled downtime.

To carry out the second phase of Blue Green Upgrade:

1. Shut down the Blue and Green application Servers.
2. Create a data dump of all newly created RCU schemas on the Green application server.

> **Note**
>
> Backup of the upgraded MDS schema is not required.

3. On the production CDB (Blue application server), create a new RCU schema using the Oracle Fusion Middleware 14c Repository Creation Utility (RCU) with the same schema prefix used on the Green application server.
4. Import the schema dump from the Green application server to the corresponding schema on the Blue application server.

> **Note**
>
> You must perform this step because, because, when Data Guard is re-enabled, any schemas that exist on the standby (Green) but not on the primary (Blue) are removed from the standby during the resynchronization to maintain data consistency. To preserve the newly created schemas, ensure they are present on the primary before reactivating Data Guard.

5. Reactivate Data Guard to synchronize the Green PDB with the most recent data from the Blue production environment.

> **Note**
>
> This process will revert the Green MDS schema to the older version currently used in the production database. This step is mandatory to ensure that all the latest production data is transferred to the staging environment.

6. Monitor and verify that data synchronization is achieved.
7. Disable Data Guard.
8. Connect to the staging PDB as a SYSDBA user and manually update the SCHEMA_VERSION_REGISTRY table for the replicated MDS schema by setting VERSION to '12.2.1.0.0', EDITION to NULL, and UPGRADED to 'N'.

> **Note**
>
> This step must be performed so that the schema upgrade utility considers the replicated MDS schema as eligible for upgrade.

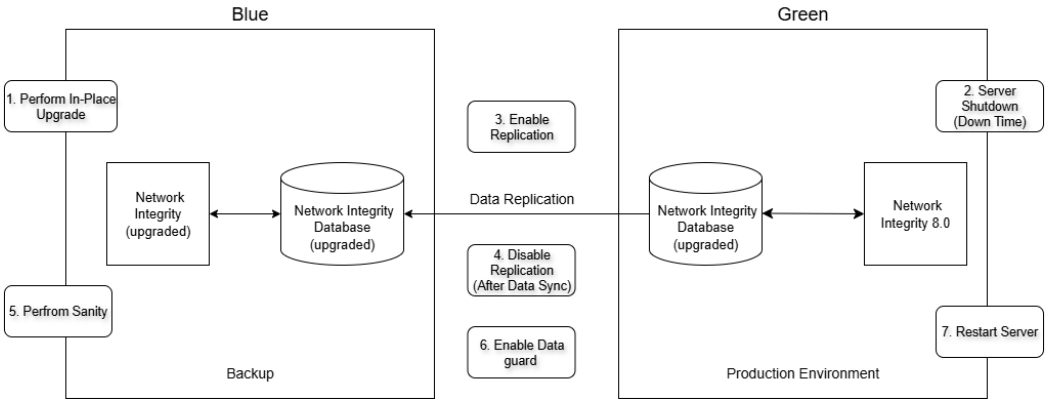
9. Perform the schema upgrade again on the replicated MDS schema by following the step 5 of the Staging and Validation phase.
10. Perform the model upgrade again on the replicated MDS schema as described in 6 of the Staging and Validation phase.
11. Restart all Green environment servers after clearing the **tmp** files and cache from each server.
12. Redeploy all the latest 8.0.0.0 cartridges that were deployed during the Blue-Green upgrade and perform Sanity Test.
13. Redirect production traffic to the upgraded Green environment by updating the production URLs accordingly.

Once this phase is completed, the Green environment will function as the new production environment.

Upgrading the Blue Environment

Figure 9-3 depicts the third phase of the Blue Green upgrade method.

Figure 9-3 Phase 3: Upgrading the Blue Environment



After completing the second phase of the Blue Green upgrade, the Green environment functions as the active production environment. The Blue environment will function as backup once the upgrade and data synchronization is completed.

To upgrade the Blue environment:

1. Upgrade the Blue environment using the in-place upgrade steps outlined in In-Place Upgrade.
2. Shut down the Green Environment servers.

> **Note**
>
> This process requires downtime for the production setup running on the Green environment. You must plan an appropriate downtime window and complete all the following steps during this period.

3. Initiate Data Guard replication from Green to Blue environments to synchronize all data changes.
4. Suspend Data Guard replication once synchronization is completed.
5. Test the Blue environment to make sure everything works correctly.
6. Shut down Blue environment server and keep it as a backup.
7. Enable Data Guard replication from Green to Blue environments.
8. Start the Green environment for production use.

After completing these steps, the Green environment will operate as the primary production setup, while the Blue environment functions as the standby or backup.

Upgrading Network Integrity Using Blue Green Upgrade

Upgrading Network Integrity using Blue Green method can be done in one of two ways:

- Blue Green Upgrade Using Interactive Install
- Blue Green Upgrade Using Silent Mode

Blue Green Upgrade Using Interactive Install

To upgrade Network Integrity using Interactive installer (using Blue Green method):

1. Create a directory (*dir*).
2. Download the Network Integrity Installer software from the Oracle software delivery website and save it to *dir:*
   https://edelivery.oracle.com
3. Export JDK Home by running one of the following command. See Software Requirements for JDK version information.

   ```
   export JAVA_HOME=$JDK_HOME
   ```
4. Run the Oracle Nextgen Network Integrity Installer using the following command:

   ```
   java -jar NetworkIntegrityInstaller_{release}.jar
   ```

   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 Installation Location Screen appears.
   - If you have installed any Oracle products on the system prior to installing Network Integrity, the The Installation Location Screen appears.
7. In **NI_Home** field, enter or browse the path to the folder where you want to install Network Integrity and click **Next**.
   The Installation Type Screen appears.
8. Select **Complete** and click **Next**.

   The WebLogic Administration Server Connection Information screen appears.
9. Do the following:
   a. In the **Host Name** field, enter the IP address or the host name of the Administration
   b. In the **Port Number** field, enter the Administration Server port
   c. In the **User Name** field, enter user name with which you connected to the Administration Server.
   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** checkbox as per your requirements.
   f. In the **Keystore** field, enter the keystore location if the **Use SSL** checkbox is selected.
   g. Click **Next**.

The Target Selection screen appears

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

    The DB Type Selection Page appears.

    > **Note**
    >
    > If you select cluster option, ensure that all the managed servers are running.

11. In the Database Type Selection screen, select the same database type as used in the Blue side production environment

    a. If the **Standard Oracle Enterprise Database** option is selected. the Standard DB Connection screen appears.

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

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

       iii. In the **User Name** field, enter the user name of the standby database, **SYSDBA**.

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

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

       vi. Click **Next**.
       The NI Schema Table Creation screen appears.

    b. If the **Oracle Real Application Cluster Database** option is selected, the RAC DB Connection screen appears.

       i. In the **RAC Database Connection String** field, enter the connection details to connect to the Oracle RAC database of standby Database.
       For example:

       HOST NAME1:PORT1:SERVICE NAME1,HOST NAME2:PORT2:SERVICE NAME2

       ii. In the **User Name** field, enter the user name for the Oracle RAC database **SYSDBA**.

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

       iv. Click **Next**.

       The Network Integrity Schema Table Creation screen appears.

12. Select **No** and click **Next**.
    The MDS Schema User Connection screen appears.

13. Do the following:

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

    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.

> **⚠ Caution**
>
> You need to use the replicated MDS schema which got updated.

14. Select the type of security provider you want to use by performing one of the following steps:
    a. If you select **Embedded_LDAP** option, the Admin User Creation screen appears. (Optional) Do the following:
        i. In the **User Name** field, enter the user name for accessing and using Network Integrity.
        ii. In the **Password** field, define a password for the Network Integrity.

> **ⓘ Note**
>
> The password requirements are as follows:
>
> - Password length must be between 8 to 12 characters.
> - It should contain at least one uppercase letter, one lowercase letter, one number and one special character.
> - It must not contain the username either directly or in reverse.
> - You may use a character 3 times in a row maximum, but not more than 4 times in total.

        iii. In the **Confirm Password** field, enter the password again to confirm it.
        iv. Click **Next**. The Internal user Creation screen appears.
    b. If you select **External Security Provider**, the External Security Provider Connection Information screen appears.
    Do the following:
        i. In the **LDAP Server Host Name** field, enter the host name for the external LDAP
        ii. In the **LDAP Server Port Number** field, enter the port number for the external LDAP server.
        iii. In the **LDAP Server User Name** field, enter the user name for the external LDAP
        iv. In the **LDAP Server Password** field, enter the password for the external LDAP
        v. In the **User Base DN** field, enter the user base
        vi. In the **Group Base DN** field, enter the group base.
        vii. Click **Next**.
        the Internal user Creation screen appears.
    c. If you select **Other Security Provider**, and click **Next**, the Disable unsecured Port screen appears. Proceed directly to step 16.
15. In Internal user Creation Screen, do the following:
    a. In the **User Password** field, define a password for the Network Integrity internal user.

> **Note**
>
> The password requirements are as follows:
>
> - Password length must be between 8 to 12 characters.
> - It should contain at least one uppercase letter, one lowercase letter, one number and one special character.
> - It must not contain the username either directly or in reverse.
> - You may use a character 3 times in a row maximum, but not more than 4 times in total.

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

c. Click **Next**.
The Disable Unsecured Listen Port screen appears.

16. Select whether to disable the unsecured listen port by doing one of the following:

    a. Select **Yes** if you are configuring Network Integrity to communicate and listen over SSL-enabled ports only, by disabling non-SSL Ports.

    b. Select **No** if you are configuring Network Integrity to communicate and listen over both SSL and non-SSL ports.

17. Click **Next**.
The Java Home Location screen appears.

18. Accept the default settings and click **Next**.

    The Installation Summary screen appears.

19. Review the content in the summary and click **Next**.

    The Installation Progress Screen appears.

20. You can view the installation progress.

> **Note**
>
> During the installation progress, two pop-up messages will appear. The first message asks for confirmation to stop the WebLogic Servers and the second message lists the order in which the servers must be manually restarted. Click **OK** on both the messages to continue.

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

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

23. To start the server, do the following:

    a. Start the AdminServer using the following command:

    ```
    ./startNI.sh
    ```

    b. If your are using Cluster environment ,Start the managed servers, using the following command:

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

24. Open the following file once the installation is complete, to get the URL to access Network Integrity: *NI_Home*/**install/readme.txt**, where *NI_Home* is the directory where Network Integrity is installed.
25. Copy the URL and paste it in the browser window's address field and press **Enter** to access Network Integrity.

    You can access Network Integrity.

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

After verifying a successful installation, perform the required post-installation actions. For more information, see Network Integrity Post-Installation Tasks.

Blue Green Upgrade Using Silent Mode

You can use the silent install mode when you are installing Network Integrity using the same configuration repeatedly. The silent mode does not use the GUI and 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 response file templates come as part of the Network Integrity installation package: **oracle.communications.integrity.rsp**

The response file templates contain all the fields that the installer requires to perform installation in silent mode

When you extract the installer JAR file, the response file templates are saved in the **Response** directory at the following location: **Disk1/stage/Response**.

Table 9-2 describes the Network Integrity response file template properties, along with the values that should be specified for a complete installation scenario.

Table 9-2 Response File Template Properties

Response File Template Name	Property Name	Description (with Default Value)
Installation Location Details (Required)	ORACLE_HOME	Directory path where the NI application will be installed
Installation Type Details (Required)	INSTALLATION_TYPE	Type of installation (Allowed values: Complete or Upgrade). Set "**Complete**" for Blue Green Upgrade .
WebLogic Admin Server Connection Details (Required)	APP_ADMIN_HOST	Hostname or IP address of the WebLogic Admin Server
WebLogic Admin Server Connection Details (Required)	APP_ADMIN_PORT	Port number for the WebLogic Admin Server (enclose in double quotes). For SSL-based deployment, provide the SSL port value and specify the keystore file location in the APP_SERVER_KEYSTORE property.

Table 9-2 (Cont.) Response File Template Properties

Response File Template Name	Property Name	Description (with Default Value)
WebLogic Admin Server Connection Details (Required)	APP_SERVER_USER	Username for the WebLogic Admin Server
WebLogic Admin Server Connection Details (Required)	APP_SERVER_PASSWD	Password for the WebLogic Admin Server
WebLogic Admin Server Connection Details (Required)	APP_SERVER_KEYSTORE	Path to the keystore file required for SSL-based deployment (e.g., certs/Keystore.jks)
Target Selection Details (Required)	APP_TARGET_NAME	Name of the target (such as AdminServer or CL1) where the NI application will be installed
Database Selection Details (Required)	DATABASE_TYPE	Type of database used (Accepted values: Standard Oracle Enterprise Database or Oracle Real Application Cluster Database).Use the Same Type used in Production environment.
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_HOST_NAME	Hostname of the standard Oracle database
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_HOST_PORT	Port number of the standard Oracle database (enclose in double quotes)
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_USER_NAME	Username with SYSDBA privileges for the standard Oracle database
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_PASSWORD	Password for the SYSDBA user of the standard Oracle database
Standard DB Details (Required only if DATABASE_TYPE = Standard Oracle Enterprise Database)	DB_SERVER_SERVICE	Service name of the standard Oracle database
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_CONNECTION_STRING	Connection string details for Oracle RAC, in the format: HostName1:Port1:Service1,Host Name2:Port2:Service2
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_SERVER_USER	Username for connecting to the Oracle RAC database
RAC DB Details (Required only if DATABASE_TYPE = Oracle Real Application Cluster Database)	RAC_SERVER_PASSWORD	Password for the Oracle RAC database server
Network Integrity Schema Table Creation (Required only if INSTALLATION_TYPE=Complete)	DB_SCHEMA	Flag to indicate whether to create the app schema table (Allowed values: “**true**” or “**false**”). For Blue Green Upgrade installation, provide “**false**”

Table 9-2 (Cont.) Response File Template Properties

Response File Template Name	Property Name	Description (with Default Value)
MDS Schema Information Details (Required)	SCHEMA_OWNER_NAME	Username for the MDS (Metadata Services) Note: Details of Replicated upgraded MDS schema Details
MDS Schema Information Details (Required)	SCHEMA_OWNER_PASSWD	Password for the MDS (Metadata Services) schema user Note: Details of Replicated upgraded MDS schema Details
Security Provider Selection Details	SECURITY_PROVIDER_NAME	Type of security provider to select (Allowed values: Embedded_LDAP or External_LDAP)
Embedded LDAP Details (User creation is optional; values can be left empty even if SECURITY_PROVIDER_NAME is set to Embedded LDAP)	LDAP_USER_NAME	Username to be created in the embedded LDAP directory
Embedded LDAP Details (User creation is optional; values can be left empty even if SECURITY_PROVIDER_NAME is set to Embedded LDAP)	LDAP_PASSWD	Password for the newly embedded LDAP user Note: Password Requirements: · Length must be between 8 to 12. · It should contain at least one uppercase letter, one lowercase letter, one number and one special character. · It must not contain username directly or in reverse · No character can appear more than 4 times in total or more than 3 times in a row.
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_HOST	Hostname of the external LDAP server
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_PORT	Port number of the external LDAP server
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_USER	Username for connecting to the external LDAP server
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_PASSWORD	Password for the external LDAP server user

Table 9-2 (Cont.) Response File Template Properties

Response File Template Name	Property Name	Description (with Default Value)
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_USER_BASE_DN	User BASE DN information of external LDAP server
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_GROUP_BASE_DN	Group BASE DN information of external LDAP server
External LDAP Details (Required only if SECURITY_PROVIDER_NAME= External LDAP)	LDAP_SERVER_KEYSTORE	Path to the keystore file for the external LDAP server (e.g., certs/externalLDAPKeystore.jks)
NI Internal user Details (Required)	LDAP_DEF_USER_PASSWD	Password for the NI internal user Password Requirement: Length must be between 8 to 12. · It should contain at least one uppercase letter, one lowercase letter, one number and one special character. · It must not contain username directly or in reverse · No character can appear more than 4 times in total or more than 3 times in a row.
Disable Non-SSL Port Option (Required)	DISABLE_NONSSLPORT	Option to disable the non-SSL port (Allowed Values: set to “true” to disable, or “false” to keep enabled)

> **Note**
>
> Before using the response file, ensure that any optional properties or values not required by the installer are left empty.

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 upgrade Network Integrity in silent mode (using Blue Green method):

1. Export JDK Home by running the following command. See Software Requirements for JDK version information.

   ```
   export JAVA_HOME=$JDK_HOME
   ```

2. Use the following command to start the silent installer, here *absolute_path* is the fully qualified response file location:

   ```
   java -jar NetworkIntegrityInstaller_{release}.jar -responseFile
                    {absolute_path}
   ```

The installation runs silently in the background.

> **Note**
>
> The installer shuts down all of the servers, including the Administration Server and the Managed Serversm after silent installation. You must start all of the servers manually after the installation is complete.

3. At the end of the installation, the command window displays the location of the installer log files. Users can review these logs to verify that the installation was successful.
4. To start the server, do the following:
   a. Start the AdminServer, using the following command:

      ```
      ./startNI.sh
      ```

   b. If your are using a Cluster environment, start the managed servers using the following command:

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

5. Open the following file once the installation is complete to get the URL to access Network Integrity: *NI_Home***/install/readme.txt**
   Where *NI_Home* is the directory where Network Integrity is installed.
6. Copy the URL and paste it in the browser window's address field and press **Enter** to access Network Integrity.

   You can access Network Integrity.

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

After verifying a successful installation, perform the required post-installation actions. For more information, see Network Integrity Post-Installation Tasks.

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.

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 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

Uninstalling Network Integrity

To uninstall Oracle Communications Network Integrity:

1. **Stop the WebLogic Server**: Perform a graceful shutdown of all application servers.
2. **Delete the Application Domain**: Manually remove the domain directory of the application and its contents from the file system.
3. **Remove the RCU Schemas**: Use the Repository Creation Utility (RCU) to remove the associated schemas from the database.
4. **Remove Additional Software** (if required): Uninstall any related software components, if required.

12

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: 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: 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*.

A

Configuring Oracle HTTP Server as Proxy

Oracle HTTP Server (OHS) can be used as a proxy server for Network Integrity. It can be installed in either collocated mode or in a standalone mode. Oracle recommends using the standalone mode to install OHS. This section provides instructions for installing OHS in standalone mode.

Directory Placeholders Used

Configuring Oracle HTTP Server as Proxy describes all the directory placeholders used in this section.

Table A-1 Description of Directory Placeholders

Placeholder	Directory Description
Oracle_Home	The home directory where OHS is installed.
OHS_Domain	The location where domain is created. The default location is *Oracle_Home***/user_projects/domains/***OHS_DomainName* where *OHS_DomainName* is the name of the OHS domain.
OHS_Component	Component directory that is created during domain creation.
Wallet_Path	The directory where Oracle Wallet is created. By default, it is set to *Oracle_Home***/ohsfmw/user_projects/domains/***OHS_DomainName***/config/fmwconfig/components/OHS/instances/***OHS_Component***/keystores/***Wallet_Name* where *Wallet_Name* is the name of Oracle wallet.

Configuring Oracle HTTP Server

To configure Oracle HTTP Server when installed in standalone domain:

> **Note**
>
> For learning about the system requirements and specifications to install OHS, see *Oracle Fusion Middleware System Requirements and Specifications*.

1. Download and install Oracle HTTP Server 14.1.2.
   For more information on installing Oracle HTTP Server, see *Oracle Fusion Middleware Installing and Configuring Oracle HTTP Server*.
2. After installing Oracle HTTP Server, navigate to the **/oracle_common/common/bin***Oracle_Home*directory and run the **config.sh** script to create a domain.
3. After creating a domain, start the Node Manager.

If the node manager port of Oracle HTTP Server conflicts with the node manager port of WebLogic domain, change it using WLST.

4. Start the Node Manager using the following options:
   - Run the `./startNodeManager.sh` command.
   - Run the `nohup ./startNodeManger.sh` command to start the Node Manager with nohup.

   You can locate this file in your *OHS_Domain***/bin** directory.

   > **Note**
   >
   > Use the `./stopNodeManager.sh` command to stop the Node Manager.

5. Run the following command to view the output:

   ```
   tail -f nohup.out
   ```

6. Once Node Manager is running, start your Oracle HTTP Server component by using the following command and provide the node manager password when prompted:

   ```
   ./startComponent.sh ComponentName
   ```

   A message indicating a successful connection to the component appears. You can locate this file in your *OHS_Domain***/bin** directory.

7. Access the following Oracle HTTP Server URL to verify that the Oracle HTTP Server is running.

   ```
   http://<OHS_HostName>:<OHS_NonSSLPort> or https://OHS_HostName:OHS_SSLPort
   ```

   The Oracle HTTP Server welcome page appears.

Changing Node Manager Port

To change the node manager port, go to **<Oracle_Home>/oracle_common/common/bin** and run `./wlst.sh`:

```
[bin]$ ./wlst.sh
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands
wls:/offline> readDomain('<Oracle_Home>/user_projects/domains/<OHS_DomainName>')
wls:/offline/ohsop80idp4>cd('Machine')
wls:/offline/ohsop80idp4/Machine>cd('localmachine')
wls:/offline/ohsop80idp4/Machine/localmachine>cd('NodeManager')
wls:/offline/ohsop80idp4/Machine/localmachine/NodeManager>cd('localmachine')
wls:/offline/ohsop80idp4/Machine/localmachine/NodeManager/localmachine>ls()
-rw-   Adapter                                    null
-rw-   AdapterName                                null
-rw-   AdapterVersion                             null
-rw-   DebugEnabled                               false
-rw-   Id                                         0
-rw-   InstalledVMMAdapter
-rw-   ListenAddress                              localhost
-rw-   ListenPort                                5556
-rw-   NMSocketCreateTimeoutInMillis             15000
-rw-   NMType                                    null
-rw-   Name                                      localmachine
```

```
-rw-   NodeManagerHome                                  null
-rw-   Notes                                            null
-rw-   PasswordEncrypted                                ********
-rw-   ShellCommand                                     null
-rw-   Tag
-rw-   UserName                                         null
wls:/offline/ohsop80idp4/Machine/localmachine/NodeManager/
localmachine>set('ListenPort',5555)
wls:/offline/ohsop80idp4/Machine/localmachine/NodeManager/localmachine>updateDomain()
wls:/offline/ohsop80idp4/Machine/localmachine/NodeManager/localmachine>closeDomain()
wls:/offline>exit()
Exiting WebLogic Scripting Tool.
```

Updating the mod_wl_ohs.conf File

You must edit the **mod_wl_ohs.conf** file to enable the Oracle HTTP Server instance to forward requests to the applications deployed on the Oracle WebLogic Server or clusters.

To update the **mod_wl_ohs.conf** file:

1. Navigate to **<OHS_Domain>/config/fmwconfig/components/OHS/instances/<OHS_component>** and open **mod_wl_ohs.conf**.
2. Add directives as follows:
   - To forward requests to the UIM application running on a single Oracle WebLogic Server instance, specify `/NetworkIntegrity` within the `<location>` element as follows:

     ```
     <Location /NetworkIntegrity >
     SetHandler weblogic-handler
     WebLogicHost host
     WebLogicPort port
     </Location>
     ```

     Where:

     – *host* is the name of the WebLogic Administration server machine.

     – *port* is the port of the server on which UIM 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:

     ```
     <Location /NetworkIntegrity >
     SetHandler weblogic-handler
     WebLogicCluster host1:port1,host2:port2
     </Location>
     ```

     Where:

     * *host1* and *host2* 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:

     ```
     <Location /NetworkIntegrityApp-NetworkIntegrityControlWebService-context-root>
     SetHandler weblogic-handler WebLogicHost host WebLogicPort port
     </Location>
     ```

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 single Oracle WebLogic Server instance into which you want to deploy cartridges, specify **/cartridge** within the `<location>` element as follows:

```
<Location /cartridge>
SetHandler weblogic-handler WebLogicHost host WebLogicPort port
</Location>
```

Where:

- *host* is the name of the WebLogic Administration server machine.
- *port* is the port of the server on which Network Integrity is installed.

- Similarly, specify `/em` within the `<location>` element to access em console.

```
<Location /cartridge> SetHandler
weblogic-handler WebLogicHost host
WebLogicPort port
</Location>
```

Where:

- *host* is the name of the WebLogic Administration server machine.
- *port* is the port of the server on which Network Integrity is installed.

Configuring SSL for OHS

Pre-requisite: The custom certificate and corresponding keystore should be generated for Network Integrity.

To configure SSL for OHS:

1. Go to the path **<OHS_Domain>/ config/fmwconfig/components/OHS/instances/ <Component> /keystores/** and create Oracle wallet for OHS as follows:

```
./orapki wallet create -wallet <Wallet_Name> -auto_login_only
./orapki wallet add -wallet <Wallet_Name> -trusted_cert -cert <CERT_FILE> -
auto_login_only
```

The wallet is created.

2. Add keystore to the wallet as follows:

```
./orapki wallet jks_to_pkcs12 -wallet <Wallet_Name> -keystore <Keystore file> -
jkspwd <Password>
```

3. Go to **<Oracle_Home>/user_projects/domains/<OHS _Domain>/config/fmwconfig/ components/OHS/instances/<OHS_Component>** to edit the **ssl.conf** file. Search for **Path to the wallet** and update the **SSLWallet** sample path with the created wallet path.

4. Update the **mod_wl_ohs.conf** file, located at **<Oracle_Home>/user_projects/domains/ <OHS Domain>/config/fmwconfig/components/OHS/instances/<OHS component>** with the created wallet as follows:

```
<IfModule weblogic_module>
   WLSSLWallet "<Wallet_Path>"
</IfModule>
```

```
SSL ports of managed servers should be mentioned for WeblogicCluster and add
SecureProxy ON and WLProxySSLPassThrough ON parameters in <Location/>.
Example:
<Location /NetworkIntegrity >
    SetHandler weblogic-handler
    WebLogicCluster <Host1>:<MS1_SSL_Port>,<Host2>:<MS2_SSL_Port>
    Debug ALL
    DebugConfigInfo ON
    SecureProxy ON
    WLProxySSLPassThrough ON
  </Location>
```

5. Restart the component after updating SSL and **mod_wl_ohs.conf** as follows:

   ```
   ./restartComponent.sh ComponentName
   ```

6. Verify if all files are created in keystore, instance PEM, CRT, and SSO.
7. Go to **CL1**. In **General tabs**, go to **Advance Fields** and enable the WebLogic plugin for Admin Server and Managed Servers.
8. In the WebLogic console, update the frontend host and HTTPS port with the OHS host and port.
9. To configure the SSL Policy/Certificate in WebLogic Console, follow the procedure provided in *Network Integrity System Administrator's Guide*.