Oracle® Communications Network Integrity

System Administrator's Guide

Release 7.5
G13610-01
December 2024

ORACLE

Oracle Communications Network Integrity System Administrator's Guide, Release 7.5

G13610-01

Contents

5 Managing Network Integrity Performance

Preface

This guide provides instructions for monitoring and managing the Oracle Communications Network Integrity application; for example, managing and monitoring the Network Integrity system, backing up files and data, and troubleshooting.

> **Note:**
>
> Information pertaining to Managing Network Integrity security has been removed from this guide and consolidated in *Network Integrity Security Guide*.

Audience

This document is intended for Network Integrity system administrators.

Before reading this guide, you should be familiar with Network Integrity. See *Network Integrity Concepts* for an introduction to Network Integrity.

It is assumed that you have a working knowledge of the following:

- Oracle Fusion Middleware
- Oracle WebLogic Administration Server
- Database management
- Oracle Communications Unified Inventory Management (UIM)
- Oracle Communications MetaSolv Solution (MSS)
- Oracle Business Intelligence (BI) Publisher
- Unix fundamentals

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

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

1

Network Integrity System Administration Overview

This chapter provides an overview of Oracle Communications Network Integrity basic administration tasks, and the tools to perform those tasks.

Overview of Network Integrity Administration Tasks

As a Network Integrity administrator you are responsible for the day-to-day tasks of maintaining and managing Network Integrity and its users. The tasks also include managing Network Integrity components and database.

> **Note:**
>
> See *Network Integrity Developer's Guide* for information on managing cartridges in Network Integrity.

You perform the following tasks as a Network Integrity administrator:

- Manage users (create, disable, and re-enable users)
- Manage user groups (create and delete groups)
- Assign roles
- Manage Network Integrity components, which includes the following:
  - Manage third party applications in Network Integrity
  - Manage adapters in Network Integrity
- Backup and restore data
- Check and monitor Network Integrity. This includes the following tasks:
  - Monitoring Network Integrity using Enterprise Manager Grid Control
  - Monitoring Network Integrity using Enterprise Manager Fusion Middleware Control
  - Monitoring Network Integrity using WebLogic Administration Console
  - Monitoring processes (process control)
- Maintain the database

Network Integrity administration involves managing and maintaining the application and its users, and also the components and servers that you installed along with the application.

> **Note:**
>
> To manage installation and administration, log in to the OS with the same user with which you were logged in when you installed Network Integrity. This user has permission to view and modify the files in your installation's Oracle home.

About Network Integrity Administration Tools

Network Integrity is deployed on a WebLogic server. The most common tool for managing Network Integrity administration is Oracle WebLogic Server Administration Console. Following is a list of tools that you can use to manage Network Integrity administration:

> **Note:**
>
> Use these tools to perform all administrative tasks unless a specific procedure requires that you edit a file. Editing files directly might introduce inconsistencies in settings that could generate problems.

- **Oracle WebLogic Server Administration Console**

  Use the WebLogic Administration Console to perform basic system administration tasks, such as configuring security, configuring and deploying components, and monitoring the system.

  For information on the Administration Console, see *Oracle Fusion Middleware Administration Console Online Help for Oracle WebLogic Server*.

- **Oracle Enterprise Manager Fusion Middleware Control**

  For more information on Fusion Middleware Control, see the guide *Administering Oracle Fusion Middleware*.

- **Enterprise Manager Grid Control**

  Use Fusion Middleware Control to monitor and control WebLogic domains, and the Fusion Middleware components that run in the domain.

  For more information on Enterprise Manager Grid Control, see *Overview of Enterprise Manager Grid Control*.

- **Fusion Middleware Control MBean Browsers**

  Use the MBean browser to configure Network Integrity parameters such as setting the age out time limits.

  To know more about MBean browsers, see the guide *Administering Oracle Fusion Middleware*.

- **WebLogic Scripting/Command Line Tool**

  Use the WebLogic Scripting/Command Line Tool to manage and configure Network Integrity and its components.

  For more information on WebLogic Scripting/Command Line Tool, see the guide *Understanding the WebLogic Scripting Tool*.

- **Oracle Process Manager and Notification Server (OPMN)**

For more information on OPMN, see the guide OPMN: Overview.

Setting Up Environment Variables

To use Network Integrity, set the environment variables as shown in Table 1-1.

Table 1-1 Environment Variables Values for Operating Systems

Environment Variable	Value
DISPLAY	`hostname:display_number.screen_number`
LD_LIBRARY_PATH	On Solaris, ensure that the value contains the following directory: ***ORACLE_Home*/lib32** On Linux, ensure that the value contains the following directory: ***ORACLE_Home*/lib** Value for Linux: **/opt/oracle/11.1.0.7:*LD_LIBRARY_PATH***
(Solaris only) LD_LIBRARY_PATH_64	Ensure that the value contains the following directory: ***ORACLE_Home*/lib**
(AIX only) LIBPATH	Ensure that the value contains the following directory: **/opt/oracle/11.1.0.7:LIBPATH** export LIBPATH
TNS_ADMIN	Value for Linux: **/opt/oracle/11.1.0.7** export TNS_ADMIN export PATH=PATH:TNS_ADMIN

About Cartridge Deployment

See the *SCD Design Studio Modeling Network Integrity* for information about deploying cartridges interactively from Design Studio. See *SCD Developer's Guide* for information about automating cartridge deployment using the Design Studio Cartridge Management Tool (CMT). See *Network Integrity Installation Guide* for information about the Network Integrity Cartridge Deployer Tool (CDT).

2

Understanding Network Integrity Security

This chapter describes security fundamentals for Oracle Communications Network Integrity, and also provides procedures to configure user passwords and manage users.

About Network Integrity Security

Network Integrity security includes the following aspects:

- User Management.
- Secure centralized storage for users and roles that also enables secure and fast retrieval of that information.
- Guidelines regarding password policies for Network Integrity, and also for those of the application's integration with external applications, servers, and databases.
- An audit mechanism to perform audits on security related aspects and provide an audit trail of user activities (such as login attempts).

Network Integrity supports two categories of application security:

- **Authentication** is the process of identifying users or computer processes by user name and password to ensure that they are allowed to access the system. See "Authentication" for more information.
- **Authorization** controls access to specific parts of Network Integrity, such as pages, actions, and data entities. Users are granted access as a result of being assigned to security roles, which are in turn associated with security policies. For example, when an authenticated user logs in, the content of the main work area depends on their level of access. Users with unrestricted access see links to all pages in the Tasks pane while others see only links to the pages they are authorized to access. See "Authorization" for more information.

Network Integrity uses the following application systems to manage most of its security:

- Oracle Enterprise Manager enables you to create and manage users, groups, security roles, and security policies. Security roles and security policies define what pages users can access and what actions they can perform.
- WebLogic Server Administration Console enables you to create and manage users and groups.

You can also use the following application systems for additional application security measures:

- Oracle Internet Directory is an LDAP-compliant security directory that runs on the Oracle database. It is fully integrated into Oracle Fusion Middleware.
- Oracle Identity Management is an enterprise-scale tool for managing the end-to-end life cycle of user identities across all resources. Oracle Identity Management is a member of the Oracle Fusion Middleware family of products.

You can choose to use other third-party security applications. See *Administering Security for Oracle WebLogic Server* for information about configuring WebLogic with other security applications.

Oracle Platform Security Services

Oracle Platform Security Services (OPSS) provides a security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications. OPSS is both a security framework exposing security services and APIs, and a platform offering concrete implementation of security services. It includes the following elements:

- Common Security Services (CSS): The internal security framework on which Oracle WebLogic Server is based
- Oracle Platform Services: This framework provides security to Oracle applications, for example, Oracle Application Development Framework (ADF), Oracle WebCenter, Oracle SOA Suite, Oracle Web Services Manager (OWSM)
- User and Role APIs
- Oracle Fusion Middleware Audit Framework
- Oracle Security Developer Tools

Security Realms

A security realm comprises mechanisms for protecting WebLogic resources. Each security realm consists of a set of configured security providers, users, groups, security roles, and security policies. A user must be defined in a security realm to access any WebLogic resources belonging to that realm. When a user attempts to access a particular WebLogic resource, WebLogic Server tries to authenticate and authorize the user by checking the security role assigned to the user in the relevant security realm and the security policy of the particular WebLogic resource.

Security Providers

Security providers are modules that “plug into" a WebLogic Server security realm to provide security services to applications. They call into the WebLogic Security Framework on behalf of applications. You can use the security providers that are provided as part of the WebLogic Server product, purchase custom security providers from third-party security vendors, or develop your own custom security providers.

You have a choice of the following three security providers, during installation, for Network Integrity:

- The default WebLogic security provider (Embedded LDAP)
- Any external security provider
- Any other security provider, if using only the Authentication provider

See Network Integrity Installation Guide for more information on setting up security providers for Network Integrity.

About the Embedded LDAP Server

WebLogic Server uses its embedded LDAP server as the database that stores user, group, security roles, and security policies for the WebLogic security providers. The embedded LDAP server supports the following access and storage functions:

- Access and modification of entries in the LDAP server

- Use of an LDAP browser to import and export security data into and from the LDAP server
- Read and write access by the WebLogic security providers

> **Note:**
>
> WebLogic Server does not support adding attributes to the embedded LDAP server.

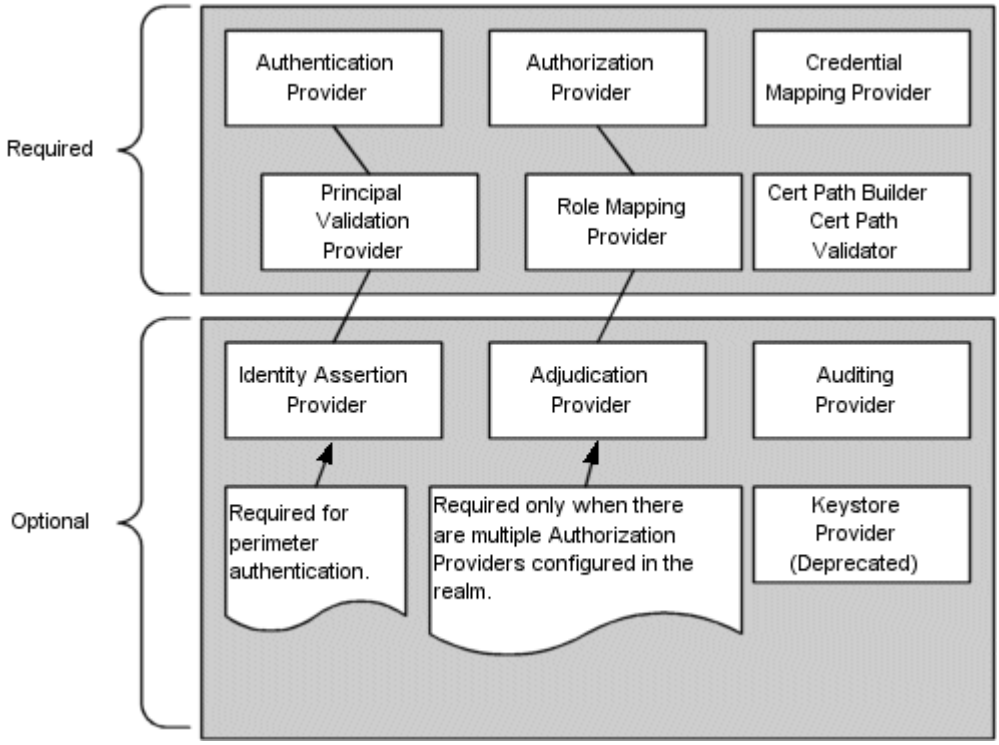
Table 2-1 provides the usage information for the WebLogic Server's embedded LDAP server.

Table 2-1 Usage Information for WebLogic Server's Embedded LDAP Server

WebLogic Security Provider	Embedded LDAP Server Usage
Authentication	Stores user and group information
Identity Assertion	Stores user and group information
Authorization	Stores security roles and security policies
Adjudication	None
Role Mapping	Supports dynamic role associations by obtaining a computed set of roles granted to a requester for a given WebLogic resource
Auditing	None
Credential Mapping	Stores user name and password credential mapping information
Certificate Registry	Stores registered end certificates

Figure 2-1 provides an illustration of the embedded LDAP server.

Figure 2-1 Embedded LDAP Server Illustration



About External Security Provider - Oracle Internet Directory

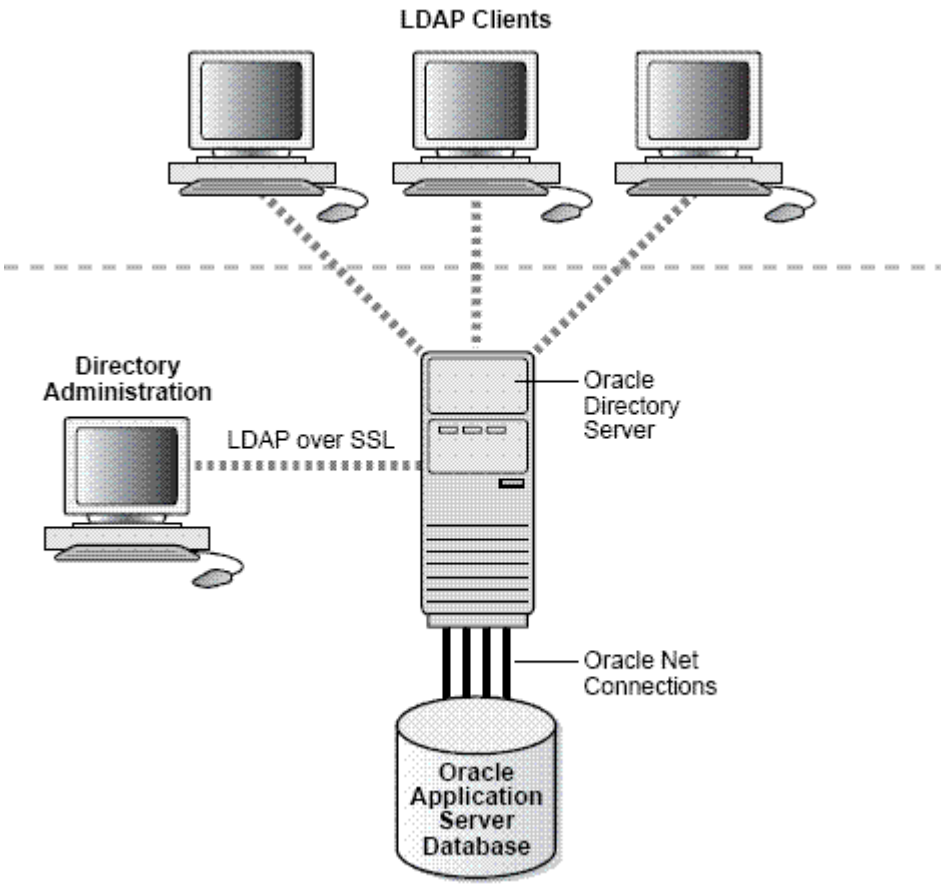
Oracle Internet Directory is a general purpose directory service that combines Lightweight Directory Access Protocol (LDAP) Version 3 with an Oracle Database. It is a component of Oracle Identity Management which is an integrated infrastructure that provides distributed security services for Oracle products and other enterprise applications. Oracle Internet Directory runs as an application on an Oracle Database. It communicates with the database by using Oracle Net Services, Oracle's operating system-independent database connectivity solution. The database may or may not be on the same host.

Oracle Internet Directory includes:

- Oracle directory server, which responds to client requests for information about people and resources, and to updates of that information, by using a multi-tiered architecture directly over TCP/IP.
- Oracle directory replication server, which replicates LDAP data between Oracle directory servers.
- Directory administration tools, which include:
  - Oracle Directory Manager, which has a Java-based graphical user interface.
  - A number of command-line administration and data management tools invoked from LDAP clients.
  - Directory server management tools within Oracle Enterprise Manager. These tools enable you to:
    * Monitor real-time events and statistics from a normal browser
    * Start the process of collecting such data into a new repository
- Oracle Internet Directory Software Developer's Kit.

Figure 2-2 provides an illustration of the Oracle Internet Directory.

Figure 2-2 Oracle Internet Directory Illustration



For more information on Oracle Internet Directory, see the Oracle Internet Directory documentation at the following link:

http://www.oracle.com/technology

> **Note:**
>
> For information on any other external security providers, see the respective product documentation.

Security Provider Databases

A security provider database contains the users, groups, security roles, security policies, and credentials used by some types of security providers to provide security services. For example, an authentication provider requires information about users and groups; an authorization provider requires information about security policies; a role mapping provider requires information about security roles, and a credential mapping provider requires information about credentials to be used to remote applications. These security providers need this information to be available in a database to function.

The security provider database can be the embedded LDAP server (as used by the WebLogic security providers), a properties file (as used by the sample custom security providers, available on the web), or a production-quality, customer-supplied database that you may already be using.

Initialize the security provider database the first time you use security providers. That is, before the security realm containing the security providers is set as the default (or, active) security realm. This initialization can be done:

- When a WebLogic Server instance boots
- When a call is made to a security provider's MBeans

At minimum, the security provider database is initialized with the default groups, security roles, and security policies provided by WebLogic Server.

See *Administering Security for Oracle WebLogic Server* for more information.

If you have multiple security providers of the same type configured in the same security realm, these security providers may use the same security provider database. This behavior holds true for all of the WebLogic security providers.

For example, if you configure two WebLogic Authentication providers in the default security realm (called `myrealm`), both WebLogic Authentication providers use the same location in the embedded LDAP server as their security provider database, and thus, use the same users and groups. Furthermore, if you add a user or group to a WebLogic Authentication provider, the user or group appears in the other WebLogic Authentication provider as well.

> **Note:**
>
> If you have two WebLogic security providers of the same type configured in two different security realms, each uses its own security provider database. Only one security realm can be active at a time.

3rd party security providers can be designed so that each instance of the security provider uses its own database or so that all instances of the security provider in a security realm share the same database.

Configuring the Authentication Provider

When you use an external authentication provider, you must configure to use it with Network Integrity.

To configure the authentication provider:

> **Note:**
>
> The use of Oracle Internet Directory and Oracle Identity Manager (OIM) requires a separate license from Network Integrity.
>
> Please contact your Oracle representative for information on acquiring a license.

1. Log in to the WebLogic Administration console.

2. In the Home page, select **Security Realms**.

   The Summary of Security Realms screen appears.

3. Select *YourRealm*.

   The Setting for *YourRealm* screen appears.

4. Select the **Providers** tab to display it.

   The Authentication tab is displayed by default. If not, then select to display it.

5. Click **Lock & Edit** in the Change Center in the left pane, to activate all buttons in this tab.

6. Click **New**.

   The Create a New Authentication Provider screen appears.

7. In the **Name** field, enter the name *NewAuthProvider* of the authentication provider.

8. From the Type list, select **OracleInternetDirectoryAuthenticator**.

9. Click **OK**.

   The Settings for *YourRealm* screen appears.

   The Authentication tab is displayed by default.

   You can see the newly created authentication provider, *NewAuthProvider*, in the Authentication Providers table.

10. Click *NewAuthProvider*.

    The Settings for *NewAuthProvider* screen appears.

    In the Configuration tab, the Common tab is displayed by default.

    If the **Common** tab is not displayed, select it to display it.

11. In the **Control Flag** list, select **SUFFICIENT**.

12. Click **Save**.

13. Select the **Provider Specific** tab to display it.

14. In the Connection section, do the following:

    a. In the **Host** field, enter the IP address of the host.

    b. In the **Port** field, enter the relevant port number.

    c. In the **Principal** field, enter the value for the principal.

    d. In the **Credentials** field, enter the relevant credentials.

    e. In the **Confirm Credentials** field, enter the credentials again.

15. In the Users section, do the following:

    a. In the **User Base DN** field, provide a value, like the one shown here:

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

    b. In the **All User Filter** field, provide the relevant value.

    c. In the **User From Name Filter** field, provide the relevant value.

    d. In the **User Search Scope** field, provide the relevant value.

    e. In the **User Name Attribute** field, provide the relevant value.

    f. In the **User Object Class** field, provide the relevant value.

16. In the Groups section, do the following:

a. In the **Group Base DN** field, provide a value, like the one shown here:

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

b. In the **All Groups Filter** field, provide the relevant value.

c. In the **Group From Name Filter** field, provide the relevant value.

d. In the **Group Search Scope** field, provide the relevant value.

e. In the **Group Membership Searching** field, provide the relevant value.

f. In the **Max Group Membership Search Level** field, provide the relevant value.

17. Click **Save**.
18. Restart the WebLogic server.

To reorder the authentication providers:

1. Log in to the WebLogic Administration console.
2. In the Home page, select **Security Realms**.

   The Summary of Security Realms screen appears.
3. Select *YourRealm*.

   The Setting for *YourRealm* screen appears.
4. Select the **Providers** tab to display it.

   The Authentication tab is displayed by default. If not, then select to display it.
5. Click **Reorder**.

   The Reorder Authentication Providers screen appears.
6. Use and Up and Down arrows to the right of the Authentication Providers table to reorder them.
7. Click **OK**.

Authentication

Authentication verifies that you are who you claim to be. Network Integrity requires authentication by user name and password before allowing any user access to the application. User name and password are required for access to the application home page or via direct URL to a specific work area.

> **Note:**
>
> Failed login attempts are recorded within the USERLOGIN table in the Network Integrity database schema.

The login page is configured to not allow auto-completion of user names and passwords. Password text is not echoed to the field as you type. If you enter an invalid user name or password, an error message is displayed.

By default, you manage user names and passwords in the WebLogic Server Administration Console. You can choose to use another application to manage user security. The actual authentication process is performed by the Default Authentication provider or the

authentication provider provided by the chosen LDAP. The WebLogic Server Administration Console uses the embedded LDAP by default.

Password requirements are determined by the authentication provider. In the case of the WebLogic Server Embedded LDAP, passwords must be a minimum of eight characters and include at least one numerical and one alphabetic character. Password expiration policies are also determined by the authentication provider.

You can create groups that include similar users. Grouping users makes it easier to set up authorization. You can assign a group to a role, which automatically grants all permissions associated with the role to all members of the group.

See the WebLogic Server Administration Console documentation and Help for information about creating, deleting, and managing users, groups, and passwords.

To grant access to individual pages and actions in Network Integrity, you associate users and groups with security roles, which are in turn associated with security policies. See "Authorization" for more information.

About Network Integrity User Passwords

You manage Network Integrity user passwords using the Oracle WebLogic Administration Console.

Changing the Network Integrity User Password

You can change a Network Integrity user password in Network Integrity if you are using the Embedded LDAP (provided by Oracle WebLogic).

You can also change the user password using the Oracle WebLogic Administration Console. See Oracle Fusion Middleware Administration Console Online Help for Oracle WebLogic Server for more information.

For information on changing application user passwords when you are using an external security provider, see the respective product documentation.

To change the logged-in user password in Network Integrity:

1. Log in to the Network Integrity application.

   The Manage Scans screen appears.

2. In the Links section in the left pane, select **Change Password**.

   The Change Password screen appears.

   You can see the user name for the account for which you are changing the password.

3. Do the following:

   a. In the **Current Password** field, enter the current password for this user account.

   b. In the **New Password** field, enter the new password to which to want to change the password.

   c. In the **Verify New Password** field, enter the new password again.

   d. Click **Save and Close**.

      The password for this user is changed.

Changing the WebLogic Administrator Password

You can change the WebLogic administrator password using the WebLogic Administration Console. See Oracle Fusion Middleware Administration Console Online Help for Oracle WebLogic Server for more information.

Setting User Lockout Attributes

You set the user lockout attributes using the Oracle WebLogic Administration Console.

To set the user lockout attributes:

1. Log in to the Oracle WebLogic Server Administration Console as an administrator.

   The WebLogic Administration Console Home appears.
2. In the Change Center on the left, click **Lock & Edit**.
3. Select **Security Realms** under Your Application's Security Settings.

   The Summary of Security Realms screen appears.
4. In the Realms table, select *YourRealm*.

   The Settings for *YourRealm* screen appears.
5. In the Configuration tab, select the **User Lockout** tab to display it.
6. Do the following:
   a. Select **Lockout Enabled** to enable user lockout.
   b. In the **Lockout Threshold**, enter a value for the maximum number of consecutive invalid login attempts that can occur before a user's account is locked out.
   c. In the **Lockout Duration** field, enter the value for the user lockout duration, which is the number of minutes that a user's account is locked out.
   d. In the **Lockout Reset Duration** field, enter the value, in minutes, for the duration within which consecutive invalid login attempts cause a user's account to be locked out. The user is not locked out if the lockout threshold is not reached in this duration.
   e. In the **Lockout Cache Size** field, enter a value for the number of invalid login records (between 0 and 99999) that the server places in a cache.
   f. In the **Lockout GC Threshold** field, enter the value for the maximum number of invalid login records that the server keeps in memory.
7. Click **Save**.
8. In the Change Center of the Administration Console, click **Activate Changes**.
9. Restart WebLogic Server.

   User lockout attributes are set.

Unlocking User Accounts

To unlock a user account:

1. Log in to the Oracle WebLogic Server Administration Console as an administrator.

   The WebLogic Administration Console Home appears.
2. In the Change Center on the left, click **Lock & Edit**.

3. In the left pane, select *YourDomain*.

   The Settings for *YourDomain* screen appears.

4. Select the **Security** tab to display it, then select and display the **Unlock User** tab.
5. In the **Unlock User** field, enter the name of the user to be unlocked.
6. Click **Save**.
7. In the Change Center of the Administration Console, click **Activate Changes**.

   The specified user is unlocked.

Authorization

Authorization determines whether an authenticated user has permission to view a work area or to take action. For example, if an authenticated user does not have permission to view or edit scan information, the link to the Manage Scans work area does not appear in the Tasks panel of the Network Integrity home page.

There are two types of authorization in Network Integrity:

- **Taskflow** authorization controls the ability to view work areas, such as the Manage Scans work area. See Table 2-2 for a complete list.
- **Resource** authorization controls the ability to take actions, such as creating or deleting a scan. These actions are triggered by clicking a button or making selections from the Actions menu. See Table 2-3 for a complete list.

Users are granted permissions by their assignment to security roles and security policies.

- Security roles define groups of users that require particular kinds of access. For example, you can define a role for users who must be able to view but not edit scan information. You could define another role for users who need to be able to make changes to scan information.
- Security policies are groups of permissions that grant access to pages and actions. You associate security roles to security policies to define the access granted to users who are assigned to those roles. For example, to grant view access for scans, you can create a policy that includes permissions to view the manage scans page.

You use Oracle Enterprise Manager (or another system of your choice) to manage roles and policies for Network Integrity. Changes you make are applied immediately without the need to restart the server. User permission changes require that the user log out and log in again.

Using Security Roles

You create security roles that define the access levels appropriate for users performing particular functions. You can create as many roles as you need and you can assign as many or as few roles to a user as is necessary.

The actual permissions associated with any role are the result of the role being associated with security policies. Each policy defines access to a work area or action. See "Using Security Policies" for more information.

The default role, **NetworkIntegrityRole**, grants users complete access to all work areas and actions. In some cases, such as in testing or development environments, this may be the only role that is required.

See "Configuring Role-Based Access Control for Network Integrity" for more information.

Configuring Role-Based Access Control for Network Integrity

Network Integrity allows you to manage user access using roles and policies. Roles enable and control access to pages within Network Integrity. You can assign users when you create roles. You can also update existing roles by adding and removing users. Policies enable and control permissions on pages within Network Integrity. You use Oracle Enterprise Manager to create and manage users, groups, security roles, and security policies. You can also use Oracle WebLogic Administration console to create and manage users and groups.

Role-based access control configuration tasks include:

- Creating a User
- Configuring a Role
- Assigning Policies to a Role

The following procedure provides only the basic steps to create and associate users to groups, roles, and policies. See Oracle Fusion Middleware Administration Console Online Help for Oracle WebLogic Server for more information.

Creating a User

To create a user:

1. Launch the Oracle Fusion Middleware Control Enterprise Manager by entering the following in a Web browser:

   `http://ServerName:Port/em`

   where *ServerName* is the name of the Administration Server machine and *Port* is the Administration Server port number.
2. Enter the WebLogic server administration user name and password.
3. Navigate to **WebLogic Domain**, then **Security**, and then **Users and Groups**.

   The User and Groups page appears.
4. On the **Users** tab, click **Create**.

   The Create a New User page appears.
5. Enter the required information in the **Name**, **Description**, **Password**, **Confirm Password** fields; from the **Provider** list, select a value, and then click **Create**.

   A confirmation message appears on the Users and Groups page, informing you that the user has been created successfully.
6. Click the newly created user.

   The Setting for User page appears.
7. Click the **Groups** tab.
8. In the **Available** list, select **NetworkIntegrityRole** and **JDGroup** and click the single right arrow button to move both groups to the **Chosen** list.
9. Click **Save**.

   A confirmation message appears informing you that the settings have been updated successfully.

Configuring a Role

To configure a role:

1. Log in to Fusion Middleware Control Enterprise Manager.
2. Navigate to **WebLogic Domain**, then **Security**, and then **Application Roles**.

   The Application Roles page appears.
3. From the **Application Stripe** list, select **Network Integrity**, and then click **Create**.

   The Create Application Role page appears.
4. In the **Role Name** field, enter a name for the role.
5. In the **Display Name** field, enter a display name.
6. Click **Add**.

   The Add Principal page appears.
7. From the **Type** list, select **User**, and then click search (blue button with a green arrow).

   The Searched Principals section displays the list of users.
8. Select the users to whom you want to assign the role and click **OK**.
9. On the Create Application Role page, click **OK**.

Assigning Policies to a Role

To assign policies to a role:

1. Log in to Fusion Middleware Control Enterprise Manager.
2. Navigate to **WebLogic Domain**, then **Security**, and then **Application Policies**.

   The Application Policies page appears.
3. From the **Application Stripe** list, select **Network Integrity**.
4. From the **Principal Type** list, select **Application Role**, and then click the search button.

   The list of roles is displayed at the bottom of the page.
5. Select **NetworkIntegrityRole** and click **Create Like**.

   The Create Application Grant Like Grant To: NetworkIntegrityRole page appears.
6. Click **Add**.

   The Add Principal page appears.
7. From the **Type** list, select **Application Role**, and then click the search button.

   The Searched Principals section displays the list of roles.
8. Select the roles to which you want to assign the permissions and click **OK**.

   On the Create Application Grant Like Grant To: NetworkIntegrityRole page, under the Permissions section, all the permissions are listed because you are creating a role like the **NetworkIntegrityRole**.
9. (Optional) Select the permissions that you do not want to be assigned to the newly created role and click **Delete**.

> **Note:**
>
> You can delete only one permission at a time.

10. Click **OK**.

    The permissions are assigned to the role.

Using Security Policies

You use security policies to associate specific permissions, such as the ability to view the Scan Results work area or make changes to Scans, with roles. Policies are groupings of specific permissions that you grant to users assigned to roles.

It is possible to associate policies directly with users, but using roles reduces duplicative work and is therefore recommended.

Because there are separate permissions for each work area and for the ability to make changes on those work areas, there are a large number of specific permissions that can be assigned. As a result, you can tailor policies to grant exactly the permissions required for a role.

For example, suppose you have two roles associated with Scans. One role (Scan_View) is associated with a policy that includes permissions for viewing Scans information. Another role (Scan_Admin) is associated with a policy that includes those same permissions as well as permission to edit Scan information.

You use Oracle Enterprise Manager to manage policies. To create policies, you combine the permissions that apply to a role and then associate those permissions to a role.

The Oracle Enterprise Manager Application Policies page lists all the policies defined for the application, including the policies for the default NetworkIntegrityRole role.

See the Oracle Enterprise Manager Documentation and online Help for detailed information about working with policies.

Changing Security Policy Providers

By default, Oracle Enterprise Manager uses an XML file as the security policy store. This file, *Domain_Home***/config/fmwconfig/system-jazn-data.xml**, is installed automatically when you install Network Integrity.

You can configure Oracle Enterprise Manager to use a different policy store instead of the default XML file. For example, you may have a pre-existing LDAP server that you want to use for this purpose.

You specify the security policy store in the Enterprise Manager Security Provider Configuration page. See Oracle Enterprise Manager Administration and related documentation for detailed instructions.

User Permissions

Table 2-2 lists the Network Integrity taskflow permissions.

Table 2-2 Network Integrity Taskflow Permissions

Component	Permission String	Access
Review discrepancies	/WEB-INF/oracle/communications/integrity/ui/flow/discrepancies-flow-definition.xml#discrepancies-flow-definition	Allow access to the Review Discrepancies page
Display scan results	/WEB-INF/oracle/communications/integrity/ui/flow/scanrun-flow.xml#scanrun-flow	Allow access to the Display Scan Results page
Manage scans	/WEB-INF/oracle/communications/integrity/ui/flow/Local-Region-Task-Flow.xml#Local-Region-Task-Flow	Allow access to the Manage Scans page
Manage tags	/WEB-INF/oracle/communications/integrity/ui/flow/tags-flow.xml#tags-flow	Allow access to the Manage Tags page
Manage blackout windows	/WEB-INF/oracle/communications/integrity/ui/flow/blackout-flow-definition.xml#blackout-flow-definition	Allow access to the Manage Blackout Windows page
Manage import system	/WEB-INF/oracle/communications/integrity/ui/flow/manage-inventory-flow.xml#manage-inventory-flow	Allow access to the Manage Import System page

Table 2-3 lists the Network Integrity resource permissions.

Table 2-3 Network Integrity Resource Permissions

Component	Type	Permission Name	Use
Scans	Button, menu, right-click	Scan.CREATE	Create a scan from Manage Scans work area
Scans	Button, menu, right-click	Scan.EDIT	Edit a scan from Manage Scans work area
Scans	Button, menu, right-click	Scan.DELETE	Delete a scan from Manage Scans work area
Scans	Button, menu, right-click	Scan.START	Start a scan
Scans	Menu, right-click	Scan.STOP	Stop a scan
Scans	Menu, right-click	Scan.ENABLE	Enable a scan
Scans	Menu, right-click	Scan.DISABLE	Disable a scan
Scan Results	Right-click	ScanRun.DELETE	Delete a Scan Run or Scan Result
Import System	Button	Import.CREATE	Create an Import System
Import System	Button	Import.EDIT	Edit an Import System
Import System	Button	Import.DELETE	Delete an Import System
Blackout	Button, right-click	Blackout.CREATE	Create a Blackout Window
Blackout	Button, right-click	Blackout.EDIT	Edit a Blackout Window
Blackout	Button, right-click	Blackout.DELETE	Delete a Blackout Window
Tags	Button, right-click	Tags.CREATE	Create a Tag
Tags	Button, right-click	Tags.EDIT	Edit a Tag
Tags	Button, right-click	Tags.DELETE	Delete a Tag
Discrepancies	Menu, right-click	Discrepancies.CORRECT	Correct Discrepancies
Discrepancies	Menu, right-click	Discrepancies.IGNORE	Ignore Discrepancies
Discrepancies	Menu, right-click	Discrepancies.CANCELRESOLUTION	Cancel Resolution
Discrepancies	Menu, right-click	Discrepancies.EDIT	Edit Discrepancies

Table 2-3 (Cont.) Network Integrity Resource Permissions

Component	Type	Permission Name	Use
Discrepancies	Button	Discrepancies.SUBMIT	Submit Discrepancies

Working with the Application Role

You manage Application Roles using the Enterprise Manager Console. Oracle recommends backing up the **system-jaxn-data.xml** file in the *Domain_Home***/config/fmwconfig/** directory before making any changes to Application Roles.

All the changes made to Application Roles will be in effect immediately, without restarting the application server.

Oracle recommends not making any changes to the NetworkIntegrityRole role and its policies.

If you want to provide restricted access to a user then create a new Application Role, add policies to be allowed and assign user to that Application Role.

See Oracle Enterprise Manager Administration for information about working with Application Roles.

Working with the Application Policy

You manage Application Policies using the Enterprise Manager Console. Oracle recommends backing up the **system-jaxn-data.xml** file in the *Domain_Home***/config/fmwconfig/** directory before making any changes to Application Policies.

All the changes made to Application Policies will be in effect immediately, without restarting the application server.

See Oracle Enterprise Manager Administration for information about working with Application Policies.

Encrypting Properties

Properties can be encrypted so that they can be configured as Secret properties in a property group on a processor. Properties can be configured to have secret values to pass sensitive information in Network Integrity. See Network Integrity Developer's Guide for more information.

Before running the encryption, create the property. See Network Integrity Developer's Guide for more information.

To encrypt a property:

1. On the system where Network Integrity is installed, go to *NI_Home***/integrity**.

   Where *NI_Home* is the directory where Network Integrity is installed.
2. Run the property encryption tool by running the following command:

   ```
   ./runPropertyEncryptor.sh
   ```
3. At the prompt, enter the name of the property.
4. At the prompt, enter the property value.
5. At the prompt, confirm the property value.

The encrypted property value is displayed.

6. Enter the encrypted value as the property value using the MBean interface at deployment time.

Encrypt Decrypt Utility

In Network Integrity, a scan parameter group is modeled as an *attribute/characteristic* set, wherein an attribute is a *name/value* pair. These values can be sensitive data, such as passwords. Therefore, all values stored in the database are encrypted. It is not possible to see stored passwords in plain text either in the UI or in the database. The *EncryptDecryptUtil.jar* utility provides support for the encryption of any input value. An administrator can use this utility to perform necessary actions.

To use this utility:

1. On the system where Network Integrity is installed, go to **NI_Home/integrity**.
2. Run the Encrypt Decrypt tool from the WebLogic domain by running the following command:

   ```
   ./runEncryptDecryptUtil.sh
   ```

3. At the prompt, provide the database details of NI where the application data is stored.
4. At the prompt, provide the operation you want to perform (ex: ENCRYPT).
5. At the prompt, enter the input value to be encrypted or decrypted.
6. Once the details are entered successfully, the utility connects to the database and prints the output text.

> **Note:**
>
> By default, the script points to the JRE path that is used during NI application installer. Please update the JRE path if in case it has changed later.

3
Monitoring Network Integrity

This chapter describes procedures related to checking and monitoring the processes running on Oracle Communications Network Integrity.

The chapter also provides information about the tools that you use to check and monitor Network Integrity; and to maintain a historical view of application activity.

About Monitoring Tools

This section describes tools to monitor the following components:

- **JVM**

  Use **JVisualVM** when you are working with the Sun Hotspot JVM for monitoring the heap size, garbage collection, and CPU usage of the application server. For more information, see the JVisualVM documentation at the following location:

  `http://download.oracle.com/javase/6/docs/technotes/tools/share/jvisualvm.html`

- **Database**

  To monitor and manage the Network Integrity database, it is recommended to use Oracle Enterprise Manager. With the Grid Control version of this product, you can also monitor the performance of the application servers and host systems in your Network Integrity installation. See Oracle Enterprise Manager Concepts for more information.

  > **Note:**
  >
  > The AWR (Automatic Workload Repository) reports and ADDM (Automatic Database Diagnostic Monitor) features included in Oracle Enterprise Manager are particularly useful in helping to identify and correct any performance issues or bottlenecks in the database.

- **Operating System**

  To monitor the operating system of your Network Integrity application servers and database servers, you can use any or all of the following Unix/Linux tools and commands:

  - `iostat` for disk activity statistics
  - `mpstat` for CPU statistics
  - `netstat` for TCP/IP network connections and protocol statistics
  - `ps` for CPU consumption, memory size, execution time, and so on, of individual processes
  - `top` for load averages, CPU and memory usage of the whole system and the top consuming processes
  - `vmstat` for virtual memory statistics

Monitoring Network Integrity

Regular monitoring of your system ensures fast recognition and resolution of any problems or issues. Among other things, monitoring the Network Integrity system involves monitoring the general health and performance of Network Integrity and monitoring the Oracle WebLogic server domain and servers.

Viewing General Health and Performance of Network Integrity

To view general application-related information for Network Integrity:

1. Log on to the Enterprise Manager console using the administrator's credentials.

   The *Farm* screen appears.

2. Expand **Application Deployments** in the left pane, and select **NetworkIntegrity**.

   The NetworkIntegrity screen appears.

   You can view the following information about the Network Integrity application:

   - Summary information
   - Modules currently deployed
   - Entry Points descriptions
   - Graph showing response and load time for requests
   - Most requested services and requests.

Monitoring an Oracle WebLogic Server Domain

You can monitor a domain and its health using the Enterprise Manager Console. To monitor the domain's health, refer to:

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

To monitor an Oracle WebLogic server domain:

1. Log in to the Enterprise Manager console using the administrator's credentials.

   The *Farm* screen appears.

2. Expand **WebLogic Domain** in the left pane and select the domain, *DomainName*, you want to monitor.

   The *DomainName* screen appears.

   You can view general information about the selected WebLogic domain.

Monitoring an Oracle WebLogic Administration or Managed Server

A server is any combination of hardware or software designed to provide services to clients. When used alone, the term typically refers to a computer which may be running a server operating system. Commonly used, the term refers to any software or dedicated hardware capable of providing any given services.

For information on monitoring servers using the Enterprise Manager, see the Oracle Enterprise Manager guide located at the following link:

http://www.oracle.com/technology

For any server you can monitor the following:

- General run time information
- Server health
- Server channels
- Server performance
- Garbage collection pause time
- Server threads: Thread activity for the current server
- Executing queues: You configure the server to use executing queues
- Security: Monitor user lockout management statistics for a server
- Default store statistics: View run-time statistics for the default store for the server
- Default store connections: View run-time statistics for all of the active default store connections
- JMS connections: Monitor statistics on all the active JMS connections on your server
- SAF agents: Monitor statistics on all the active SAF agents on your server
- JDBC data source: Monitor the activity of the data source (displays statistics associated with this JDBC data source)
- JTA transactions summary: Monitor the summary of all transaction information for all resource types on the server
- JTA, transactions by name: Monitor statistics about named transactions coordinated by the server
- JTA, XA resources: Monitor statistics about transactions coordinated by the server for each transactional (XA) resource accessed by the server
- JTA, non-XA resources: Monitor information about transactions in which non-XA resources on the server participate
- JTA transactions: Monitor information about current transactions coordinated by the server or in which server resources participate
- JTA recovery services: Monitor information about transactions that were processed by the server as part of recovery on server startup or after a failure
- Workload: View statistics for the Work Managers, constraints, and request classes that are configured for this server
- Timers: Monitor information about the timers used by a server

Monitoring Logging Levels

You should monitor the application server log files regularly to ensure that there are no exceptions that would indicate problems with the Network Integrity system.

Monitoring a Cluster

A cluster is a group of linked computers working so that they virtually form one system. The components of a cluster are commonly, but not always, connected to each other through fast local area networks (LAN). Clusters are usually deployed to improve performance or

availability over that of a single computer, while typically being much more cost-effective than single computers of comparable speed or availability.

You can monitor clusters using the Oracle WebLogic Server Administration Console. To monitor the run-time status of clusters that are part of the current WebLogic Server domain, perform the steps documented at the Oracle Technology Network web site.

Monitoring Configured Schedule Events

If you redeploy the Network Integrity application for any reason, the Network Integrity application tracks the configured schedule events by comparing the active timers with the persistent schedule database records and creates the timers accordingly.

Network Integrity logs error messages if the container active timers conflict with the persisted schedule records. The Network Integrity administrator must monitor error messages related to the additional active timers and create a new schedule if the error messages are valid.

About Oracle Diagnostic Logging

The Oracle Diagnostic Logging framework, or ODL, provides plug-in components that complement the standard Java framework to automatically integrate log data with Oracle log analysis tools. In the ODL framework, log files are formatted in XML, enabling them to be more easily parsed and reused by other Oracle Application Server and custom developed components.

The ODL framework provides support for managing log files, including log file rotation. You can also define the maximum log file size and the maximum size of log directories.

You can view ODL-formatted log files through the web-based Oracle Enterprise Manager console. Using the Enterprise Manager you can aggregate and view the logging output generated by all components and applications running within OC4J from one centralized location.

For information on WebLogic server related log files, see the Oracle Fusion Middleware Administrator's Guide.

About Java Logging and ODL

In the Java logging framework, applications record events by making calls on Logger objects, which are instances of the `java.util.logging.Logger` class. A Logger is a named entity that is associated with a system or application component. Each Logger is assigned a specific log level, and records events only at that level of severity or higher.

Logging messages are forwarded to a Handler object, which can in turn forward the messages to a variety of destinations for publication. The `oracle.core.ojdl.logging` package includes a Handler class, ODLHandler class, which generates the Logger output in XML-based ODL format.

Configuring the Network Integrity Log File

Enabling Java Loggers to output log messages in the ODL format is accomplished by mapping each Logger to the ODLHandler. This mapping is managed through a logging configuration file, **logging.xml**, which is generated by server in the **DefaultDomain/config/fmwconfig/servers/DefaultServer** directory.

For Network Integrity, all log files are managed and configured using the **logging.xml** file.

To manage logging for Network Integrity, configure the following two elements, or tags, within the `logging-configuration` root element of the **logging.xml** file:

- **Log handlers**

  This element includes `log_handler` elements defining three different log handlers:

  – OC4J-handler

    This is the log handler for the Oracle logger.

  – oracle-webservices-management-auditing-handler

    This is the log handler for the **oracle.webservices.management.auditing** logger.

  – oracle-webservices-management-logging-handler

    This is the log handler for the **oracle.webservices.management.logging** logger.

  The following properties are specified in `property` sub-elements for each log handler:

  – Path

    Specifies the directory in which the handler generates log files.

    > **Caution:**
    >
    > Oracle recommends that you do not modify this value.

  – MaxFileSize

    Sets the maximum size, in bytes, for any log file in the directory. When a file exceeds this limit, a new file is generated.

  – MaxLogSize

    Sets the maximum size, in bytes, for the log file directory. When this limit is exceeded, log files are purged, beginning with the oldest files.

- **Loggers**

  This element includes a `logger` element defining the following parameters:

  – Name

    The Logger name.

    > **Caution:**
    >
    > Oracle recommends that you do not modify this value.

  – Level

    This specifies the minimum log level that this logger acts upon. This level is set by default to the `ODL NOTIFICATION:1` value, which maps to the INFO Java log level displayed on the Logger Configuration page in the Oracle Enterprise Manager console.

    Oracle recommends to not use FINE or lower logging levels for Network Integrity, because the logs could contain messages and stack traces that could pose a security risk to the system. See Network Integrity Security Guide for more information. By default, WebLogic Server uses a higher log level for Network Integrity.

– useParentHandlers

  Indicates whether the logger should use its parent handlers. Because this value is set to `false` by default, the Oracle logger does not inherit the log level set for its parent, the root logger.

> **Note:**
>
> For some logs the handler is not mentioned. By default that log goes to **console-handler**.

In the following example the default log level is set to FINEST as the ODL Message Type: Log Level. This log level can be changed. Table 3-1 provides all other valid log levels.

```
<logging_configuration>
  <log_handlers>
   <log_handler name='NI-handler' class='oracle.core.ojdl.logging.ODLHandlerFactory'
filter='oracle.dfw.incident.IncidentDetectionLogFilter'>
    <property name='path' value='${domain.home}/servers/${weblogic.Name}/logs/$
{weblogic.Name}-diagnostic.log'/>
    <property name='maxFileSize' value='10485760'/>
    <property name='maxLogSize' value='104857600'/>
    <property name='encoding' value='UTF-8'/>
    <property name='useThreadName' value='true'/>
    <property name='supplementalAttributes'
value='J2EE_APP.name,J2EE_MODULE.name,WEBSERVICE.name,WEBSERVICE_PORT.name,composite_inst
ance_id,component_instance_id,composite_name,component_name'/>
    <property name='logreader:' value='off'/>
    <property name='format' value='ODL-Text'/>
    <property name='useThreadName' value='true'/>
    <property name='locale' value='en'/>
    <property name='encoding' value='UTF-8'/>
    <property name="baseRotationTime" value="04:00"/>
    <property name="rotationFrequency" value="daily"/>
   </log_handler>
  </log_handlers>

  <loggers>
   <logger name='oracle.communications.integrity.auditlog' level='FINEST'
useParentHandlers='false'>
    <handler name='NI-handler'/>
   <logger/>
  </loggers>
</logging_configuration>
```

Table 3-1 Valid Log Levels

Java Log Level	ODL Message Type:Log Level	ODL Description
NULL	N/A	The logger inherits the log level set for its parent.
SEVERE	ERROR:1	Log system errors requiring attention from the system administrator.
WARNING	WARNING:1	Log actions or conditions discovered that should be reviewed and may require action before an error occurs.

Table 3-1 (Cont.) Valid Log Levels

Java Log Level	ODL Message Type:Log Level	ODL Description
INFO	NOTIFICATION:1	Log normal actions or events. This could be a user operation, such as login completed, or an automatic operation, such as a log file rotation.
CONFIG	NOTIFICATION:16	Log configuration-related messages or problems.
FINE	TRACE:1	Log trace or debug messages used for debugging or performance monitoring. Typically contains detailed event data.
FINER	TRACE:16	Log fairly detailed trace or debug messages.
FINEST	TRACE:32	Log highly detailed trace or debug messages.

About ODL Log File Rotation and Naming

Using ODL, application server components write diagnostic log files to a logging directory (***domain.home*/servers/*weblogic.Name*/logs/*weblogic.Name*-diagnostic.log)** mentioned in the “path" property of the `log_handler` in the **logging.xml** file.

When the log file reaches the rotation point, it is renamed and a new log file, ***weblogic.Name*-diagnostic.log** is created.

> **Note:**
>
> You specify the rotation point by specifying the maxFileSize property of `log_handler` tag in the **logging.xml** file.

Segment files are created when the ODL log file ***weblogic.Name*-diagnostic.log** reaches the rotation point. That is, the ***weblogic.Name*-diagnostic.log** is renamed to ***weblogic.Name*-diagnostic.logn**, where **n** is an integer, and a new***weblogic.Name* -diagnostic.log** file is created when the component generates new diagnostic messages.

About Size-Based Rotation

To limit the size of the ODL log, components use maxLogSize property of the `log_handler` in the **logging.xml** configuration file. Whenever the sum of the sizes of all of the files in the log directory reaches the maximum, the oldest archive is deleted to keep the total size under the specified limit.

For example, when the maximum directory size is reached, with the starting segment file named log9872, the following files could be present in the log file directory:

Table 3-2 Log File Directory Files

File	Size
log.log	10002
log.log9872	15000

Table 3-2 (Cont.) Log File Directory Files

File	Size
log.log9873	15000
log.log9874	15000
log.log9875	15000
log.log9876	15000

In this case, when **log.log** fills up, **log.log9872** is removed and **log.log** is moved to the new file **log.log9877**. New diagnostic messages reuse **log.log**.

About Time-Based Rotation

For time-based rotation, you specify the following properties in the `log_handler` element in logging.xml configuration file:

- baseRotationTime (Optional)

  The base time for the rotation. The format for the base time can be any of the following:

  - hh:mm, for example, 04:20. This format uses the local time zone.
  - yyyy-MM-dd, for example, 2006-08-01. This format uses the local time zone.
  - yyyy-MM-ddThh:mm, for example 2006-08-01T04:20. This format uses the local time zone.
  - yyyy-MM-ddThh:mm:ss.sTZD, where TZD is the time zone indicator. TZD can be Z, indicating UTC, or {+|-}hh:mm. For example, 2006-03-01T04:20:00-08:00 represents March 1, 2006 4:20:00 in US Pacific Standard Time time zone.

  > **Note:**
  >
  > If you do not specify baseRotationTime, the default value is Jan. 1, 1970, 00:00 UTC.

- rotationFrequency

  The frequency of the rotation, in minutes. In addition, you can specify one of the following values: hourly, daily, weekly.

  For example, to specify that the log files are rotated every day at 4:00AM local time, or when they reach 2000000 bytes, use the following:

```
<log_handler name="h1" class="oracle.core.ojdl.logging.ODLHandlerFactory">
     <property name="path" value="log"/>
     <property name="baseRotationTime" value="04:00"/>
     <property name="rotationFrequency" value="daily"/>
     <property name="maxFileSize" value=" 2000000"/> </log_handler>
```

About Logs in a Clustered Environment

In the clustered environment every server has its own configuration file **logging.xml**.

Searching for and Viewing Log Files

You can view ODL-formatted log files using the web-based Oracle Enterprise Manager console.

To search for the log messages:

1. Log in to the Enterprise manager.

   The start page of your farm appears.
2. In the left pane, expand **WebLogic Domain**.
3. Select the *DomainName* for your domain to expand it.
4. Right-click the *ServerName* of the server for which you want to view the logs, under the domain where the server exists, select **Logs**, then select **View Log Messages**.

   The Log Messages screen for *ServerName* appears.
5. Do the following:
   a. From the **Date Range** list, select the appropriate value and enter the time value for which you want to view the logs in the corresponding fields.
   b. Select the appropriate **Message Type** for your search.
   c. From the **Message** list, select the appropriate option and enter the keywords in the corresponding box.
   d. (Optional) Click **Add Fields** to make your search specific.
   e. Click **Search**.

      The log messages are displayed.

Log Configuration using Fusion Middleware Enterprise Manager Console

The system administrator can create or edit log handlers and modify the logger levels using the Enterprise Manager console. Refer to "Configuring Settings for Log Files" in the *Oracle Fusion Middleware Administrator's Guide 11g Release 1* for more details.

4

Managing Network Integrity and Its Components

This chapter provides information on managing Oracle Communications Network Integrity, and Network Integrity components.

About Managing the Oracle Database Server

To manage the Oracle Database server, see the Oracle Database administrator's guide on the Oracle Technology Network web site:

http://www.oracle.com/technology

Perform all required administration tasks for the database.

About Managing Network Integrity

This section explains how to perform various Network Integrity management tasks.

Starting Network Integrity Instances

To start a Network Integrity instance:

1. Ensure that the server hosting Network Integrity is running.
2. Log in to the WebLogic server Administration console using Administrator credentials.

   The Home screen appears.
3. Click **Configure applications**.

   The Summary of Deployments screen appears.
4. In the Deployments table, select the check box corresponding to the Network Integrity instance.
5. On the **Start** drop-down menu, select the appropriate option.

Stopping Network Integrity Instances

To stop a Network Integrity instance:

1. Ensure that the server hosting Network Integrity is running.
2. Log in to the WebLogic server Administration console using Administrator credentials.

   The Home screen appears.
3. Click **Configure applications**.

   The Summary of Deployments screen appears.
4. In the Deployments table, select the check box corresponding to the Network Integrity instance.

5. On the **Stop** drop-down menu, select the appropriate option.

Starting and Stopping the Reporting Tool

> **Note:**
>
> Before starting or stopping the reporting tool using the WebLogic Administration console, ensure that the server hosting the reporting tool is running.

To start or stop a deployed reporting tool:

1. Log in to the WebLogic server Administration console using Administrator credentials.

   The Home screen appears.
2. Select **Deployments** under Your Deployed Resources.

   The Summary of Deployments screen appears.
3. In the Deployments table, select the check box corresponding to the Reporting tool.
4. Do one of the following:
   - To start the reporting tool, click **Start**.
   - To stop the reporting tool, click **Stop**.
5. Select the required options.

Starting and Stopping the WebLogic Administration Server

To start or stop the WebLogic server on which Network Integrity is installed:

1. Log in to the Linux system on which Network Integrity is installed.
2. Open the Console window.
3. Go to the *Domain_Home*/**bin** folder
4. Do one of the following:
   - To start the WebLogic server

     ```
     . startWebLogic.sh
     ```
   - To stop the WebLogic server

     ```
     . stopWebLogic.sh
     ```

Starting and Stopping a Managed Server

You can use the WebLogic scripting and command line tool to start or stop a Managed WebLogic server.

To start a Managed WebLogic server:

1. Run the following script:

   ```
   MW_Home/user_projects/domains/domain_name/bin/startManagedWebLogic.sh
   managed_server_name admin_url
   ```

where:

- *MW_Home* is the location where Fusion Middleware products (such as WebLogic Server) are installed.
- *domain_name* is the name of the domain.
- *managed_server_name* is the name of the managed server being started.
- *admin_url* is the URL for the managed server being started.

2. At the prompt, provide your user name and password.

   The managed server starts.

To stop a Managed WebLogic server:

1. Run the following script:

   ```
   MW_Home/user_projects/domains/domain_name/bin/stopManagedWebLogic.sh
   managed_server_name admin_url user_name password
   ```

   where:

   - *MW_Home* is the location where Fusion Middleware products (such as WebLogic Server) are installed.
   - *domain_name* is the name of the domain.
   - *managed_server_name* is the name of the managed server being stopped.
   - *admin_url* is the URL for the managed server being stopped.

2. At the prompt, provide your user name and password.

   The managed server starts.

Adding Additional Managed Servers to a WebLogic Domain

You add additional managed servers to an existing cluster to increase the capacity and performance of your system.

> **Note:**
>
> If you add new member servers to an existing cluster, the new member servers inherit all applications and services targeted to that cluster.

To add a managed server to a domain:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.

   The Home screen appears.

2. In the Change Center, click **Lock & Edit**.
3. Under Environment, select **Servers**.

   The Summary of Servers screen appears.

   The **Configuration** tab is displayed by default.

4. Click **New**.

   The Create a New Server screen appears.

5. Do the following:
   a. In the **Server Name** field, enter a name for the new server.
   b. In the **Server Listen Address** field, enter the IP address of the host system.
   c. In the **Server Listen Port** field, enter the port number from which to access the server.
   d. Select whether this server is a member of an existing cluster.
   e. Click **Next**.

      The Review Choices page of the Create a New Server screen appears.
   f. Review the information and click **Finish**.

      The new server appears in the Servers table.

Creating a Cluster

A WebLogic server cluster is a group of multiple WebLogic servers, called member servers, working as one large server, thereby increasing the capacity, performance, and reliability of your system. The member servers can either be on the same, or different systems.

> **Note:**
>
> Each member server in a cluster must run the same version of WebLogic Server.

To create a cluster:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.

   The Home screen appears.
2. In the Change Center, click **Lock & Edit**.
3. Under Environment, select **Clusters**.

   The Summary of Clusters screen appears.
4. Click **New**.

   The Create a New Cluster screen appears.
5. Do the following:
   a. In the **Name** field, enter a name for the new cluster.
   b. From the **Messaging Mode** list, choose the messaging mode for the cluster.

      Oracle Recommends that you use **Multicast** messaging.
   c. Configure the messaging mode settings:

      For Unicast messaging, in the Unicast Broadcast Channel field, enter the channel that is used to transmit messages within the cluster.

      For Multicast messaging:

      - In the Multicast Address field, provide the multicast address that the cluster members use to communicate with each other.
      - In the Multicast port field, provide the multicast port (between 1 and 65535) that the cluster members use to communicate with each other.

d. Click **OK**.

   The newly created cluster is in the Clusters table.

   You can now add member servers to this cluster.

Adding Managed Servers to an Existing Cluster

To add a new managed server to an existing clustered environment:

1. Log in to the Oracle WebLogic Server Administration Console using the Administrator credentials.

   The Home screen appears.
2. In the Change Center, click **Lock & Edit**.
3. Under Environment, click **Servers**.

   The Summary of Servers page appears.
4. Click **New**.

   The Create a New Server page is displayed.
5. Do the following:
   a. In the **Server Name** field, enter the name for the new managed server.
   b. In the **Server Listen Address** field, enter the IP address of the managed server to add to the cluster.
   c. In the **Server Listen Port** field, enter the port number of the new managed server.
   d. Select **Yes, make this server member of existing cluster**.
6. Click **Next**, and then click **Finish**.
7. Click **Save**.
8. Enable SSL for the newly added managed server:
   a. Click **Domain**, and then select **Environments**.
   b. Click **Server,** and then select the new managed server.

      The Settings page for the new managed server is displayed.
   c. Click the **Configuration** tab, and then click the **General** tab.
   d. Select **SSL Listen Port Enabled** and assign a unique port in the **SSL Listen Port** field.
   e. Click **Save**, and then click **Release Lock**.

During Network Integrity installation, the installer creates JMS servers for each member server of the cluster. JMS servers and filestores are among the WebLogic entities that cannot be targeted to a cluster.

> **Note:**
>
> The pattern followed is *EntityName-N*, where *N* is greater than 0 but less than the number of member servers in the cluster. For example, for a cluster with two member servers, these entities are named **EntityName-0** and **EntityName-1**. Create JMS servers manually and target them to the newly added managed servers.

To manually create filestores for the added managed server:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.

   The Home screen appears.
2. In the Change Center, click **Lock & Edit**.
3. Click **Domain**, and then click **Services**.
4. Select **Persistent Stores New**, and then click **Create File Stores**.

   > **Note:**
   >
   > **Persistent Stores New** is the new persistent store.
5. Target the new file store to the newly created servers migratable target.
6. Set the directory attribute to `./`.
7. Create **JDJMSServer-M-1** using the new filestore as its persistent store.

   To manually create JMS server for the added managed server:

   a. Log in to the Oracle WebLogic Server Administration Console using the Administrator credentials.

      The Home screen of the Administration Console appears.

   b. Click **Lock & Edit**.

   c. Click **Domain**, and then click **Services**.

   d. Select **Messaging**, and then click **JMSServersNew**.

      > **Note:**
      >
      > **JMSServersNew** is the new JMS server.

   e. Change the target of JD sub-deployment to include the newly created JMS server migratable target.

   f. Click **Domain**, and then select **Services**.

   g. Click **JMS Modules**, and then select **(JDJMSModule)**.

   h. Click the **SubDeployments** tab.

   i. Select the new JMS server as the target.

   j. Click **Save**, and click **Release Lock**.

   k. Start the newly created managed server.

Changing the Listen Address to Network Integrity Servers

To change the listen address to Network Integrity servers:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.

   The Home screen appears.
2. Select **Servers** under Environment.

The Summary of Servers screen appears.

3. Click **Lock & Edit** in the Change Center in the left pane.
4. In the Servers table, click the Network Integrity server name. It could be the Administration, or managed server.

   The Settings for *ServerName* screen appears.

   The **General** tab is displayed by default.
5. In the **Listen Address** field, enter the IP address of the required administration or managed server.
6. Click **Save**.
7. Click **Release Lock**.
8. Restart the server.

Configuring the SSL Policy and SSL Certificate

This section describes the configuration of SSL with Oracle WebLogic.

To generate a new private key and self-signed certificate in the *WL_Home***/server/lib** directory:

1. Go to the **lib** directory of the Oracle WebLogic Server installation, and use the following keytool command with complete path of the keytool:

   ```
   Java_Home/bin/keytool -genkey -alias alias -keypass keypass -keystore keystore.jks -
   storepass keystorepass -keyalg RSA -keysize 2048
   ```

   where

   - *Java_Home* is the JDK installation directory
   - *alias* is the name
   - *keypass* is the password
   - *keystore*.jks is the key store name
   - *keystorepass* is the key store password

   > **Note:**
   >
   > -keyalg and -keysize are provided to support SSL for higher versions of jdk1_7.75.

2. At the **What is your first and last name?**, enter the application server host name.
3. Provide relevant information for the following prompts:
   a. **What is the name of your organizational unit?**
   b. **What is the name of your organization?**
   c. **What is the name of your City or Locality?**
   d. **What is the name of your State or Province?**
   e. **What is the two-letter country code for this unit?**

      A summary is displayed showing the information you entered, as shown in the example below:

Is CN=*HostNameProvided*, **OU=***OrganizationalUnit*, **O=***Organization*, **L=***Locality*, **ST=***State*, **C=***CountryCode* **correct?**

f. Enter **Yes**.

The **mykeystore.jks** is created.

You must configure the new self-signed certificate in the WebLogic Administration Console.

To configure the new self-signed certificate in the Administration Console:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.

   The Home screen appears.
2. Select **Servers** under Environment.

   The Summary of Servers screen appears.
3. In the Servers table, click **AdminServer**.

   The Settings for AdminServer screen appears.

   The **General** tab is displayed by default.
4. Select **SSL Listen Port Enabled**.
5. In the **SSL Listen Port** field, update the value as appropriate.
6. Click **Save**.
7. Click the **Keystores** tab.
8. From the **Keystores** list, select **Custom Identity and Java Standard Trust**.
9. Do the following:
   a. In the **Custom Identity Keystore** field, enter the full path to your JKS file as follows:

      *WL_Home***/server/lib/DemoIdentity.jks**
   b. In the **Custom Identity Keystore Type** field, enter **jks**.
   c. In the **Custom Identity Keystore Passphrase** field, enter the keystore password.
   d. Leave the Java standard trust key as the default.
   e. Click **Save**.
10. Click the **SSL** tab.
11. Do the following:
    a. From the **Identity and Trust Locations** list, select **Keystores**.
    b. In the **Private Key Alias** field, enter the alias name.
    c. In the **Private Key Passphrase** field, enter the private key password.
    d. Click **Advanced** to expand the Advanced section.
    e. From the **Hostname Verification** list, select **None**.
    f. From the **Two Way Client Cert Behavior** list, select **Client Certs Requested But Not Enforced**.
    g. Click **Save**.
12. Click **Activate Changes** in the Change Center in the left pane.

For more information on SSL configuration, refer to the Administration Console Help.

> **Note:**
>
> To replace a self-signed certificate with a production-quality certificate, or to import a trusted CA certificate into a keystore, run the following command:
>
> ```
> Keytool -import -alias alias -file cert.pem -keypass keypass -keystore
> keystore.jks -storepass keystorepass
> ```

> **Note:**
>
> If you import a trusted CA certificate, no existing entry for **alias** should be in the keystore.
>
> While accessing the application, the browser asks to install the certificate. Install the certificate in **Trusted Root Certification Authorities**.

Switching the Database Instances

Network Integrity has the following data sources:

- CMWSPersistentDS
- JobDispatcherDS
- JobDispatcherPersistentDS
- mds-commsNIRepository
- mds_owsm
- NIDatasource
- NIPersistentDS
- NIPomsPersistentDS

To change connection details for one or more data sources:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.

   The Home screen appears.
2. Under Services, select **JDBC**.

   The Summary of Services: JDBC screen appears.
3. In the **Section** column, click **Data Sources**.

   The Summary of JDBC Data Sources screen appears.
4. Click **Lock & Edit**.
5. In the Data Sources table, select a data source.

   The Settings screen appears for the selected data source.
6. Click the **Connection Pool** tab.
7. Do the following:
   a. In the **URL** field, enter the URL for the database JDBC.

b. In the **Properties** field, change database user name.

   For example, **user=niuser**.

c. In the **Password** field, enter the database user password.

d. In the **Confirm Password** field, enter the database user password again.

e. Click **Save**.

8. Click **Release Configuration**.
9. Restart all Network Integrity managed servers.

> **Note:**
>
> In case of Oracle Real Application Cluster (RAC) DB, you must create Multi datasources for each of the NI datasources mentioned above in the beginning of this section.

Configuring the JTA Transaction Timeout

To configure the JTA transaction timeout:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.

   The Home screen appears.

2. Under Services, select JTA.

   The Settings screen appears for the selected data source.

3. Click the **JTA** tab.
4. Click **Lock & Edit**.
5. In the **Timeout Seconds** field, enter the transaction timeout seconds for active transactions.
6. Click **Save**.
7. Click **Release Configuration**.
8. Restart all Network Integrity managed servers.

Configuring the Job Dispatcher Parameter for Timeout

A job refers to any of the following tasks:

- Discovery job
- Discrepancy job
- Resolution job
- Assimilation job
- Inventory import job

You specify a timeout value for these jobs and configure the Job Dispatcher parameters to maximize performance.

To configure the Job Dispatcher parameters for timeout:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.
   The Home screen appears.
2. Under Services, select **Messaging**.
   The Summary of Services: JMS screen appears.
3. Click **Lock & Edit**.
4. In the **Section** column, select **JMS Modules**.
   The **JMS Modules** screen appears.
5. In the JMS Modules table, click **JDJMSModule**.
   The Settings for JDJMSModule screen appears.
6. In the Summary of Resources table, click **JobQueue**.
   The Settings for JobQueue screen appears.
7. Click the **Overrides** tab.
8. In the **Time-to-Live Override** field, enter the value in milliseconds.
   This value applies to all job tasks.
9. Click **Save**.
10. Click **Release Configuration**.
11. Restart all Network Integrity servers.

Configuring the Timeout Parameter for Work Items

A work item is any single unit of a Network Integrity job.

For example, a work item for a Discovery job consists of scanning a single IP address.

To configure the timeout parameter for a work item:

1. Log in to the WebLogic server Administration Console using the Administrator credentials.
   The Home screen appears.
2. Under Services, select **Messaging**.
   The Summary of Services: JMS screen appears.
3. Click **Lock & Edit**.
4. In the **Section** column, select **JMS Modules**.
   The **JMS Modules** screen appears.
5. In the JMS Modules table, click **JDJMSModule**.
   The Settings for JDJMSModule screen appears.
6. In the Summary of Resources table, select **WorkItemQueue**.
   The Settings for WorkItemQueue screen appears.
7. Click the **Overrides** tab.
8. In the **Time-to-Live Override** field, enter the value in milliseconds.
   This value applies to all work items for all job tasks.
9. Click **Save**.

10. Click **Release Configuration**.
11. Restart all Network Integrity servers.

About Node Managers

For information on Node managers, and information on using a Node manager to control the starting and stopping of application managed servers, refer to *Node Manager Administrator's Guide*:

http://download.oracle.com/docs/cd/E12840_01/wls/docs103/nodemgr/overview.html

> **Caution:**
>
> For the Node manager **properties** file the `StartScriptEnabled` flag is enabled.
>
> Change the **nodemanager.properties** and ensure that the following property is changed to true (default is false) as shown:
>
> ```
> StartScriptEnabled=true
> ```

Using JMS File Store

By default, Network Integrity uses JDBC JMS stores. To configure the WebLogic server to use File JMS stores instead of JDBC HMS stores:

1. From the WebLogic server Administration Console, create the following filestores:
   - **CMWSPersistentFILEStore**
   - **JDPersistentFILEStore**
   - **NIPOMSPersistentFILEStore**
   - **NIPersistentFILEStore**

   Refer to your WebLogic Server documentation for more information.
2. Click **JMS Servers**.
3. Select each **CMWSJMSServer** and save the persistent store to **CMWSPersistentFILEStore**.
4. Select each **JDJMSServer** and save the persistent store to **JDPersistentFILEStore**.
5. Select each **NIPOMSJMSServer** and save the persistent store to **NIPOMSPersistentFILEStore**.
6. Select each **NIJMSServer** and save the persistent store to **NIPersistentFILEStore**.

> **Note:**
>
> In a clustered environment, there are multiple JMS servers of each type, for example: **CMWSJMSServer-0**, **CMWSJMSServer-1**, **CMWSJMSServer-2**, and so on.

Configuring JMS Auto Migration

JMS Auto Migration is configured as a pre-installation step to installing Network Integrity. See Network Integrity Installation Guide for more information.

About the System MBean Configuration Services

You can use the System MBean Configuration Services to perform configuration tasks on Network Integrity.

MBeans are viewed and used using the System MBean Viewer. See "Accessing the System MBean Viewer" for more information.

This section describes the MBeans available in Network Integrity. See "About Network Integrity MBeans" for more information.

This section also explains how to use MBeans to run tasks. See "About Using MBeans to Execute Configuration Tasks on Network Integrity" for more information.

Accessing the System MBean Viewer

The System MBean Viewer is a component of Oracle Enterprise Manager.

To view MBeans in the System MBean Viewer:

1. Access the Enterprise Manager using the following URL:

   `http://AdminServer-IP:AdminServer-PORT/em`

2. Log on to the Enterprise Manager using WebLogic user credentials.
3. In the left pane, select and expand your WebLogic domain.
4. Right-click the server on which you are working and select **System MBean Browser**.

   The System MBean Viewer screen appears.

MBeans for Network Integrity are found in the following directory of the System MBean Browser:

Application Defined MBeans/oracle.communications.integrity/Server: *Managed_Server_Name*

where *Managed_Server_Name* is the name of the managed server.

About Network Integrity MBeans

This section lists all the Network Integrity MBeans that you can use to perform configuration tasks on Network Integrity:

- ActionProperties MBean
- CMWSConfigurationService MBean
- FileTransferJCA MBean
- NIConfigurationService MBean
- NIRegionalLinksService MBean

CMWSConfigurationService MBean

The CMWSConfigurationService MBean is located in the **cmws.jmx.AdapterMXBean** folder.

Use the CMWSConfigurationService MBean to recover Network Integrity from a failed state.

The CMWSConfigurationService MBean provides the following operation:

- startRecoveryProcess: Starts the process to recover the Network Integrity application from a failed state.

The CMWSConfigurationService MBean has the following attributes:

- StopRunningScansWaitTime: Configures the waiting time (in milliseconds) for the server to stop. The default is **240000**.
- RestartAppWaitTime: Configures the waiting time (in milliseconds) for Network Integrity to restart after deployment or undeployment. The default is **1800000**.

NIConfigurationService MBean

The NIConfigurationService MBean is located in the **ResourceProviderMXBean** folder.

Use the NIConfigurationService MBean to start and stop the Age Out process.

The NIConfigurationService MBean provides the following operations:

- startAgeOutProcess: Starts the age out process.
- stopAgeOutProcess: Stops the age out process.
- initializeTimers: Initialise TIMERS for Schedules, DisBlackout Schedules, Ageout Schedules.

The NIConfigurationService MBean has the following attributes:

- AgeOutScheduleData: Provides the age out process schedule data.
- AgeoutMinResults: Configures the minimum number of latest scan results that remain after an ageout purge process. The default is **2**.
- AgeoutPurge: Enables or disables the age out process. The default is **True**.
- AgeoutWindowTime: Configures the minimum age (in days) of the scan results for deletion by the age out process. The default is **90**.
- jobDispatcherThrottle: Configures the number of work items that can be in the Job Dispatcher queuethrottle value for JobDispatcher. For example, a value of 10 means that a maximum of 10 work item can be in the JobDispatcher queue.
- LdapHost: Configures the host name or IP address of the LDAP server.
- LdapPort: Configures the port number for the LDAP server.
- LdapUserBase: Configures the domain name of the LDAP search base for Network Integrity users.
- MinBlackPeriod: Configures the minimum blackout period (in minutes).
- SSLEnable: Enables or disables SSL for the embedded LDAP server.
- UIRefreshInterval: Configures the Network Integrity UI scan status pane refresh interval time (in seconds). Valid values range from `1` to `30`.

- PersistResultsInParallel: Enables/disables the parallel persisting of entities. It is best-suited for FTP scans where persisting entities may lag compared to modeling. It is set to 'False' by default.
- DisableValidationForSpecExtension: Enables/disables the validation check for specification extension. When disabled, the cartridge deployment fails if existing characteristics are removed in the specification design. It is set to 'False' by default.

NIRegionalLinksService MBean

The NIRegionalLinksService MBean is located in the **RegionalLinksMXBean** folder.

Use the NIRegionalLinksService MBean to add URLs to the Links pane of the Network Integrity interface.

The NIRegionalLinksService MBean has the following attributes:

- URL*n*: Configures a URL on the Links pane (*n* can be from 1 to 30).
- URLName*n*: Provides a name to the configured URL, as it is to appear in the Links pane (*n* can be from 1 to 30).

ActionProperties MBean

The ActionProperties MBean is located in the **ActionProperty** folder.

Use the ActionProperties MBean to configure property values on a managed property group during run time.

The ActionProperties MBean provides the following operations:

- addProperty: Adds a new property to a managed property group.
- listProperties: Lists all properties of the specified managed property group.
- listPropertyGroups: Lists all managed property groups.
- removeProperty: Removes a property from a managed property group.
- restorePropertyDefaultValue: Restores the default value to a managed property.
- setProperty: Sets a value to a specified managed property.

The managed properties available for a particular action are explained in the Cartridge guide for the action.

FileTransferJCA MBean

The FileTransferJCA MBean is located in the **FileTransferConfigMXBean** folder.

Use FileTransferJCA MBean to manage the properties of the File Transfer JCA.

For information about file transfer functionality, see Network Integrity File Transfer and Parsing Guide.

The FileTransferJCA MBean has the following attribute:

- LocalStorageDirectory: Configures the full path where the File Transfer JCA temporarily stores local copies of remote files. The directory must exist and be readable and writable by WebLogic Server.

For example, *Middleware_Home*/**user_projects/domains/***domain_name*/**servers/***server_name*/**FileTransferAdapter**, where *server_name* is the name of the administration or managed server.

> **Note:**
>
> If the File Transfer JCA is deployed to a cluster, the specified directory must be shared and be readable and writable by all servers in the cluster.

About Using MBeans to Execute Configuration Tasks on Network Integrity

This section explains the administration tasks you can perform on Network Integrity using Enterprise Manager to run MBean operations.

Starting and Stopping the Age Out Process

The startAgeOutProcess and stopAgeOutProcess operations on the NIConfigurationService MBean are used to start and stop the AgeOut process.

To start the AgeOut process for Network Integrity:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Operations** tab, select **startAgeOutProcess**.

   The Operation: startAgeOutProcess screen appears.
3. In the **startDate** field, enter the start date for the age out process in the following format:

   ```
   yyyy-mm-dd hh:mm:ss z
   ```

   For example, 2010-04-21 16:45:50 GMT
4. In the **recurrenceRule** field, enter the frequency as an iCalendar expression, which represents the interval at which the age out process will repeat.

   > **Note:**
   >
   > You cannot specify the frequency to run the ageout start process only once.

   The valid formats for providing the recurrence rule are as follows:

   - To specify the frequency as daily, enter the following:

     ```
     FREQ=DAILY;BYHOUR=09;BYMINUTE=10;BYSECOND=00;
     ```
   - To specify the frequency as weekly, enter the following:

     ```
     FREQ=WEEKLY;BYHOUR=09;BYMINUTE=10;BYSECOND=00;BYDAY=MO, WE, TH;
     ```

     In the above expression, a value of **MO**, **WE**, **TH** for BYDAY indicates that the ageout process will repeat on Monday, Wednesday, and Thursday of a week.

     You can specify multiple days of the week. For example, BYDAY=MO, TU, WE, TH, FR, SA, SU.

- To specify the frequency as monthly, do one of the following:
  - To specify the frequency on a day from the beginning of the month, enter the following:

    ```
    FREQ=MONTHLY;BYHOUR=09;BYMINUTE=10;BYSECOND=00;BYMONTHDAY=2;
    ```

    In the above expression, a value of **2** for BYMONTHDAY indicates that the ageout process will repeat on the 2nd day of each month.

    You must specify a number between 1 and 28 for BYMONTHDAY.
  - To specify the frequency on a day from end of month, enter the following:

    ```
    FREQ=MONTHLY;BYHOUR=09;BYMINUTE=10;BYSECOND=00;BYMONTHDAY=-6;
    ```

    In the above expression, a value of **-6** for BYMONTHDAY indicates that the ageout process will repeat on the day that falls six days before the end of each month.

    You must specify a number between -1 and -7 for BYMONTHDAY.
  - To specify the frequency on the day of the month using an ordinal and the day of the week, enter the following:

    ```
    FREQ=MONTHLY;BYHOUR=09;BYMINUTE=10;BYSECOND=00;BYDAY=2MO;
    ```

    In the above expression, a value of **2MO** for BYDAY indicates that the ageout process will repeat on the second Monday of the month.

    Supported ordinals are first (1), second (2), third (3), fourth (4), fifth (5), and last (-1).
- To specify the frequency as yearly, do one of the following:
  - To specify the frequency for the month and the day of the year, enter the following:

    ```
    FREQ=YEARLY;BYHOUR=09;BYMINUTE=10;BYSECOND=00;BYMONTH=3;BYMONTHDAY=24;
    ```

    In the above expression, a value of **3** for BYMONTH and a value of **24** for BYMONTHDAY indicates that the ageout process will repeat on March 24 each year.

    You must specify a number between 1 and 12 for BYMONTH and a number between 1 and 28 for BYMONTHDAY.
  - To specify the frequency on a day of the year using an ordinal, the day of the week, and the month, enter the following:

    ```
    FREQ=YEARLY;BYHOUR=09;BYMINUTE=10;BYSECOND=00;BYDAY=2MO;BYMONTH=2;
    ```

    In the above expression, a value of **2MO** for BYDAY and a value of **2** for BYMONTH indicates that the ageout process will repeat on the second Monday in the month of February each year.

    Supported ordinals are first (1), second (2), third (3), fourth (4), fifth (5), and last (-1).

5. Click **Invoke**.

   The AgeOut process starts.

To stop the AgeOut process for Network Integrity:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Operations** tab, select **stopAgeOutProcess**.

The Operation: stopAgeOutProcess screen appears.

3. Click **Invoke**.

   The AgeOut process stops.

Enabling and Disabling the Ageout Purge Process

The AgeoutPurge attribute on the NIConfigurationService MBean is used to enable and disable the purging of scan results that are older than a specified value.

To configure the AgeoutPurge attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **AgeoutPurge**.

   The Attribute: AgeoutPurge screen appears.
3. In the **Value** list, select **True** to enable the Ageout Purge Process, select **False** to disable the Ageout Purge Process.
4. Click **Apply**.

Configuring the Minimum Number of Remaining Scans After Ageout Purge

The AgeoutMinResults attribute on the NIConfigurationService MBean is used to configure the minimum number of scan results to remain after the Ageout Purge Process is run.

To configure the AgeoutMinResults attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **AgeoutMinResults**.

   The Attribute: AgeoutMinResults screen appears.
3. In the **Value** field, enter the minimum number of scan results to remain after the Ageout Purge Process is run.
4. Click **Apply**.

Configuring the Expiration Time for Scan Results

The AgeoutWindowTime attribute on the NIConfigurationService MBean is used to configure the minimum number of days after which a scan result gets deleted by the Ageout Purge Process.

To configure the AgeoutWindowTime attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **AgeoutWindowTime**.

   The Attribute: AgeoutWindowTime screen appears.
3. In the **Value** field, enter the minimum number of days after which a scan result gets deleted by the Ageout Purge Process.
4. Click **Apply**.

Configuring the Throttle Value for Job Dispatcher

The jobDispatcherThrottle attribute on the NIConfigurationService MBean is used to configure the number of work items permitted in the queue for the Job Dispatcher.

To configure the jobDispatcherThrottle attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **jobDispatcherThrottle**.

   The Attribute: jobDispatcherThrottle screen appears.
3. In the **Value** field, enter the number of work items permitted in the queue for the Job Dispatcher.
4. Click **Apply**.

Enabling/Disabling SSL for the Embedded LDAP Server

The SSLEnable attribute on the NIConfigurationService MBean is used to enable or disable SSL for the embedded LDAP server.

To configure the SSLEnable attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **SSLEnable**.

   The Attribute: SSLEnable screen appears.
3. From the **Value** list, select **True** to enable SSL, select **False** to disable SSL.
4. Click **Apply**.

Configuring the LDAP Host

The LdapHost attribute on the NIConfigurationService MBean is used to configure the host name or IP address of the LDAP server.

To configure the LdapHost attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **LdapHost**.

   The Attribute: LdapHost screen appears.
3. In the **Value** field, enter the host name or the IP address of the LDAP server.
4. Click **Apply**.

Configuring the LDAP Port

The LdapPort attribute on the NIConfigurationService MBean is used to configure the port number of the LDAP server.

To configure the LdapPort attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **LdapPort**.

   The Attribute: LdapPort screen appears.
3. In the **Value** field, enter the port number of the LDAP server.
4. Click **Apply**.

Configuring the Scan Results Status Window Refresh Time

The UIRefreshInterval attribute on the NIConfigurationService MBean is used to configure how often the scan status results are refreshed in the Network Integrity interface.

To configure the UIRefreshInterval attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **UIRefreshInterval**.

   The Attribute: UIRefreshInterval screen appears.
3. In the **Value** field, enter the number of seconds between scan result refreshes.
4. Click **Apply**.

Setting the Minimum Time Limit for a Blackout Period

The MinBlackPeriod attribute on the NIConfigurationService MBean is used to configure the minimum blackout period.

To configure the MinBlackPeriod attribute:

1. In the System MBean Browser of Enterprise Manager, select the **NIConfigurationService** MBean.
2. On the **Attributes** tab, select **MinBlackPeriod**.

   The Attribute: MinBlackPeriod screen appears.
3. In the **Value** field, enter the number of minutes for the minimum blackout period.
4. Click **Apply**.

Configuring Links on the Links Panel

The URL and URLName attributes on the NIRegionalLinksService MBean are used to configure links on the **Links** panel. You can use the URL and URL attributes to add, change, and remove links from the **Links** panel.

To add links to the **Links** panel of the Network Integrity Interface:

1. In the System MBean Browser of Enterprise Manager, select the **NIRegionalLinksService** MBean.
2. On the **Attributes** tab, select a URL attribute with a blank value.

   The Attribute: *URL* screen appears, where *URL* is the URL attribute you selected.
3. In the **Value** field, enter the URL you want to add to the **Links** panel.
4. Click **Apply**.

5. On the **Attributes** tab, select the URL name attribute that corresponds with the URL attribute.

   The Attribute: *URL_Name* screen appears, where *URL_Name* is the URL name attribute you selected.

6. In the **Value** field, enter a name for the URL as you want it to appear in the **Links** panel.
7. Click **Apply**.

To configure links on the **Links** panel of the Network Integrity Interface:

1. In the System MBean Browser of Enterprise Manager, select the **NIRegionalLinksService** MBean.
2. On the **Attributes** tab, select a URL attribute with a configured value.

   The Attribute: *URL* screen appears, where *URL* is the URL attribute you selected.

3. Do one of the following:
   - To modify the URL, enter a new URL in the **Value** field.
   - To delete the URL, make the **Value** field empty.
4. Click **Apply**.

   A confirmation message appears.

5. Click **Return**.
6. On the **Attributes** tab, select the URL Name attribute that corresponds with the URL attribute.

   The Attribute: *URL_Name* screen appears, where *URL_Name* is the URL Name attribute you selected.

7. Do one of the following:
   - To modify the URL name, enter a new URL name in the **Value** field, as you want it to appear in the Links panel of the Network Integrity interface.
   - To delete the URL name, make the **Value** field empty.
8. Click **Apply**.

   A confirmation message appears.

Redirecting the Import and Discovery Scans to Managed Server for Achieving a Better Load Balancing in a Cluster

You can redirect the Import and Discovery scans to a Managed Server (MS) for achieving a better Load Balancing in a Weblogic or NI cluster domain.

To achieve this better load balancing:

1. Configure new JMS sub-deployments and JMS Connection Factory.
2. Create and model the Discovery or Import scan to have a new custom attribute **JMS_CF**.

The scans will be performed in the corresponding cluster MSs if you have created a new Discovery or Import scan with the Connection Factory values in the **JMS_CF** attribute at the scan-level. This process of scheduling the scans and redirecting them to each MS helps you in attaining a better load balancing.

> **Note:**
>
> - This process works efficiently if the scans have one or two work items that are running.
> - It is recommended to avoid this process for scans involving many work items, as it may lead to MS overloading.

Configuring the Server Load Balancer

Multiserver deployments consist of clusters, managed servers, and standalone servers in single, or multiple WebLogic Server domains. A server farm like this achieves high availability and scalability through server load balancing by appearing as a single server to client systems.

There are two types of client requests that are managed when you employ load balancing: HTTP and JMS.

This section briefly discusses these server requests and how the respective loads can be balanced.

Load Balancing HTTP Sessions Using Server Load Balancer

Server load balancer (SLB) provides a virtual server acting as the single point of entry for a group of real servers and distributes requests across the real servers depending on the load balancing algorithm and the availability of the servers.

> **Note:**
>
> Oracle recommends the hardware-based load balancer for reliability and scalability. Hardware SLB contains application-specific integrated circuits (ASICs) that enable high-speed forwarding of network traffic, without operating system overhead.

Server Load Balancer Requirements

For information on server load balance requirements while working with the WebLogic server, see the following Fusion Middleware document:

`http://download.oracle.com/docs/cd/E12839_01/web.1111/e13709/load_balancing.htm#CLUST175`

> **Note:**
>
> The SLB examples provided at this link refer the F5 BIG-IP Application Switches LTM, Cisco ACE, and Brocade ServerIron.

> **Note:**
>
> Oracle recommends the SSL acceleration module to process SSL transactions efficiently. Furthermore, it eliminates cost installing SSL certificates on all WebLogic servers.

Server Load Balancer Configurations

Network Integrity uses TCP-levels load balancing.

Keep the following considerations in mind for virtual server and real server configurations:

- Use the following URL to identify the Network Integrity managed servers in a cluster and configure the hardware load balancer to balance the loads on UI and web service Network Integrity requests:

  `https://IP:Port/NetworkIntegrity/index.html`

  Where *IP* is the IP address of the Network Integrity server, and *Port* is the port number where the Network Integrity server is running.

  > **Note:**
  >
  > Oracle recommends BIG IP LTM 3600 as a hardware load balancer.

- Working with sticky sessions, which basically means that a user's requests are sent to the same server where the sessions was first initiated. The server must be enabled for HTTP/HTTPS requests until it is not available.

During HTTP request processing, such as dynamic web service discovery, the response may contain a real server listening address which may not be accessible from client systems. In such scenarios, consider the following:

- Use an SLB-specific feature to replace the listening address and port of a real server with the listening addresses and port of a virtual server. Because the HTTP response content is modified, you must reconfigure the HTTP content-length header. Verify with your SLB vendor if this feature is supported.
- Configure the HTTP front end host and the HTTP/HTTPS front end port for the WebLogic server or cluster. This approach is recommended if SLB does not support HTTP response modification. When configured, any attempt to access real servers directly is directed back to the virtual server.

Network Configurations

In a production environment, Network Integrity may be deployed with other Oracle Communications products, such as Unified Inventory Management (UIM). Network Integrity sends web service requests to the UIM application server for inventory import. If UIM is deployed on a cluster, the web service requests must go through the UIM virtual server. Therefore, the Network Integrity application server must be multi-homed.

Provided here are some examples of network deployment.

- **Management network**: This network is used for system administration and software installation. This is the default WebLogic server listening address.

- **Client network**: This network is used for client systems to send requests to the Network Integrity or UIM cluster.
- **Application server network**: This network is used for when the server load balancer is required to distribute client requests to clusters. It is advisable that you create a network channel for each application server.
- **Database server network**: Use this network when the application servers are required to send SQL requests to the database through JDBC.
- **Storage network**: If SAN is deployed, WebLogic server domains, JMS file stores, and database files could be placed on SAN. For performance, JMS file stores should be separated from WebLogic domains.

> **Note:**
>
> You do not necessarily need multiple networks to configure an SLB. If required, you can combine a management network, application server network, and database network.

> **Note:**
>
> Use link aggregation to increase bandwidth.

Load Balancing in a Clustered Environment

For load balancing in a clustered environment, use the Apache proxy server with the Oracle WebLogic server.

See the Apache web site to download and install the Apache server:

`http://httpd.apache.org/download.cgi`

Download the Apache plug-in for the WebLogic server from the Oracle Technology Network web site:

`http://www.oracle.com/technetwork/middleware/ias/downloads/wls-plugins-096117.html`

> **Note:**
>
> You must accept the Oracle Technology Network License Agreement to download this software.

For more information on how the plug-in works in WebLogic, see the following Oracle web site:

`http://download.oracle.com/docs/cd/E13222_01/wls/docs100/plugins/apache.html`

To configure the server load balancer:

1. Extract **mod_wl_22.so** for the particular operating system where Apache is running from the WebLogic plug-in you downloaded earlier.

2. Save the extracted files in the **Modules** folder of the Apache server. For example:

   C:\Program Files\Apache Software Foundation\Apache2.2\modules

3. Open **\Apache2.2\modules\httpd.conf**.

4. Modify the file by making the following entries:

```
IfModule mod_weblogic.c

WebLogicCluster
10.147.240.145:7755,10.147.240.137:7744,10.147.240.145:7055,10.147.240.137:7044
MatchExpression /NetworkIntegrity/*
MatchExpression /NetworkIntegrityApp-NetworkIntegrityControlWebService-context-root/*
Debug ON
DebugConfigInfo ON
WLLogFile /opt/oracle/weblogic.log
</IfModule>

<IfModule mod_weblogic.c>
WebLogicHost 10.147.240.145
WebLogicPort 7777
MatchExpression /xmlpserver/*
</IfModule>
```

   where *WebLogicCluster* is the IP address or port number of the WebLogic Server cluster, and `MatchExpression` has the context root of the web application.

> **Note:**
>
> In Network Integrity, reports are deployed on a non-clustered Managed Server. Therefore, it is recommended that you use a WebLogicHost instead of a WebLogicCluster in the `<ifmodule>` in the above example.

5. Restart the HTTP server.

   You can now access the application from the proxy server.

You can connect to the following services at the provided URLs:

- Webservices wsdl:
- `http://localhost:82/NetworkIntegrityApp-NetworkIntegrityControlWebService-context-root/NetworkIntegrityControlServicePortType?wsdl`
- UI:
- `http://localhost:82/NetworkIntegrity/faces/IntegrityUIShell`
- Reports:
- `http://localhost:82/xmlpserver/`

Load Balancing JMS Messages

For applications that are not running within a WebLogic server instance, load balancing JMS messages is achieved by specifying the `PROVIDER_URL` when creating `JNDI initialContext` object to connect to a server or cluster.

For applications running within a WebLogic server instance, creating `initialContext` without providing `PROVIDER_URL` implicitly returns the `JNDI context f`or the local server or cluster.

When you use the JMS Store-and-Forward (SAF) feature to provide highly-available JMS message production, by connecting a local server and reliably forwarded messages to a remote JMS destination, SAF remote context defines the URL of the remote server instance or cluster where the JMS destination is exported from. It also contains the security credentials to be authenticated and authorized in the remote cluster or server(s).

To import remote destinations from a remote cluster or servers, you must supply one of the following for the `PROVIDER_URL` or SAF remote context:

- A comma-delimited list of DNS server names
- A comma-delimited list of IP addresses
- Remote cluster's cluster address defined in DNS (recommended for production environment)

The following examples are of a URL used when a remote SAF context defines a remote cluster from which it imports distributed destination members:

- `<URL> t3://192.180.0.10:7012,192.168.0.11:7012,192.168.0.12:7012</URL>`
- `<URL> t3://192.180.0.10:7012,192.168.0.11:7012,192.168.0.12:7012</URL>`

where, `UIMCluster` is the cluster address for the UIM application cluster consisting of servers with IP addresses 192.168.0.10, 192.168.0.11, and 192.168.0.12.

> **Note:**
>
> Server load balancer has no part in load balancing JMS messages and may be used only for initial host name resolution.

For information about deploying the BIG-IP system with Oracle WebLogic Server, refer to the deployment guide at the F5 Networks Web site.

For information on Oracle Fusion Middleware Configuring and Managing Store-and-Forward for Oracle WebLogic Server, see the documentation at the following Oracle web site:

`http://download.oracle.com/docs/cd/E12839_01/web.1111/e13742/toc.htm`

5
Managing Network Integrity Performance

This chapter describes the tuning measures you can take to enhance the overall performance of the Oracle Communications Network Integrity system.

Tuning Network Integrity

Tuning Network Integrity improves the performance and throughput of the application and maximizes response time for the chosen hardware platform.

Network Integrity tuning tasks include:

- Tuning the Operating System(s)
- Tuning the Oracle Database
- Tuning the Java Virtual Machine (JVM) Startup Parameters
- Tuning the WebLogic Administration Server for Network Integrity
- Tuning Network Integrity

Tuning the Operating System(s)

This section provides recommended tuning adjustments for each operating system.

Tuning Recommendations for Solaris 10

- Edit the **/etc/system** file and set the following parameters:

```
set rlim_fd_cur=65535
set rlim_fd_max=65535
set shmsys:shminfo_shmmax=4294967295
set autoup=1
set tune_t_fsflushr=1
```

- Edit the **/lib/svc/method/net-init** file and set the following parameters using the following commands:

```
ndd -set /dev/tcp tcp_conn_req_max_q 16384
ndd -set /dev/tcp tcp_conn_req_max_q0 16384
ndd -set /dev/tcp tcp_time_wait_interval 60000
ndd -set /dev/tcp tcp_xmit_hiwait 131072
ndd -set /dev/tcp tcp_recv_hiwait 131072
ndd -set /dev/tcp tcp_keepalive_interval 7200000
ndd -set /dev/tcp tcp_xmit_hiwaiter_def 1048576
ndd -set /dev/tcp tcp_ip_abort_interval 60000
ndd -set /dev/tcp tcp_rexmit_interval_initial 4000
ndd -set /dev/tcp tcp_rexmit_interval_min 3000
ndd -set /dev/tcp tcp_rexmit_interval_max 10000
ndd -set /dev/tcp tcp_smallest_anon_port 32768
ndd -set /dev/tcp tcp_naglim_def 1
```

- Tune Solaris 10 for M series by editing the **/etc/system** file and set the following parameters:

```
set ddi_msix_alloc_limit=8
set ip:ip_soft_rings_cnt=16
set ip_squeue_soft_ring=1
set ip_threads_per_cpu=2
```

- Tune Solaris 10 for CMT (T5440/T5240/T5140/T5220/T5120/T2000/T100), edit the **/etc/system** file and set the following parameters:

```
set ip:ip_soft_rings_cnt=16
```

> **Caution:**
>
> Reboot the server after making these changes.

See Solaris platform documentation for more information about tuning.

Tuning Recommendations for Linux

You can modify the following parameters for a Linux environment:

- **kernel.msgmni**

  The default message queue is 16 which supports 16 users.

  Update the file **/etc/sysctl.conf** with the following entry:

```
kernel.msgmni=1024
```

> **Note:**
>
> **mtu** is the largest number of bytes that a packet can carry over a network. For better performance, set the parameter as:
>
> **/sbin/ifconfig** lo mtu 1500

- **net.ipv4.tcp_max_syn_backlog**

  This specifies the maximum number of remembered connection requests that have not received an acknowledgment from the connecting client.

  Update the file **/etc/sysctl.conf** with the following entry:

```
net.ipv4.tcp_max_syn_backlog=8192
```

- **/etc/security/limits.conf**

  Update this file with the following parameters:

  soft nofile 131072

  hard nofile 131072

  soft nproc 131072

  hard nproc 131072

  soft core unlimited

  hard core unlimited

  soft memlock 50000000

hard memlock 500000

Tuning Recommendations for AIX

Adjust the following parameters for an AIX environment.

Edit the **.profile** file, located in the directory where AIX is installed, to add the following entries:

```
AIXTHREAD_COND_DEBUG=OFF
export AIXTHREAD_COND_DEBUG
AIXTHREAD_MUTEX_DEBUG=OFF
export AIXTHREAD_MUTEX_DEBUG
AIXTHREAD_RWLOCK_DEBUG=OFF
export AIXTHREAD_RWLOCK_DEBUG
AIXTHREAD_SCOPE=S
export AIXTHREAD_SCOPE
LC__FASTMSG=true
export LC__FASTMSG
LDR_CNTRL=MAXDATA=0XB00000000@DSA
export LDR_CNTRL
```

Tuning the Oracle Database

This section describes the Network Integrity database tuning parameters.

Setting the Initialization Parameters

> **Note:**
>
> These parameters also apply to the Unified Inventory Management (UIM) system.

To set the database initialization parameters, execute the following script as the SYS user:

```
alter system set db_file_multiblock_read_count=16 scope=spfile;
alter system set distributed_lock_timeout=7200 scope=spfile;
alter system set dml_locks=9700 scope=spfile;
alter system set job_queue_processes=10 scope=spfile;
alter system set log_buffer=31457280 scope=spfile;
alter system set open_cursors=5000 scope=spfile;
alter system set parallel_max_servers=640 scope=spfile;
alter system set plsql_code_type=NATIVE scope=spfile;
alter system set query_rewrite_integrity=STALE_TOLERATED scope=spfile;
alter system set processes=3000 scope=spfile;
alter system set sessions=4528 scope=spfile;
alter system set transactions=4980 scope=spfile;
shutdown immediate
startup
```

> **Note:**
>
> The **memory_target** and **max_memory_target** parameters (which determine how much of RAM is allocated to the database SGA and PGA) should be set to as high a value as your database server platform allows.
>
> Oracle recommends a value of 8GB or higher.

Gathering the Schema Statistics

> **Note:**
>
> This section also applies to the Unified Inventory Management (UIM) system.

You can gather schema statistics to generate table and index statistics that the database engine query optimizer can use to select the best method for executing different SQL statements.

To gather schema statistics, execute the following command as the SYS user:

```
execute dbms_stats.gather_schema_stats(ownname => 'USERID',estimate_percent => 25,
method_opt => 'for all indexed columns size auto', cascade => true);
```

Where `USERID` is the name of the primary schema for the application selected at the time of installation.

> **Note:**
>
> Oracle recommends that you run this command periodically (weekly, or monthly) as the database gets populated continuously.

Relocating Indexes

During Network Integrity installation, all indexes are created in the same tablespace as data records. It is a good idea for the index data to be on disks separate from the table data. If your disks are set up this way (that is, you are not using RAID), then you may want to create a tablespace just for indexes (for example NINDEX) and then relocate the existing indexes to this tablespace.

To create a tablespace just for indexes and then relocate the existing indexes to this tablespace:

1. Use a script similar to the one provided below to create a second script.

```
set lin 90
spool move_index.sql
select 'alter index '||owner||'.'||index_name||' rebuild tablespace nindex;'
from dba_indexes
where owner='USERID' and not (index_name like 'SYS%')
```

```
order by owner,index_name;
spool off
```

The script creates the new script with the name **move_index.sql**.

2. Edit this new **move_index.sql** script to remove lines that are not `alter index` commands.
3. Execute the **move_index.sql** script as the SYS user.

Creating New Indexes

You can improve the performance of frequently used Network Integrity specific SQL statements by creating new indexes.

> **Note:**
>
> The following script shows how to create four new indexes.
>
> You **must** create these four indexes to improve performance.

To create new indexes, execute the following script as the SYS user.

```
create index idx_logicaldevice_01 on logicaldevice
(nativeemsname,entityclass) tablespace nindex compute statistics;
create index idx_physicaldevice_01 on physicaldevice
(nativeemsname,entityclass) tablespace nindex compute statistics;
create index idx_disrootentityref_01 on disrootentityref
(rootentityref,rootentityclass) tablespace nindex compute statistics;
create index idx_specification_01 on specification (name) tablespace nindex
compute statistics;
```

Managing and Monitoring Disk Space

Frequently monitoring your database is important to ensure that none of your disks or tablespaces are run out of required space. Make sure you know where the audit and trace files are located so you can delete them before they fill the disk.

For more information on Oracle database management and monitoring activities, see *Oracle Database Administrator's Guide*.

> **Note:**
>
> Oracle recommends that you use the Oracle Enterprise Manager for performing most of your DBA activities, including managing disk space.

> **Note:**
>
> Using RAID disks and faster disks for your Network Integrity database server gives you better performance and higher reliability.

Tuning the Java Virtual Machine (JVM) Startup Parameters

Keep the following in mind when selecting a JVM for running the application servers for Network Integrity:

Use the largest possible heap size that can be allocated based on the amount of RAM on your server.

The following environment variable names are used for the Network Integrity JVM in the rest of this section:

- AS_USER_MEM_ARGS (JVM startup parameters for the Administration Server)
- MS_USER_MEM_ARGS (JVM startup parameters for the Managed Server)

In the variables provided in this section, AS_ and MS_ represent Administration server and Managed server, respectively.

For the Administration server use the following variable:

```
export AS_USER_MEM_ARGS="JVM_Startup_Parameters"
export USER_MEM_ARGS=$AS_USER_MEM_ARGS
```

For a Managed server use the following variable:

```
export MS_USER_MEM_ARGS="JVM_Startup_Parameters"
export USER_MEM_ARGS=$MS_USER_MEM_ARGS
```

where "*JVM_Startup_Parameters*" are the JVM startup settings for your OS. For example, for 64-bit Sun Hotspot JVM Administration server on Solaris:

```
export MS_USER_MEM_ARGS="-d64 -Xms1g -Xmx20g -XX:PermSize=512m -XX:MaxPermSize=1012m -
XX:GCTimeRatio=1 -XX:MaxGCPauseMillis=30000 -XX:+UseCompressedOops"
export USER_MEM_ARGS=$MS_USER_MEM_ARGS
```

You can set these variables in the following two ways:

- In one command session, export AS_USER_MEM_ARGS and launch the Administration server. Then, in a second command session, export MS_USER_MEM_ARGS and launch the Managed servers.
- Write your own startup scripts for the Administration and Managed servers.

Setting JVM Startup Parameters for Solaris

This section provides the parameters for setting the JVM startup for Solaris.

64-bit Sun Hotspot JVM (assuming the maximum amount of RAM you can allocate is 21GB)

- AS_USER_MEM_ARGS = "-d64 -Xms1g -Xmx1g -XX:PermSize=384m -XX:MaxPermSize=484m"
- MS_USER_MEM_ARGS = "-d64 -Xms1g -Xmx20g -XX:PermSize=512m -XX:MaxPermSize=1012m -XX:GCTimeRatio=1 -XX:MaxGCPauseMillis=30000 -XX:+UseCompressedOops"

Setting JVM Startup Parameters for Linux

This section provides the parameters for setting the JVM startup for Linux.

64-bit Sun Hotspot JVM (assuming the maximum amount of RAM you can allocate is 21GB)

- AS_USER_MEM_ARGS = "-d64 -Xms1g -Xmx1g -XX:PermSize=384m -XX:MaxPermSize=484m"
- MS_USER_MEM_ARGS = "-d64 -Xms1g -Xmx20g -XX:PermSize=512m -XX:MaxPermSize=1012m -XX:GCTimeRatio=1 -XX:MaxGCPauseMillis=30000 -XX:+UseCompressedOops"

Setting JVM Startup Parameters for IBM AIX

This section provides the parameters for setting the JVM startup for AIX.

- AS_USER_MEM_ARGS = "-d64 -Xms1g -Xmx1g -XX:PermSize=384m -XX:MaxPermSize=484m"
- MS_USER_MEM_ARGS = "-d64 -Xms1g -Xmx1g -XX:PermSize=512m -XX:MaxPermSize=1012m"

Tuning the WebLogic Administration Server for Network Integrity

This section lists the recommended changes for tuning the WebLogic application server for Network Integrity.

To tune the WebLogic Administration Server for Network Integrity:

1. Log in to the Oracle WebLogic Server Administration Console using the Administrator credentials.

   The Home screen of the Administration Console appears.
2. Under JDBC, under the main heading Services, select **Data Sources**.

   The Summary of JDBC Data Sources screen appears.
3. In the Data Sources table, click **JobDispatcherDS**.

   The Settings for JobDispatcherDS screen appears.
4. Select and display the **Connection Pool** tab.
5. Do the following:
   a. In the **Initial Capacity** field, enter the value as **50**.
   b. In the **Maximum Capacity** field, enter the value as **100**.
   c. In the **Capacity Increment** field, enter the value as **2**.
6. Come back to the Summary of JDBC Data Sources screen.
7. In the Data Sources table, click **NIDataSource**.

   The Settings for NIDatasource screen appears.
8. Select the **Transaction** tab.
9. Configure the following parameters:
   - Select the **XA Transaction Timeout** check box.
   - In the **XA Transaction Timeout** field, enter **0**.
10. Select the **Connection Pool** tab.
11. Do the following:
    a. In the **Initial Capacity** field, enter the value as **50**.

b. In the **Maximum Capacity** field, enter the value as **100**.

c. In the **Capacity Increment** field, enter the value as **2**.

12. Go back to Home.

13. Select **Work Managers** under Environment.

    The Summary of Work Managers screen appears.

14. In the Global Work Managers, Request Classes and Constraints table, click **NI-MaxThreadConstraint**.

    The Settings for NI-MaxThreadConstraint screen appears.

15. In the **Count** field, enter an appropriate value.

    Keep the following in mind regarding the **NI-MaxThreadConstraint** parameter:

    - This is a critical tuning value. It directly affects the throughput of critical Network Integrity batch operations such as network scans and discrepancy detection. A value approximately equal to (max_heap_size-300mb)/160 is generally used initially. However, you can experiment with this throttle to find the perfect balance between a lower value (for example, 10) that reduces the chance of flooding the system with too many simultaneous tasks (which could result in a JVM out of memory error) and a higher value (for example, 70) that improves the throughput of batch operations. The optimum value depends on a variety of factors such as JVM type, heap size, RAM available, CPU number and speed, disk speed, database performance, and so on.
    - This is also a very important setting for the WebLogic Administration Server as the server might become unstable under out-of-memory conditions. If the **NI-MaxThreadConstraint** parameter is set too high, the WebLogic Administration Server may run out of memory trying to process too many requests at one time. You must tune for the worst case; the maximum parallelism of the largest network elements. The WebLogic Administration Server does offer some safeguards to prevent continued operation under overload conditions. You can configure the managed servers to automatically shut down a server under overload conditions. You do this by setting a **Panic Action** or a **Failure Action** on the **Overload** tab for the managed server(s) in the WebLogic Administration Server Console.

      For more information, see the WebLogic Administration Server administration guide at the following location:

      http://www.oracle.com/technology
    - This parameter also affects interaction with external systems. For example, tune the UIM system to support up to NI-MaxThreadConstraint concurrent web service operations, to support uploading large quantities of resolved discrepancies to UIM. Configure the UIM InventoryTxDataSource with a maximum number of connections greater than the NI-MaxThreadConstraint value.
    - You must restart the managed server(s) after changing this value.

> **Note:**
>
> For information on tuning the WebLogic Administration Server for Oracle Communications Unified Inventory Management (UIM), see the related UIM documentation.

Tuning Network Integrity

This section provides recommendations on maximizing Network Integrity performance.

Performing Tasks in Parallel

To support a large network of many thousands of network elements, performing tasks such as inventory imports, network scans, and discrepancy detection in parallel, maximizes performance.

You get parallelism for network scans and discrepancy detection automatically. The degree of parallelism is determined by the **NI-MaxThreadConstraint** value. For example, let's say you have a network scan (with discrepancy detection enabled) of 200 devices and **NI-MaxThreadConstraint** set to 50. When the scan starts, the first 50 devices are scanned. As each device completes, another device begins so that you always have 50 devices being scanned at the same time. When all 200 devices are scanned, then the discrepancy detection begins in the same way, the first 50 begin and completed ones are replaced with new ones to be scanned.

You do not get parallelism automatically for inventory imports though. For example, an inventory import scan of 200 devices imports those 200 devices in serial (regardless of the **NI-MaxThreadConstraint** value).

The best approach is to divide the 200 devices into N batches (where N is the number of CPU cores on your Network Integrity application server) and schedule them to all run at the same time. For example, if you have 8 CPU cores, you should create 8 inventory import scans, manually, of 25 devices each. This reduces the total time to import those devices in 8 parallel scans to approximately 20% of what it would take to import those devices serially in 1 large scan.

> **Note:**
>
> This approach is critical to maximizing the reconciliation throughput of the Network Integrity system and thereby supporting as large a network as possible.

Limiting the Total Number of Requests

You can reduce chances of application server memory related problems due to too many concurrent work requests being generated by the Network Integrity UI and web services users by configuring the **Shared Capacity for Work Managers** parameter to have a much lower value.

To lower the value of the **Shared Capacity for Work Managers** parameter:

1. Log on to the Oracle WebLogic Administration Server.

   The Home screen of the Administration Console appears.

2. Under Environment, select **Servers**.

   The Summary of Servers screen appears.

3. In the Servers table, click the managed server, *ManagedServerName*, for which you want to configure the parameter.

   The Settings for *ManagedServerName* screen appears.

4. Select the **Overload** tab to display it.
5. In the **Shared Capacity For Work Managers** field, enter a lower value.

> **Note:**
>
> The exact value depends on the capacity of your platform and the amount of scans and user requests being initiated.

Working with Stuck Threads

The following three timeout parameter settings affect the operation of Network Integrity jobs. If a job does not complete before these timeout values expire, then the job is abandoned.

- **Java Transaction API (JTA) timeout**

  This is the WebLogic console setting for the time limit of a java transaction.

  To set the JTA timeout:

  1. Log on to the Oracle WebLogic Administration Console.

     The Home screen of the Administration Console appears.
  2. Under Services, select **JTA**.

     The Settings screen appears with the JTA tab displayed.
  3. In the **Timeout Seconds** field, enter the appropriate value.

     > **Note:**
     >
     > A safe value is 7200 seconds (2 hours). If you have extremely large devices in your UIM system, you may want to increase this value to something like 10800 (3 hours) or 144000 (4 hours).

- **Stuck Thread Max Time**

  This is the Weblogic console setting for the length of time a thread can work for before the server considers it stuck.

  To set the Stuck Thread Max Time value:

  1. Log on to the Oracle WebLogic Administration Console.

     The Home screen of the Administration Console appears.
  2. Under Environment, select **Servers**.

     The Summary of Servers screen appears.
  3. In the Servers table, click the *Managed_Server*.

     The Settings for *Managed_Server* screen appears.
  4. Select the **Tuning** tab to display it.
  5. In the **Stuck Thread Max Time** field, enter the appropriate value.

> **Note:**
>
> A safe value is 7200 seconds (2 hours). If you have extremely large devices in your UIM system, you may want to increase this value to something like 10800 (3 hours) or 144000 (4 hours).

- **JobDispatcher TimeToLive**

  This is the Network Integrity Mbean property value for the time limit of a Network Integrity job.

> **Note:**
>
> These three parameters should have the same value.

You can adjust the stuck thread timeout values using the WebLogic Server Administration Console.

> **Note:**
>
> Stuck threads add to the server load and could cause problems. Configuring the Stuck Thread Count value puts the server into a Failed state if too many threads are stuck. A value of 4 may be appropriate.

Configuring Page Size for Viewing Discrepancy Results

You can configure the Review Discrepancy page size to view the desired number of results by using the **discrepancies.page.size** property located within the **system-config.properties** file in the *domain_home***/ni/config** directory. This property defines the number of discrepancy results to be fetched from the database at a time.

By default, the value is set to 200. You can customize the property by setting it to a value within the allowed range (1-1000) to fetch the desired number of discrepancy results.

6

Backing Up and Restoring Network Integrity Data

This chapter describes how to back up and restore Oracle Communications Network Integrity data. It covers the following topics:

About Backup in Network Integrity

You can backup discovered data and application configurations using Network Integrity. Network Integrity has an effective backup mechanism which can be set up to run at regular time intervals for a systematic backup of all the required Network Integrity data and configuration, and also restore it as and when required. One option is to perform a routine backup on a daily basis setting it up as an overnight process.

> **Note:**
>
> You must perform regular database integrity checks. It is recommended that this check be performed on the backed-up database, and not the live system.

Data can be backed up even if the server is not running, or if the database is not in use.

For more information about backup, and to perform a backup, see the Oracle Fusion Middleware documentation at the following location:

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

About Backing up Data

All data is critical and has to be backed up. There is no data which can be considered non-critical and hence not be backed up. Network Integrity backs up the following information:

- **Database information**

  This type of data is database driven or database specific. Following are the database information types:

  - Network Integrity tablespaces: Contains information on configuration, scans, and discrepancies along with Network Integrity configuration. This information can be viewed using the Mbean console.
  - WebLogic persistent store: Contains information responsible for persisting the scan, discrepancy, and assimilation of jobs (if a job failure such as a server failure, it ensures that the job is resumed and completed.)

- **Domain configuration**

  This type of data contains information about the following:

  - Connection pool sizes (database, SNMP JCA)
  - Workmanager (thread pools) for cartridges
  - Security configuration (SSL), security providers (embedded LDAP or Oracle Internet Directory)
  - Other J2EE resources (JMS queues, topics, cluster configuration, and loadbalancing etc)
    * Work managers
    * GC parameters
    * Domain configuration files (set **Domainenv.sh** and so on)
    * Data sources
    * Java Message Service (JMS) resource configurations
    * Installed applications

- **Security provider**

  This type of data contains users/roles in LDAP provider (embedded LDAP or Oracle Internet Directory). If you use embedded LDAP, data is backed up as part of WebLogic domain backup. If you use external LDAP or any other system, you must follow the backup mechanism specifically mentioned in that software.

Backup Data in Offline and Online Modes

You can back up data in both offline and online modes. A complete high availability and disaster recovery strategy requires dependable data backup, restore, and recovery procedures. You can use Oracle Recovery Manager (RMAN), a command-line and Oracle Enterprise Manager-based tool for backing up and recovering your database. RMAN provides block-level corruption detection during backup and restore and optimizes performance and space consumption with file multiplexing and backup set compression. You can integrate RMAN with Oracle Secure Backup and third party media management products for tape backup.

About Restore in Network Integrity

Restore is a method whereby lost data can be recovered completely. Network Integrity has a restore feature that works as a recovery strategy for outages that involve actual data loss or corruption, host failure, or media failure where the host or disk cannot be restarted and are permanently lost. This type of failure requires some type of data restoration before the Oracle Fusion Middleware environment can be restarted and continue with normal processing.

For more information on recovering data and for steps on recovering data, see the Oracle Fusion Middleware documentation at the following location:

http://www.oracle.com/technology

Restoring In a Cluster Environment

In a cluster environment, if a Network Integrity adaptor is installed on the Administration server and the server fails, restore the entire server using a backup.

If a Network Integrity adaptor is installed on a managed server and the server fails, follow these steps to restore the server:

1. Add a new managed server to the cluster on the same system.
2. Deploy all Network Integrity components on this managed server.

7

Removing Large Volumes of Obsolete Data using Purge Scripts

This chapter describes how to remove large volumes of obsolete data using purge scripts.

About Purge Scripts

You use purge scripts to remove large volumes of obsolete data from the NI database, without using the NI application.

A date-based condition can be used for filtering the OCIM table data. This results in the required data that needs to be cleared and you can delete this data using the purge scripts.

The purge scripts:

- Provide parallel execution of OCIM and NI tables.
- Use tables to capture the following information:
  - Individual purge records on both OCIM and NI tables and scan levels.
  - Scan IDs on which the purge scripts are run.
  - Errors captured during the purge run.
- Delete the tables with comparatively high volumes of data.
- Delete the Bash shell scripts to run the SQLs with the corresponding DB connection details.

About Purge Tables

Purge tables capture the details related to every purge script. The tables that capture these details are:

- **PURGED_RECORD_DATA**: This table captures the details of every purge activity such as time taken, number of records deleted across scan IDs, and number of records deleted at the table level. The table contains the following columns:
  - **PURGED_RECORD_DATA.PURGE_ID**: A unique ID for a purge activity. This column cannot be **NULL**.
  - **PURGED_RECORD_DATA .CREATE_DATE**: The starting time of a purge activity.
  - **PURGED_RECORD_DATA .SCAN_ID**: The scan entity ID that is gathered from the DISSCANRUN table based on the filter criteria.

    > **Note:**
    >
    > One purge activity can have multiple scan IDs.

  - **PURGED_RECORD_DATA.PURGE_DURATION**: The time taken for purging records from a scan ID in a specific table. This value is calculated in milliseconds.

  - **PURGED_RECORD_DATA .TABLE_NAME**: The table name from which the data is purged.
  - **PURGED_RECORD_DATA .RECORDS_DELETED**: The number of records deleted in a scan ID from a specific table.

> **Note:**
>
> - If **TABLE_NAME** and **SCAN_ID** are both null in the same row, then the specific row provides the total purge duration and total records deleted across all tables and scan IDs in that purge activity.
> - The purge script creates the **PURGE_SEQ** sequence that is assigned to the **PURGED_RECORD_DATA.PURGE_ID** column.

- **PURGE_SCANS**: This table temporarily captures the scan IDs used by a purge activity. This table is used to avoid using any surplus IDs that are created during or after an initial purge script. The table contains **PURGE_SCANS.ENTITYID** that provides the scan entity IDs gathered from the DISSCANRUN table based on the required filter criteria. These IDs are populated by running the **REFRESH_SCANS** script.
- **PURGE_ERROR**: This table captures the details of any errors that occur during the purge activities. The table contains the following columns:
  - **PURGE_ERROR.PURGE_ID**: The purge ID for which error is observed.
  - **PURGE_ERROR.SCAN_ID**: The scan entity ID for which error is observed.
  - **PURGE_ERROR.TABLE_NAME**: The table name for which error is observed.
  - **PURGE_ERROR.ERROR**: The description of the error observed.

OCIM and NI Tables for Running Purge Scripts

You require OCIM and NI tables for running purge scripts.

When you run the purge scripts, the time taken and the volume of data purged from these tables is captured in the **PURGED_RECORD_DATA** table. The number of records purged in each table is captured against the corresponding OCIM or NI table name.

OCIM Tables Referred by Purge Scripts

The following OCIM tables are referred while running the purge scripts:

- DEVICEINTERFACE
- DEVICEINTERFACECONFIGITEM_CHAR
- DEVICEINTERFACE_CHAR
- DEVICEINT_PHYPORTREL
- DICONFIGURATIONITEM
- EQ_EQREL
- EQHOLDER_EQREL
- EQUIPMENT
- EQUIPMENT_CHAR

- EQUIPMENTHOLDER
- EQUIPMENTHOLDER_CHAR
- GROUPABLETYPE
- INVENTORYGROUP
- INVENTORYGROUP_CHAR
- INVGROUPREF
- INVGROUPREL
- LOGICALDEVICE
- LOGICALDEVICE_CHAR
- MEDIAINTERFACE
- PHYSDEVICE_EQREL
- PHYSICALDEVICE
- PHYSICALDEVICE_CHAR
- PHYSICALPORT
- PHYSICALPORT_CHAR
- PIPE
- PIPE_CHAR
- PIPEPIPETPREL
- PIPEREL
- SERVICECONFIGITEM_CHAR
- SERVICECONFIGURATIONITEM
- TRAILPATH
- TRAILPIPEREL
- TRAILPIPERELPIPEREL
- TRAILPIPERELTRAILPATHREL

NI Tables Referred by Purge Scripts

The following NI tables are referred while running the purge scripts:

- DIS_PARM_GROUP_CHAR
- DISADDRESS
- DISASSIMILATIONADDRESS
- DISCONFIG
- DISCONFIGBLACKOUTS
- DISDISCREPANCY
- DISDISCREPANCYCOUNTS
- DISINVENTORYADDRESS
- DISINVENTORYCONFIG
- DISPARAMETERGROUP

- DISRESULTGROUP
- DISROOTENTITYREF
- DISSCANADDRESS
- DISSCANRUN
- DISSCHEDULE
- DISSCOPE
- DISTAGGABLE
- DISTAGGABLESTAGS

Prerequisites for Running Purge Scripts

To run the purge scripts, you require the following permissions granted to the schema user:

- GRANT SCHEDULER_ADMIN TO <MDS Schema User>
- GRANT EXECUTE ON DBMS_LOCK TO <MDS Schema User>
- GRANT CREATE ANY VIEW TO <MDS Schema User>
- GRANT CREATE PROCEDURE TO <MDS Schema User>

> **Note:**
>
> Verify if the above permissions are granted during NI installation. If not, you must grant the permissions manually.

Running the Purge Scripts

To run the purge scripts:

1. Run stored procedures and functions in the following order, if they are not present:
   - WAIT_AND_GET_LEFOUT_JOBS
   - TIMESTAMP_DIFF_IN_MILLISECONDS
   - PURGE_DI_BATCH
   - PURGE_DI_CHAR_BATCH
   - PURGE_DICONFIGITEM_BATCH
   - PURGE_DICONFIGITEM_CHAR_BATCH
   - PURGE_EQUIP_BATCH
   - PURGE_EQ_CHAR_BATCH
   - PURGE_PHYSICALPORT_BATCH
   - PURGE_PHYSICALPORT_CHAR_BATCH
   - PURGE_SERVICECONFIGITEM_CHAR_BATCH
   - PURGE_SERVICECONFIGITEM_BATCH
   - OCIM_PURGE

- NI_PURGE_BATCH

> **Note:**
>
> Verify if the above stored procedures and functions are added during NI installation. If not, you must add them manually.

2. Run the **REFRESH_SCANS** script while setting **TIMELIMIT** with the date you plan to run the purge script.
   This script clears the existing entries and adds new scan IDs as per the selection criteria.

> **Note:**
>
> By default, this value is set to 30 which indicates that the script selects the data related to scans created 30 days or older to the purge activity.

3. Run the **OCIM_MAIN** script as follows:
   a. Run with multiple batches of fewer rows initially.
   b. (Optional) Customize the number of parallel jobs using the **parallel_jobs** variable, based on the CPU availability.
4. Run the **NI_MAIN** script.

> **Note:**
>
> You can customize the number of parallel jobs using the **parallel_jobs** variable. If required, you can tune the parallel job wait time by changing the lines 33 and 45 within the **NI_MAIN** script.

5. (Optional) To run the **OCIM_MAIN** and **NI_MAIN** scripts from a remote machine, use the bash shell scripts **startOCIMPurge** and **startNIPurge** in a local Linux environment. These scripts require the DB connection details or you can edit these scripts to set the connection details and then run the corresponding SQL script. The **nohup.out** file captures the log that is generated by running the script.

> **Note:**
>
> You require SQL*plus installed on the remote machine to run the **startOCIMPurge** and **startNIPurge** scripts.

6. Verify and resolve any errors occurred after running the **OCIM_MAIN** and **NI_MAIN** scripts.

Refreshing the Memory Space

After completing the purging activities, refresh the memory space so that you can use it for performing other tasks.

To do so:

1. Move the tables to refresh the space as follows:

   ```
   Alter table <tablename> move;
   ```

2. Rebuild the indexes.

8

About Troubleshooting Network Integrity

This chapter explains how to troubleshoot Oracle Communications Network Integrity. This chapter includes information about contacting Oracle Global Support and common troubleshooting scenarios.

See Network Integrity Installation Guide for information about troubleshooting upgrade or installation issues.

Troubleshooting Checklist

When any problem occurs, it is best to do some troubleshooting before you contact Oracle Global Support:

- You know your installation better than Oracle Global Support does. You know if anything in the system has been changed, so you are more likely to know where to look first.
- Troubleshooting skills are important. Relying on Global Support to research and solve all of your problems prevents you from being in full control of your system.

If you have a problem with your Network Integrity system, ask yourself these questions first:

- What exactly is the problem? Can you isolate it? For example, if it is a problem with an application, does it occur on one instance of the application, or all instances?

  Oracle Global Support needs a clear and concise description of the problem, including when it began to occur.
- What do the log files say?

  This is the first thing that Oracle Global Support asks for. Check the error log for the Product component you're having problems with.
- Have you read the documentation?

  Read the list of common problems and their solutions for Network Integrity. See "Common Problems and Their Solutions" for more information.
- Has anything changed in the system? Did you install any new hardware or new software? Did the network change in any way?
- Have you read the Release Notes?

  The Release Notes include information about known problems and workarounds.
- Does the problem resemble another one you had previously?
- Has your system usage recently jumped significantly?
- Is the system otherwise operating normally?
- Has response time or the level of system resources changed?
- Are users complaining about additional or different problems?
- Can you run clients successfully?
- Are any other processes on the system hardware functioning normally?

If you still cannot resolve the problem, contact Oracle Global Support. See "Getting Help for Network Integrity Problems" for more information.

Using Error Logs to Troubleshoot Network Integrity

Network Integrity error log files provide detailed information about system problems. If you're having a problem with Network Integrity, look in the log files.

Log files include errors that must be managed, or errors that do not need immediate attention (for example, invalid login attempts). To manage log files, you should make a list of the important errors for your system, as opposed to errors that do not need immediate attention.

Common Problems and Their Solutions

This section describes the following problems, and how to resolve them:

Problem: Error While Exporting Content to Excel

If you are using Internet Explorer for your browser, enable the file download setting in the browser to allow data export from Network Integrity into Microsoft Excel.

To enable file download setting:

1. In the Internet Explorer browser window toolbar, click **Tools**, and then select **Internet Options**.

   The Internet Options dialog box is displayed.
2. Select the **Security** tab.
3. Do any one of the following:
   - If the browser does not have any default settings:
     a. Click **Reset all zones to default Level**.
     b. Click **Apply** and then click **OK**.
   - If default settings exist:
     a. Click **Custom Level**.

        The Security Settings dialog box is displayed.
     b. Scroll down to **Downloads** and enable **Automatic prompting for file downloads**.
     c. Click **OK**.
4. Click **Apply** and then click **OK**.

5. Close the browser window and open it again.

Problem: Scan Failure When Transferring Files to or from a Server Using SFTP

A configured scan using a file transfer based cartridge with the **Transfer Type** field set to SFTP fails, showing the following message in the **Address** field of the Network Integrity Scan Result page:

```
No Configuration was registered that can handle the configuration named
com.sun.security.jgss.krb5.initiate.
```

An exception is also written in the log file.

To resolve this issue, do the following:

1. For each WebLogic Managed Server, edit the *NI_Domain_Home***/bin/startWebLogic.sh** startup script, where *NI_Domain_Home* is the directory where your Network Integrity domain is installed.
   a. Locate the section of the script that starts the WebLogic Server (as shown in the following example) and insert the following JVM option:

      ```
      # START WEBLOGIC
      echo "starting weblogic with Java version:"

      JAVA_OPTIONS = "${JAVA_OPTIONS} -Djava.security.auth.login.config=$
      {DOMAIN_HOME}/bin/login.conf"
      ```

   b. Save and close the **startWebLogic.sh** startup script.
2. In the *NI_Domain_Home***/bin/** directory for each Managed WebLogic Server, create a **login.conf** file with the following content:

   ```
   com.sun.security.jgss.krb5.initiate {
       com.sun.security.auth.module.Krb5LoginModule required
       doNotPrompt=true useTicketCache=true;
   };
   ```

3. Restart each managed WebLogic Server.

Problem: Cartridge Deployment/Undeployment Errors and Failures

Cartridge deployment or undeployment may fail or generate errors for many different reasons, including the following:

- Failure While Restarting the Network Integrity Application
- Cartridge Deployment/Undeployment Procedure Stops Responding

Failure While Restarting the Network Integrity Application

Cartridge deployment can fail while restarting Network Integrity because of low memory or because the database server is down.

Ensure Network Integrity is in the Active state:

1. Log on to the Oracle WebLogic Server Administration Console.
2. Click **Deployments**.

3. In the Deployments table, confirm that the state of the deployed Network Integrity application is **Active**.

   If the Network Integrity application is not Active, you must activate it for cartridge deployment and undeployment errors.

To change the state of the Network Integrity application to Active for deployment errors:

1. Stop the server where Network Integrity is installed.
2. Delete the **NetworkIntegrity.ear** from the **deploy** directory.
3. Rename the **NetworkIntegrity.ear.bak** to **NetworkIntegrity.ear**.

> **Note:**
>
> The **NetworkIntegrity.ear.bak** file is created by the Cartridge Deployer Tool in the same directory as **NetworkIntegrity.ear**.

4. Change the value in the Status column from **RUNNING** to **FAILED** in the DisCartridgeStatus table, as follows:
   a. Log in to the Network Integrity database schema as the MDS user using any SQL editor.
   b. Expand the **Tables** node (available in SQL Developer/JDeveloper).
   c. Select the **DisCartridgeStatus** table.
   d. In the Status column, change the value to **FAILED**.
5. Start the server where Network Integrity is installed.
6. Deploy the **NetworkIntegrityApp.ear** file again.

To change the state of the Network Integrity application to Active for undeployment errors:

1. Stop the server where Network Integrity is installed.
2. Delete the **NetworkIntegrity.ear** from the **deploy** directory.
3. Rename the **NetworkIntegrity.ear.bak** to **NetworkIntegrity.ear**.
4. Change the value in the Status column from **RUNNING** to **FAILED** in the DisCartridgeStatus table, as follows:
   a. Log in to the Network Integrity database schema as the MDS user using any SQL editor.
   b. Expand the **Tables** node (available in SQL Developer/JDeveloper).
   c. Select the **DisCartridgeStatus** table.
   d. In the Status column, change the value to **FAILED**.
   e. In the Command column, change the value from **undeploy** to **deploy**.
5. Start the server where Network Integrity is installed.
6. Deploy the **NetworkIntegrityApp.ear** file again.

Cartridge Deployment/Undeployment Procedure Stops Responding

The Cartridge deployment or undeployment procedure can stop responding because the WebLogic Server Administration Console is locked for editing.

To determine if the WebLogic Server Administration Console is locked for editing:

1. Log on to the Oracle WebLogic Server Administration Console.
2. In the Chance Center, in the left pane of the Administration Console, **Lock & Edit** should be in the Enabled state.

   If the WebLogic Server Administration Console is locked for editing, you must unlock it. Refer to the Oracle WebLogic Administration Console documentation for more information.

To resolve issues with the deployment or undeployment procedure not responding, perform the troubleshooting steps from "Problem: Scan Failure When Transferring Files to or from a Server Using SFTP".

Problem: Inability To Run Scans or Resolve Discrepancies After an Upgrade

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. See Network Integrity Installation Guide for more information.

Problem: Error Message in Network Integrity GUI is Truncated

If you receive an error message in the Network Integrity GUI and the error message is truncated, refer to the logs for the complete information.

Problem: Error While Logging into Network Integrity

An error occurs while logging into Network Integrity, showing the following error message:

```
Failed to open runtime service.
```

The WebLogic domain log shows the following error message:

```
java.sql.SQLException:ORA-28001: the password has expired
```

This error occurs due to the Network Integrity database schema password expiring.

To resolve this issue, update the data source configuration in the WebLogic server.

Problem: Removed Scan Parameter Group is Displayed for the Action After the Cartridge is Redeployed

If you remove a scan parameter group from an action, redeploy the cartridge, and then create a scan for the action; the removed scan parameter group is still displayed for the action.

To resolve this issue, do the following:

1. Log in and connect to the Network Integrity database schema (MDS user).
2. Run the following SQL script:

```
/* This SQL script deletes the relationship between displugin and scan parameter
group specification in the DISPLUGIN_DISPGSPEC table. */
DELETE FROM DISPLUGIN_DISPGSPEC WHERE DISPLUGIN = (SELECT ENTITYID FROM DISPLUGIN
WHERE PLUGINNAME = scan_action_name) AND  DISPARAMETERGROUPSPECIFICATION = (SELECT
ENTITYID FROM SPECIFICATION
WHERE ENTITYCLASS= 'DisParameterGroupSpecificationDAO' AND NAME=
scan_parameter_group_name)
```

where:

- *scan_action_name* is the name of your scan action
- *scan_parameter_group_name* is the name of your scan parameter group
- DISPLUGIN is the Network Integrity database table that stores the scan actions
- SPECIFICATION is the Network Integrity database table that stores all the specifications

> **Note:**
>
> If you have multiple scan parameter groups in a scan action, modify the SPECIFICATIONSORDER column in the DISPLUGIN_DISPGSPEC table to display the scan parameter groups in the required order within the Network Integrity UI.

Getting Help for Network Integrity Problems

If you cannot resolve any problems in the product, contact Oracle Global Support.

Before Contacting Oracle Global Support

Problems can often be fixed by shutting down Network Integrity and restarting the computer that it runs on. See "About Managing Network Integrity" for more information.

If that does not solve the problem, the first troubleshooting step is to look at the error log for the application or process that reported the problem. See "Using Error Logs to Troubleshoot Network Integrity" for more information.

Be sure to review the troubleshooting checklist before contacting Oracle Global Support. See "Troubleshooting Checklist" for more information.

Reporting Problems

Prepare and gather the following pertinent information:

- A clear and concise description of the problem, including when it began to occur.
- Relevant portions of the relevant log files.
- Relevant configuration files.
- Recent changes in your system, even if you do not think they are relevant.
- List of all Network Integrity components and patches installed on your system.

When you are ready, report the problem to Oracle Global Support.