Oracle® Communications Network Integrity

Concepts

Release 7.5
G13624-01
December 2024

ORACLE

Oracle Communications Network Integrity Concepts, Release 7.5

G13624-01

Contents

Preface

This guide provides an overview of Oracle Communications Network Integrity, explaining its functional architecture, and describing its features and components.

Audience

This document is intended for Network Integrity users and planners, system administrators and integrators.

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

About Network Integrity

Network Integrity enables you to keep two data sources (such as an inventory system and a live network) synchronized, improving data accuracy, which increases your service provisioning success rate. It enables better business planning, based on having an accurate view of your inventory, and supports scheduled or ad-hoc audits to ensure alignment of inventory with your network. Network Integrity can also be used as a convenient way to load network data into your inventory system.

How Network Integrity Works

Network Integrity compares two sets of data to identify and facilitate the correction of differences between the data sets.

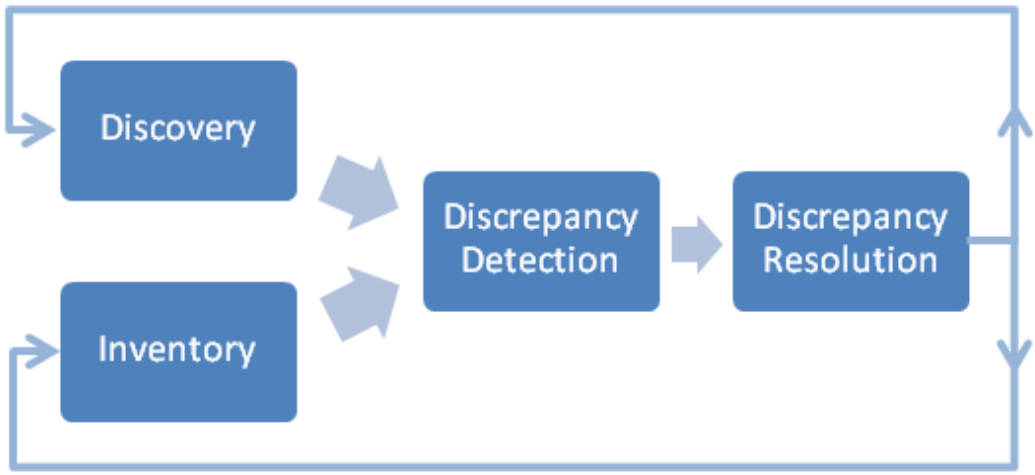
Use Network Integrity to discover network data (such as network elements, resources, and services) using discovery or assimilation scans. Use Network Integrity to import inventory data using an import scan. You can filter scan results by specifying search criteria.

The discovered data is compared with the imported data to generate lists of discrepancies, which are instances where the data from the two data sources do not match. Discrepancies can be shown for relevant entities of the device or for other objects. You can select an entity to show a side-by-side comparison of the discovered view and the inventory view. You can then resolve an individual data discrepancy or several data discrepancies.

You can even generate reports from the discovery, import, or discrepancy information.

Figure 1-1 illustrates a typical Network Integrity discovery and discrepancy resolution process flow.

Figure 1-1 Network Integrity Typical Process Flow



The typical Network Integrity process flow is:

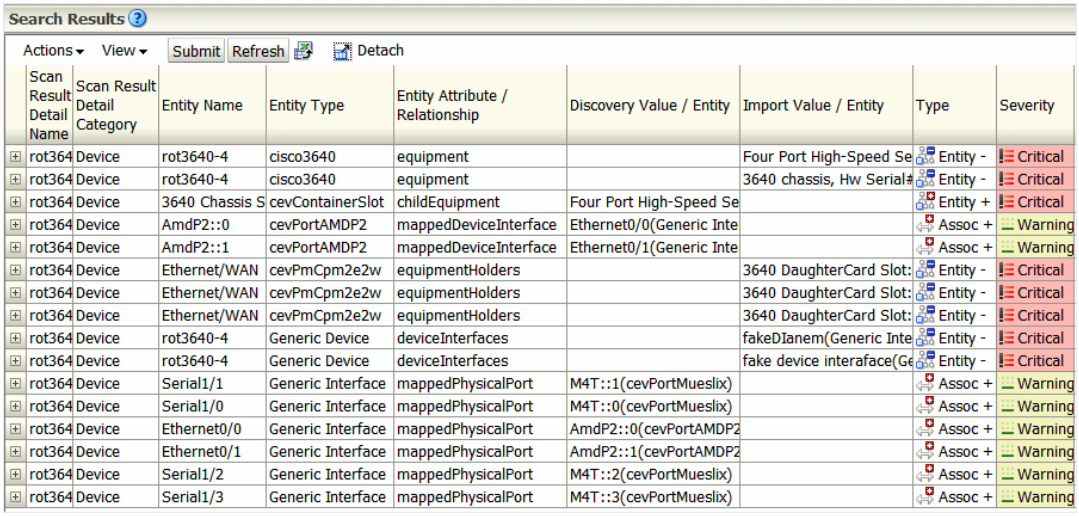
1. Run an import scan to import inventory data from an inventory system.
2. Run a discovery or assimilation scan, to discover or assimilate network data from a network system, with the **Detect Discrepancies** option enabled.

   Elements, physical resources, and logical resources in the network are discovered by scanning Network Elements (NEs), Element Management Systems (EMSs), and Network Management Systems (NMSs). For example, you poll an NE to find all ports and to determine whether each port is free or assigned, or you poll an optical EMS to find unused ports.
3. Discovered or assimilated entities are matched with the inventory view of networks and services and generate discrepancies. For example, you match the discovered NE and each port on it with objects in inventory.

   See "Managing Scans and Viewing Scan Results" for more information.
4. Discrepancies are evaluated in the Network Integrity UI, or by viewing generated reports, which can be studied to obtain a deeper understanding of the inventory discrepancies.

   For more information, see "About Discrepancy Detection, Review, and Resolution" and "About the Reporting Solution".

Figure 1-2 Network Integrity UI View of Discrepancies



Scan Result Detail Name	Scan Result Detail Category	Entity Name	Entity Type	Entity Attribute / Relationship	Discovery Value / Entity	Import Value / Entity	Type	Severity
rot364	Device	rot3640-4	cisco3640	equipment		Four Port High-Speed Se	Entity -	Critical
rot364	Device	rot3640-4	cisco3640	equipment		3640 chassis, Hw Serial#	Entity -	Critical
rot364	Device	3640 Chassis S	cevContainerSlot	childEquipment	Four Port High-Speed Se		Entity +	Critical
rot364	Device	AmdP2::0	cevPortAMDP2	mappedDeviceInterface	Ethernet0/0(Generic Inte		Assoc +	Warning
rot364	Device	AmdP2::1	cevPortAMDP2	mappedDeviceInterface	Ethernet0/1(Generic Inte		Assoc +	Warning
rot364	Device	Ethernet/WAN	cevPmCpm2e2w	equipmentHolders		3640 DaughterCard Slot:	Entity -	Critical
rot364	Device	Ethernet/WAN	cevPmCpm2e2w	equipmentHolders		3640 DaughterCard Slot:	Entity -	Critical
rot364	Device	Ethernet/WAN	cevPmCpm2e2w	equipmentHolders		3640 DaughterCard Slot:	Entity -	Critical
rot364	Device	rot3640-4	Generic Device	deviceInterfaces		fakeDIanem(Generic Inte	Entity -	Critical
rot364	Device	rot3640-4	Generic Device	deviceInterfaces		fake device interaface(Ge	Entity -	Critical
rot364	Device	Serial1/1	Generic Interface	mappedPhysicalPort	M4T::1(cevPortMueslix)		Assoc +	Warning
rot364	Device	Serial1/0	Generic Interface	mappedPhysicalPort	M4T::0(cevPortMueslix)		Assoc +	Warning
rot364	Device	Ethernet0/0	Generic Interface	mappedPhysicalPort	AmdP2::0(cevPortAMDP2		Assoc +	Warning
rot364	Device	Ethernet0/1	Generic Interface	mappedPhysicalPort	AmdP2::1(cevPortAMDP2		Assoc +	Warning
rot364	Device	Serial1/2	Generic Interface	mappedPhysicalPort	M4T::2(cevPortMueslix)		Assoc +	Warning
rot364	Device	Serial1/3	Generic Interface	mappedPhysicalPort	M4T::3(cevPortMueslix)		Assoc +	Warning

5. Discrepancies are corrected using Network Integrity. You can make individual or bulk corrections. Network Integrity synchronizes the discovered data with the inventory reference data. You can assign, rank and annotate discrepancies. Using the UI to perform synchronization reduces the likelihood of errors, compared to making changes manually, and better supports a multi-user environment.

Benefits of Network Integrity

Network Integrity offers a number of benefits for optimizing resource use and increasing provisioning efficiency.

Identifying Stranded Assets

Network Integrity allows you to locate stranded network assets. These are resources that you have, but which don't appear in your inventory. You save capital investment by using all existing resources effectively, rather than obtaining new resources prematurely.

Minimizing Fallout in Flow Through Service Fulfillment

Maintaining an accurate representation of your network means that any service fulfillment activities are more likely to complete successfully, and as designed, without going to fallout, or requiring manual intervention. This means that services are delivered more quickly, and less expensively.

Ensuring Inventory Accuracy for Operations And Planning

With an accurate view of your network, you can plan and provision new services effectively and efficiently. Network element issues can be pinpointed faster and resolved more efficiently.

Automating Manual and Error Prone Procedures

Provisioning errors due to incorrectly identified or unavailable network resources are costly to fix and detrimental to customer satisfaction. Network Integrity allows you to determine where the problems are, and what the root cause is. It then allows you to efficiently resolve these issues (which can be an error-prone activity if performed manually).

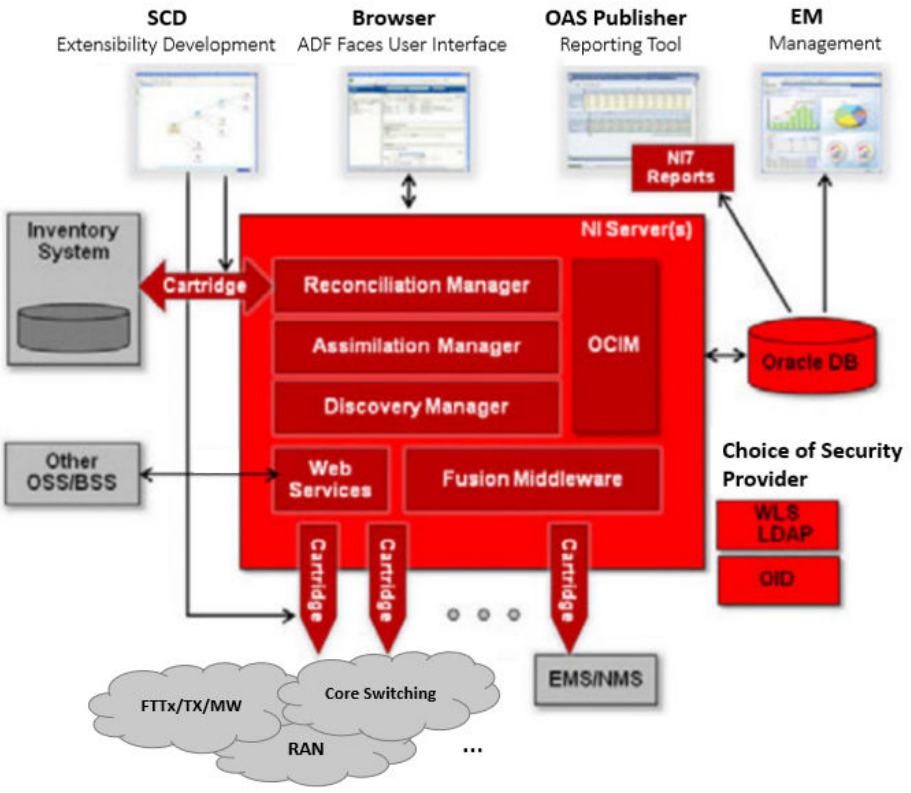
Quick Inventory Creation

Network Integrity automates the population of your inventory, reducing potential errors compared to manually discovering and recording this information. This increases efficiency and reduces organizational costs.

About the Network Integrity Architecture

Figure 1-3 outlines the Network Integrity architecture.

Figure 1-3 Network Integrity Architecture



Network Integrity runs on Oracle WebLogic Server, and includes the following features and functions:

- Support for cartridges developed in Oracle Communications Service Catalog and Design - Design Studio, to provide extensibility. See "Using Service Catalog and Design - Design Studio for Network Integrity".
- A browser-based web UI based on Oracle Fusion Middleware ADF Faces technology which provides a single user experience for network discovery and data reconciliation. The web UI supports localization. See "About the Network Integrity UI".
- Reporting provided by Oracle Business Information (BI) Publisher (optional) or other third-party solution. See "About the Reporting Solution".
- Reference implementations are provided against Oracle Communication Unified Inventory Management (UIM) and MetaSolv Solution (MSS) for the import of data and resolution of discrepancies; support for other third-party systems is possible through extensibility. See "Integrating with Inventory Systems".
- Support for the Oracle Communications Information Model, which is based on the TM Forum's Information Framework (SID). See "Integrating with UIM".

> **Note:**
>
> Network Integrity 7.4.0 supports Oracle Communications Information Model 7.3.0. For specific technical details about the Oracle Communications Information Model and the Network Integrity information model, see *Oracle Communications Information Model Reference* and *Network Integrity Information Model Reference*.
>
> *Oracle Communications Information Model Reference* and *Network Integrity Information Model Reference* are located in Network Integrity Developer Documentation on the Oracle software delivery website.

- Runs on Oracle Fusion Middleware platform. See "About Oracle Fusion Middleware Platform".
- SOA-based JEE compliant web services API to facilitate customized solutions for external management of Network Integrity. See "Managing Network Integrity Using the Web Services API".
- Support for application and database clustering for scalability and high availability.
- Able to integrate with external Security Providers, preventing replication of user accounts and credentials in Network Integrity. See "About User and Identity Management".

About the Network Integrity UI

You use the browser-based web UI to carry out discovery and reconciliation by configuring and scheduling scans, reviewing scan results, and reviewing and resolving data discrepancies.

Features offered by the Network Integrity web UI include:

- Integrated search functionality: A flexible search function supporting both basic and advanced searches for objects in Network Integrity such as scans. Advanced searches support the specification of multiple values for a particular field. This search functionality provides comprehensive historical results access with filtering options.
- Intuitive functions and layout: The Network Integrity UI supports a robust, predictable range of user interactions, which make it easy to learn and use. Icons trigger functions such as object creation and deletion. Menus are accessed as standard drop-downs, or by right-clicking on objects. Drag and drop is supported and data sorting is provided in all tables. Table columns can be moved, resized and hidden. Multiple object selection is supported. UI panels can be collapsed and expanded, detached and re-attached.
- Links panel: Frequently used web links can be placed in the Links panel by the system administrator. For example, you can store links to an inventory system login page or to the technical specifications for equipment on the network.
- Context-sensitive online Help: The Network Integrity UI provides field-level online Help that offers detailed content on supported functions and features.
- Internationalization and localization: The Network Integrity UI supports custom localization, allowing the GUI to be presented in different languages.

Using Service Catalog and Design - Design Studio for Network Integrity

Service Catalog and Design - Design Studio is a design-time platform and graphical service creation environment that enables you to design, build, and deploy cartridges. Design Studio supports multiple Oracle Communications applications including Network Integrity. You can use the same Design Studio instance for multiple Oracle Communications products.

Design Studio is based on Eclipse, a popular, open-source development environment. Design Studio provides an integrated development environment to support plug-in configuration and customizations.

You use Design Studio for Network Integrity to develop and deploy Network Integrity cartridges that extend Network Integrity for various environments, applications, or implementations. Network Integrity's cartridge-based architecture promotes cartridge and artifact reuse and extensibility. For example, you can extend Network Integrity with cartridge-based Actions and Address Handlers. Each cartridge is created or customized using Design Studio GUI wizards and editors that:

- Validate the integrity of configurations.
- Generate cartridge Java code and other cartridge artifacts.
- Build the cartridge code.
- Package the cartridge artifacts into deployable files.

Although many of the cartridge artifacts are produced automatically, you may have to manually write some Java code to complete the cartridge implementation. Cartridges offered by Network Integrity offer:

- Network discovery
- Inventory import
- Data assimilation
- Discrepancy detection
- Discrepancy resolution

About Network Integrity Security

Network Integrity conforms to Oracle security standards. Network Integrity should be installed as securely as possible and configured to listen to, read, and write data as securely as possible, to protect the integrity of the information it accesses.

"Network Integrity Security Overview" in *Network Integrity Security Guide* outlines all Network Integrity security features and explains how to install and configure Network Integrity securely.

2

About Scans and Discrepancies

This chapter describes the various scans that can be carried out using the Network Integrity UI. It also describes the different types of discrepancies that NI reports.

Managing Scans and Viewing Scan Results

Management and viewing of discovery scans is carried out using the Network Integrity UI. By carrying out scans and viewing and correcting discrepancies, you can keep your inventory synchronized with your network and with other systems. Through cartridge extensibility, Network Integrity can potentially discover any type of network, service, or data source.

Types of Scans

A scan is a set of configurations used to perform a Network Integrity operation. Configurations can include discovery operations, constraints on what parts of the network are discovered, and so on.

Network Integrity supports the following types of scans:

- **Discovery scan**: A discovery scan discovers your network. This can include network elements, physical resources, and logical resources. As part of the scan, you can specify network connection information such as name, port, community string, and time-out values. Network Integrity includes the following discovery scans:
  - **Discover Generic SNMP**: Scans all types of Generic Vendor Device and models its physical and logical device tree.
  - **Discover MIB II SNMP**: Discovers MIB II RFC1213, IF MIB RFC1573, IP-MIB for IPv6, and uses IANA MIB for support. Retrieves device information (including name, description, sysObjectId, and mgmtIpAddress) and interface details (including name, description, type, speed, status, alias and more) and uses the information to model the logical tree.
  - **Discover TL1**: Scans one or more TL1 devices to retrieve device information and interface details, modeling the discovered data in the Information Model.
  - **Discover TMF814**: Scans both physical (equipment) and logical (interface) hierarchy details of managed elements using the TMF814 CORBA interface as its discovery protocol and models the physical and logical tree.
  - **Discover Alcatel 1359IOO RI**: Scans one or more Alcatel 1359IOO RI CSV file instances in a directory, resulting in hierarchical physical device model instances.
  - **Discover Ericsson XML**: Scans one or more XML device file instances, resulting in multiple hierarchical device model instances.
  - **Discover WDM Services:** Discovers the DWDM entities like Client, OCH, ODUFlex, ODU, OTU, OMS using the TMF814 CORBA interface as its discovery protocol.
  - **Discover IMS Network FTP:** Discovers devices in IMS network over FTP protocol and models physical and logical hierarchies. This action also models the associations between the physical and logical hierarchies.

  - **Discover Optical Devices FTP:** Discovers Optical devices over FTP protocol and models physical and logical hierarchies. This action also models the associations between the physical and logical hierarchies.
  - **Discover Microwave Devices:** Discovers Microwave devices using FTP protocol and models physical and logical hierarchies. This action also models the associations between the physical and logical hierarchies.
  - **Discover SDH Connectivity and Service:** Discovers SDH entities like Topological links, Trails, Tunnel and Services using FTP protocol. It also assimilates end to end circuit stitching.
  - **Discover Generic SNMP Device:** Scans a Generic device using SNMP protocol and model discovered data to physical and logical tree.

  For more details about the above discovery scans, refer to their respective cartridge guides.

- **Assimilation scan**: An assimilation scan produces additional scan results from existing scan results. When configuring an assimilation scan, you can choose additional scans to serve as input to the assimilation scan. Network Integrity includes the following assimilation scans:
  - **Assimilate Optical Circuits**: Scans optical model input files, tracing and modeling end-to-end circuits.
  - **Assimilate IP Links:** Scans discovery result of devices provided as input, discovers and models links between the devices.
- **Import scan**: An import scan imports network data from an inventory system. Network Integrity includes the following import scans:
  - Import MIB II from UIM
  - Import from MSS
  - Import WDM Services
  - Import SDH Connectivity and Service from UIM
  - Incremental Import SDH Connectivity and Service From UIM
  - Import Logical Optical from UIM
  - Import Optical from UIM
  - Incremental Import from UIM
  - Import IP Links from UIM

Network Integrity supports the simultaneous processing of multiple scans.

See the appropriate cartridge guide for more information about the above mentioned scans.

Creating Scans

Network Integrity uses cartridges to provide support for accessing different types of inventory targets and to specify scan actions for them. A scan typically specifies a scan action and scan action parameters, such as protocol and vendor properties, addresses (scope), and schedules.

You can associate a scan with one or more tags that define or describes the scope of the scan. Tags are customizable, and can relate to geography, ownership, network type, or other references.

Scans support multiple IP address formats, including IPv4, IPv6, wildcards, and ranges. You can enter the IP addresses manually or import them from a file, and multiple IP address

specifications can be combined into one scan. For example, you can carry out a discovery scan using a combined IPv4, IPv6, and Domain Name System (DNS) host name configuration.

To search within a scope while editing or creating a Discovery scan:

1. From the Tasks panel, click **Manage Scans**.

   The Manage Scans page appears.
2. Do one of the following:
   - Click the Create icon on the **Search Results** table.

     The Create Scan page appears.
   - Select a scan record and click the Edit icon.

     The Edit Scan page appears.
3. Go to the **Scope** tab.
4. Select an option for **Search Scope** and enter the corresponding value.
5. Click **Search**.

   The scan is created or edited according to the scope.
6. (Optional) Enter a value in the text field and click the Add Address icon to add a network address.
7. (Optional) From the Network Address table, select a record and click the Delete Address icon to delete the network address.

Setting Scan Schedules and Blackout Periods

The scan schedule determines when a scan runs. You can set a scan to run immediately, regularly, or on-demand. The frequency with which scans repeat is configurable. For example, you can set scans to repeat at monthly intervals, on the last day of the month, or at a set time every night.

A blackout window defines a period of time when a specified scan should not run, or be paused if already running. This can be used to avoid running scans during peak network traffic hours, or during a planned network outage. The scheduling options available for blackout windows are identical to those for scheduling scans.

Viewing Scan Results

When a scan runs, the Scan Results table lists the outcomes for one or more Network Integrity scans. Each scan is defined by scan name and by scan action type associated with the scan - discovery, import, or assimilation. In addition, the table identifies the data source assigned to each scan, the current status of the scan (in progress, completed, completed with errors).

The scan results list the date and duration of the scan run and details of errors in the scan. If selected, the summary of detected discrepancies is presented.

All scan data is presented in one place, and filtering and sorting are supported, so you can get to the key data to identify issues. By selecting individual scan result details, you can drill down to entity details, and to individual entity attributes.

Filtering Scan Data

You can filter the search results for devices based on one or multiple resource names. This helps you to view information about specific devices. You can filter the search results according to one or more resource names.

To filter scan results:

1. Open NI user interface.
2. Go to **Display Scan Results**.
3. Click on a scan record to view the discovery scan results.
4. Go to **Resource Name** and use the filter option to choose either of the following options:
   - Equals
   - Contains
   - Starts with
   - Ends with
5. Enter the device name in the text field for the resource name.
6. Click **Search**

   The search result displays the devices with the entered names.
7. (Optional) You can view the device search results for multiple names as follows:
   a. Enter the device names separated with commas.
   b. From the filter, select **Contains**.
   c. Click **Search**.

   The search result displays all devices with the entered name.

About Discrepancy Detection, Review, and Resolution

Discrepancy detection is the process where Network Integrity compares discovered network data with imported inventory data and reports on differences between the sets of data. Discrepancy detection is an optional part of a scan run.

Network Integrity reports the following types of discrepancies:

- **Attribute Value Mismatch:** An entity exists in both the network and the inventory results, but an attribute has different values.
- **Extra or Missing Entity:** An entity (or any dependent children) is present in one set of results but is missing from the other side.
- **Extra or Missing Association:** An association exists for an entity in one set of results, but is missing from the other side.
- **Ordering or Association Ordering Error:** Matching entities or associations appear in different orders in the network and inventory results.

You can edit the details of a discrepancy, ignore the discrepancy, or send details of the data discrepancies to an external system. See "Integrating with Inventory Systems".

Discrepancy review is facilitated by extensive search capabilities, a color-coded severity system, and the ability to assign a priority and owner to each discrepancy. You can also store notes to track progress and enhance an audit trail.

Discrepancy resolution enables you to carry out in-context correction, multiple corrective actions, or bulk discrepancy correction. You can also ignore certain discrepancies. You can use Design Studio to create cartridges that extend Network Integrity to discover new types of devices, to import from different inventory systems, or to enhance Network Integrity to automatically resolve discrepancies.

For more information about discrepancies, discrepancy detection, discrepancy resolution, or cartridge creation, see "Using Design Studio to Extend Network Integrity" in *Network Integrity Developer's Guide*.

3

Integrating NI with Inventory Systems

This chapter provides an overview on integrating Network Integrity with external inventory systems.

Integrating with Inventory Systems

Network Integrity can integrate with external inventory systems, including UIM and MSS, to retrieve inventory details, and send resolution commands.

By default, Network Integrity uses the Oracle Communications Information Model as a common model for reading and writing data to and from an inventory system. The Information Model describes information and data concepts, structures, and patterns, and its use reduces complexity and integration time.

The basic workflow when Network Integrity integrates with an inventory system is as follows:

- Run an import scan to import data from the inventory system.
- Run a discovery scan to discover your network. Ensure that discrepancy detection is enabled.
- Review the discrepancies raised by Network Integrity.
- Resolve discrepancies.

  See the appropriate cartridge guide for information about which discrepancies can be resolved from Network Integrity and uploaded to your inventory system, and which discrepancies must be manually corrected in your inventory system.

Integrating with UIM

Network Integrity integrates with UIM using reference cartridges. The cartridges can be extended to meet the particularities of your UIM deployment. Network Integrity can retrieve inventory information from UIM, and communicate actions back to UIM to resolve discrepancies. The Network Integrity download includes UIM reference cartridges and sample cartridge packs for modeling logical and physical device hierarchies.

Network Integrity and UIM both use Design Studio to design and deploy the cartridges that enable extensibility and integration.

Integrating with MSS

Network Integrity integrates with MSS using reference cartridges. The cartridges can be extended to meet the particularities of your MSS system. Network Integrity can retrieve inventory information from MSS, and communicate actions back to MSS to resolve discrepancies. The Network Integrity download includes one MSS reference cartridge for modeling logical and physical device hierarchies.

Network Integrity uses Design Studio to design and deploy the cartridges that enable extensibility and integration.

4

Managing Network Integrity

This chapters provides an overview on managing Network Integrity.

About Managing Network Integrity

You use the following tools to manage Network Integrity:

- Oracle WebLogic Server Administration Console
- Oracle Enterprise Management Fusion Middleware Control
- Oracle Enterprise Management Grid Control

Network Integrity uses the Oracle WebLogic Server Administration Console primarily for application server management functions, and optionally for user management (only when the WebLogic Embedded LDAP server is used as the security provider). For complete details on monitoring and managing all aspects of Network Integrity, refer to the "Network Integrity System Administration Overview" in *Network Integrity System Administrator's Guide*.

About Oracle Fusion Middleware Platform

Network Integrity is built on the Oracle Fusion Middleware platform, an industry-standard, open standards-based suite of services. Components of this platform include Oracle WebLogic Application Server and a range of middleware options such as:

- Oracle Analytics Publisher
- Oracle Identity Manager
- Oracle Enterprise Management Fusion Middleware Control

Oracle Fusion Middleware is licensed separately from Network Integrity.

About the Reporting Solution

Network Integrity provides an open reporting interface to support reporting applications and a documented data store for integration with these reports. You use a reporting application to generate, view and extend reports based on data collected during discovery and reconciliation scans. Reports can be available in various formats such as HTML, PDF, RTF, and Microsoft Excel format.

Network Integrity is pre-integrated with Oracle Analytics Publisher. Pre-loaded report templates and sample reports which are tailored for use with Network Integrity are provided. These can be further customized to meet your needs. Examples of provided sample Oracle Analytics Publisher report templates are:

- Scan History Report
- Discrepancy Corrective Action Report
- Discovery Scan Summary Report
- Device Discrepancy Detection Summary Report

- Device Discrepancy Detection Detailed Report

OA Publisher is optional and is separately licensed.

You can use a third-party reporting tool to run reports on Network Integrity.

About Scalability and Reliability

Network Integrity is a scalable solution that can be expanded to accommodate network growth. Oracle RAC is supported, making the database reliable and highly available.

About User and Identity Management

Any compatible Security Providers can be used for user access and identity management. As a result, Network Integrity can be integrated into an enterprise's existing security infrastructure. Network Integrity is validated with Oracle WebLogic Server Embedded LDAP and Oracle Internet Directory 11*g*. User access and identity management are supported by:

- Embedded LDAP, as part of the Oracle WebLogic Administration Management Console
- Oracle Internet Directory 11*g*
- Third-party identity management system

For more information on Oracle Internet Directory, see the documentation for Oracle Identity Management Suite 11*g*. Oracle Identity Management allows enterprises to manage the end-to-end life cycle of user identities across enterprise resources independently from enterprise applications. This allows you to separate business logic from security and resource management.

Managing Network Integrity Using the Web Services API

You can manage Network Integrity from external applications using the web services API. Network Integrity's web services are consistent with Oracle's SOA strategy and allow interoperability with Oracle Fusion Middleware Suite. The Network Integrity web services API reduces the complexity of integration and supports:

- Scan management: Enables scans to be created, run, configured, stopped, and queried without using the user interface. Ad hoc scans can be triggered through the API, allowing quick response to customer inquiries.
- Scan result retrieval: Allows scan results to be fetched directly from the database.
- Resolution actions: To reconcile with inventory and other applications.
- Common UI functions.

The Network Integrity web services API is standards-based. It supports JAX WS over HTTP, uses asynchronous calls, and shares a common security framework with the user interface.

To illustrate the range of web services API support, Network Discovery-related API calls include functions to:

- Create, Get, Update, and Delete Discovery Scans
- Create, Get, Update, and Delete Blackout Schedule
- Start and Stop Discovery Scans
- Get Latest Scan Status
- Get Discovery Results

For details on all the web services API calls, and on working with the samples, see "Using Design Studio to Extend Network Integrity" in *Network Integrity Developer's Guide* and "Overview" in *Network Integrity UIM Integration Cartridge Guide*.

A
Glossary

action

Action is an entity that represents a particular software function that a deployed cartridge performs at run time. A cartridge project usually contains multiple actions.

artifact

A general term for something you can create and define in Design Studio, such as custom actions and processors.

assimilation scan

A scan that produces additional scan results from existing scan results. When configuring an assimilation scan, you can choose additional scans to serve as input to the assimilation scan.

blackout window

Defines a period of time when a specified scan should not run, or be paused if already running. This can be used to avoid running scans during peak network traffic hours, or during a planned network outage.

cartridge

A collection of actions, specifications, model collections, and scan parameter groups defined in Design Studio. Cartridges are built in Design Studio from projects. They are compiled as JAR files and then deployed into Network Integrity.

characteristic

A data element that can be added to entity specifications to supplement default data elements. Characteristics on specifications appear in the Network Integrity UI as displayed information.

discovery scan

A scan that discovers your network. This can include network elements, physical resources, and logical resources.

discrepancy detection

The process where Network Integrity compares discovered network data with imported inventory data and reports on differences between the sets of data. Discrepancy detection is an optional part of a scan run.

discrepancy resolution

The process where Network Integrity resolves discrepancies between discovered network data and imported inventory data.

import scan

A scan that imports network data from an inventory system.

model collection

Used to add specifications that exist in other cartridge projects into your cartridge project. Specifications from other cartridge projects inherit any changes and configurations you make to them in their original cartridge project.

processor

Each processor is responsible for an atomic function. An action contains one or more processors. When an action is invoked, the processors are run in the sequence they were placed inside the action.

scan parameter group

A special type of specification that adds fields to the Network Integrity UI. For example, you can add fields to the Create Scan page, allowing the Network Integrity user to pass scan parameter values to run-time scans.

scan results

Information related to outcomes for one or more Network Integrity scans, such as scan name, scan action type associated with the scan (discovery, import, or assimilation), data source assigned to each scan, current status of the scan (in progress, completed, completed with errors), date and duration of the scan run, details of errors in the scan, and a summary of detected discrepancies.

scan schedule

Determines when a scan runs. You can set a scan to run immediately, regularly, or on-demand.

specification

You use specifications to extend the Information Model, which defines a base set of entities and their relationships. Most cartridges must extend the Information Model entities and therefore must make use of specifications. A specification used for model extension is associated with a single Information Model entity type. Multiple specification types can be defined for each Information Model entity type.

specification helper

Special class that Design Studio generates for specifications.