Oracle® Communications Network Integrity

Release Notes

Release 7.3.2

E66035-01

May 2016

This document provides information about Oracle Communications Network Integrity Release 7.3.2.

This document consists of the following sections:

- Software Compatibility
- New Features
- Documentation Updates
- Known Problems in This Release

See *Oracle Communications Design Studio Release Notes* for the release notes for the Design Studio for Network Integrity feature.

See *Licensing Information User Manual* for license and dependency information for Network Integrity components and cartridges.

Software Compatibility

See *Network Integrity Installation Guide* for more information about software requirements and compatibility.

New Features

This section describes the new features introduced in this release.

Support for Single Sign-On Authentication

Network Integrity now includes support for single sign-on (SSO) authentication. Network Integrity implements the SSO authentication solution using Oracle Access Manager, which enables you to seamlessly access multiple applications without being prompted to authenticate for each application separately. The main advantage of SSO is that you are authenticated only once, which is when you log in to the first application; you are not required to authenticate again when you subsequently access different applications within the same web browser session.

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

See "Setting Up Network Integrity for Single Sign-On Authentication" in *Network Integrity Installation Guide* for more information.

Support for CPU Utilization-enabled Discovery

The Cisco Router and Switch SNMP cartridge and Cisco Router and Switch UIM Integration cartridge have been enhanced to support CPU utilization-enabled discovery. These cartridges now enable you to discover devices based on their CPU utilization by setting a threshold value (in percentage) in the discovery scan.

See *Network Integrity Cisco Router and Switch SNMP Cartridge Guide* and *Network Integrity Cisco Router and Switch UIM Integration Cartridge Guide* for more information.

If the CPU utilization value of a device exceeds the user-specified threshold value, the scan for that device is skipped. The discovery scans are run only for those devices whose CPU utilization value is less than the user-specified threshold value.

To support the discovery of devices based on CPU utilization, a new scan parameter group, **CPU Utilization Parameters**, has been added in the NetworkIntegritySDK cartridge. This scan parameter group adds the **CPU Utilization %** field to the Network Integrity UI Scan Configuration screen. The **CPU Utilization %** field accepts a value between 1 to 99.

See *Network Integrity Developer's Guide* for more information.

New CLI Cartridge Introduced

The Command Line Interface (CLI) cartridge allows you to build deployable cartridges that connect to devices and retrieve information using CLI commands over Telnet or Secure Shell (SSH) protocol.

The CLI cartridge provides the following key features:

- Telnet protocol and SSH communication with CLI devices
- Record and playback of CLI communication

The CLI cartridge is an abstract cartridge, meaning that Design Studio is used to configure and assemble the run time cartridge against devices before deploying it into Network Integrity.

The CLI cartridge ZIP file contains a reference implementation cartridge for discovering Cisco devices running the IOS XR operating system and retrieves information about virtual private LAN services (VPLSs) on the Cisco IOS XR devices.

See *Network Integrity CLI Cartridge Guide* for more information.

Extended Oracle Communications Information Model Support

Network Integrity now enables you to model packet connectivity entities in Design Studio to enhance the integration with Oracle Communications Unified Inventory Management (UIM).

> **Note:** Network Integrity 7.3.2 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*.

To support packet connectivity, Network Integrity adds support to additional Oracle Communications Information Model (OCIM) entities in the following entity categories:

- Connectivity Entities
- Logical Device Entities
- Signal Structure Entities
- Capacity Consumption Pattern Entities

Connectivity Entities

You can now define Connectivity specifications in Design Studio and classify entities based on those specifications in Network Integrity. In addition, when you define a Connectivity specification, you can designate its connectivity type.

Network Integrity now supports three types of Connectivity entities, each of which is designed for use with particular technologies. When you define a Connectivity specification, you specify one of the following connectivity types:

- **Multiplexed:** Multiplexed (or Channelized) connectivities support technologies such as E-Carrier, T-Carrier, J-Carrier, SDH, and SONET, and WDM.
- **Packet:** Packet connectivities support technologies such as Ethernet, DSL, Frame Relay, ATM, and MPLS. See "Logical Device Entities" for additional information.
- **Service:** Service connectivities deliver services to end customers. Service connectivity consumes other types of connectivity and resources, but cannot be consumed itself. Service connectivities are used as part of service arrangements involving packet technology, such as Carrier Ethernet.

Connectivity entities take advantage of pre-defined rate codes and technologies that are provided by Oracle in the ora_uim_basemeasurements and ora_uim_ basetechnologies cartridges.

See the Design Studio Modeling Inventory Help for more information.

Logical Device Entities

Network Integrity now includes Logical Device entities to support networking technologies that are based on packet connectivity, including Ethernet, Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS).

Network Integrity now includes flow interfaces and flow identifiers that are used in packet scenarios. See "Flow Interfaces" and "Flow Identifiers" for more information.

Flow Interfaces

To support packet connectivity, Network Integrity now includes Flow Interface entities.

Flow interfaces partition media interfaces (device interfaces at the top of their hierarchies) into virtual channels based on bit rate. Flow interfaces are similar to the sub-device interfaces used to terminate channelized connectivity, but are used to terminate packet connectivity only. They have configurations that capture their attributes.

When you define a Flow Interface specification, you specify one of four termination types:

- **Access:** Indicates that the purpose of an interface is to terminate connectivity that provides access to a service provider network, such as Ethernet UNI connectivity.
- **Internetwork:** Indicates that the purpose of an interface is to terminate connectivity that interconnects two service provider networks, such as Ethernet E-NNI connectivity.
- **Trunk:** Indicates that the purpose of an interface is to terminate connectivity that connects equipment and devices in the same network, such as Ethernet I-NNI connectivity.
- **Unknown:** Indicates that the purpose of the interface is unknown. Used to support scenarios not covered by the Access, Internetwork, and Trunk termination types.

Flow Identifiers

To support packet connectivity, Network Integrity now includes Flow Identifier entities. Flow identifiers are defined by specifications in Design Studio. Flow identifiers are used to represent the ways that various packet network technologies identify and distinguish network traffic. Flow Identifier specifications support technologies such as Ethernet, Frame Relay, ATM, and MPLS.

See the Design Studio Modeling Inventory Help for more information.

Signal Structure Entities

You can now define the following entity in Design Studio:

- Pipe Signal Termination Point

Pipe Signal Termination Point

You can now define Pipe Signal Termination Point specifications in Design Studio. You can associate Pipe Signal Termination Point specifications to either Connectivity specifications or Pipe specifications to define channelized facilities. You use Pipe Signal Termination Point specifications to define signal structures. A signal structure defines a multiplexing hierarchy where data streams are separated into multiple lower data communication links.

See the Design Studio Modeling Inventory Help for more information.

Capacity Consumption Pattern Entities

You can now define the following entities in Design Studio:

- Inventory Unit Of Measure
- Measurement Type

Inventory Unit Of Measure

Units of measure define the units used to measure a type of capacity. A unit of measure is a quantity or increment by which something is divided, counted, or described. For example, Kbps (kilobits per second) is a unit that measures a bit rate.

Measurement Type

A measurement type classifies related groups of units of measure. For example, a bit rate measurement type classifies units of measure, such as bits per second (bps), kilobits per second (kbps), and so on. Other possible measurement types include weight and amperage.

See the Design Studio Modeling Inventory Help for more information.

Documentation Updates

This section provides information about the Network Integrity documentation set.

Network Integrity CLI Cartridge Guide Introduced

The Network Integrity 7.3.2 documentation set includes a new guide entitled *Network Integrity CLI Cartridge Guide*. This guide explains the functionality and design of the Oracle Communications Network Integrity CLI cartridge.

Known Problems in This Release

Table 1 lists the known problems in this release.

Table 1 Known Problems

Bug Number	Notes
13087174	**Issue** Cartridge deployment fails in a clustered environment when the Cartridge Deployment Tool is configured to use SSL and the keystore location is provided. **Workaround** Do the following: 1. In the WebLogic Server Administration Console, enable the non-SSL port for the managed server (for example, networkintegrity01) on which the CMWS application is deployed. 2. Restart all the managed servers in the cluster. 3. Redeploy the CMWS application on networkintegrity01. 4. Deploy the cartridges using the Cartridge Deployment Tool. 5. After you have deployed the cartridges, disable the non-SSL port for networkintegrity01 in the WebLogic Server Administration Console.
11676449	**Issue** When a scan action is configured to use the file transfer processor when the Source File Management is set to Rename or Delete, the scan status of a running scan may change from Running to Completed, even though other processes are still running. This issue occurs when Network Integrity incorrectly changes the scan status to Completed after the processor has finished its processing and modeling, instead of changing the status to Completed after the intended file has been renamed and deleted. You may observe this issue in situations where the remote file operation is required to delete or rename a large number of files or when the network connection is slow. Failures related to the remote file rename or delete operations are not reported by the Network Integrity UI. **Workaround** None.

Table 1 (Cont.) Known Problems

Bug Number	Notes
11071255	**Issue** Manage Scans page is not displayed properly when you log in to Network Integrity again after the session times out in Internet Explorer. **Workaround** Refresh your browser if you are using Internet Explorer, or use Firefox.
10065856	**Issue** If the **Correct in UIM** operation fails due to a session time out, no error message is displayed. **Workaround** None.
19940521	**Issue** If you create new roles or policies using Oracle Enterprise Manager, the changes are not propagated to the managed servers unless the managed servers are restarted. **Workaround** After you create the roles and policies, you must restart the managed servers. Doing so enables the managed servers to receive updates related to the local LDAP server from the Administration server, and subsequently the new policies and roles are propagated to the managed servers.

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.

Document Revision History

The following table lists the revision history for this guide:

Version	Date	Description
E66035-01	May 2016	Initial release.

Network Integrity Installation Guide, Release 7.3.2
E66035-01

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.