Oracle® Communications Interactive Session Recorder

Release Notes

Release 5.1

Formerly Net-Net Interactive Session Recorder

December 2015

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.

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.

This software or hardware and documentation may provide access to or information on 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. 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.

Contents

About this Release Note

Overview

The *Interactive Session Recorder Release Notes* provides the following information:

- About the Oracle Communications Interactive Session Recorder (NN-ISR)
- NN-ISR Release Notes
- Upgrading the NN-ISR

Related Documentation

The following table lists related documents.

Document Name	Document Description
Interactive Session Recorder Installation Guide	Provides an overview of the ISR, hardware/software requirements and recommendations, storage considerations, pre-installation information, CIS and RSS installation procedures, post-install verification and configuration procedures, setting up and making a test call, and additional advanced topics about the ISR.
Interactive Session Recorder User's Guide	Contains information about using the ISR Dashboard from the User's perspective. Provides information about viewing, playing, deleting recordings, running reports, and managing user profiles (Super User, Account Administrator, and Tenant Administrator only).
Interactive Session Recorder Administrator Guide	Contains information about using theISR Dashboard for the Administrator level user (Super User, Account Administrator, and Tenant Administrator). Provides information about creating and managing accounts, routes, and users. Also provides information about configuring the ISR, running reports, and viewing active calls.
Interactive Session Recorder API Reference Guide	Contains information about Methods for Recording, VoiceXML Commands, representational state transfer (REST) application programming interface (API), Recording File Types/Formats Supported, Return Codes, sendIPCRCommand.jsp Subdialog, Advanced Options, Troubleshooting.

Document Name	Document Description
Interactive Session Recorder Monitoring Guide	Contains information about installing and configuring the ISR Monitor. It also includes the Monitor database schema as well as the Monitor MIB.
Interactive Session Recorder Remote Archival Web Services Reference Guide	Contains information about the Remote Archival Web Service, its Control methods, WSDL definitions, DataType Definitions, sample responses to requests, and importing the Remote Archival Web Service's certificate into the client keystore.

Revision History

This section contains the revision history for this document.

Date	Revision Number	Description
July 31, 2013	Revision 1.00	Initial release of the NN-ISR 5.1 software.
September 10, 2013	Revision 1.01	Updates the Tomcat port number.
October 31, 2013	Revision 1.10	• Updates various inaccurate terminology. • Updates various typographical errors. • Updates instructions for importing the new Index VM.
March 6, 2014	Revision 1.20	• Adds Configuring Automatic Start of the Upgraded VMs section. • Corrects typographical error.
December 24, 2015	Revision 1.21	• Adds the Interactive Session Recorder Remote Archival Web Services Reference Guide to the list of Related Documentation.

1 NN-ISR Release Notes

Introduction

These Release Notes provide the following information:

- About the NN-ISR
- Supported Hardware/Software
- NN-ISR Release Process
- Features
- Issues Fixed
- Known Issues

About the NN-ISR

Oracle introduces the NN-ISR to the Interactive Voice Response (IVR) and Telecom industries. Awarded 2008 Communications Solutions Product of the Year Award, the NN-ISR allows any telephony or IVR environment to handle full-duplex call recording (both pre- and post-transfer).

The NN-ISR reliably records any phone call in carrier, enterprise, or contact center. Supporting enterprise & multi-tenant architectures, the NN-ISR provides ad-hoc (partial call) recording allowing any call to be recorded at any point and for any duration. Call recording can be initiated automatically by SIP URI or conditionally by any authorized VoiceXML or web application. In addition, call data such as time of call, callerID, account number, etc. are stored in a recording database for clients to search and review. Once recording starts, recordings can continue after being transferred to an agent or employee thereby providing continuity for recordings & call data across IVR, office, and call center telephony deployments.

Using the NN-ISR, VoiceXML and representational state transfer (REST) application programming interface (API) developers now have the ability to record every call, a percentage of calls, specific VoiceXML dialogs as well as transfers to agent conversations. With simple VoiceXML and REST API code, the VoiceXML application controls recording for any call, at any point and for a specific period of time. In addition, every recording may be indexed by key VoiceXML values or identifiers (account#, unique call identifier, SIP URI, time of call, etc.).

The NN-ISR can scale from one call to thousands of concurrent calls and is a simple add-on to any SIP telephony network. An affordable software-based solution, the IP Call Recorder runs on standard Intel-based servers in VoIP and standard telephony environments.

All current Net-Net SBCs support the use of the NN-ISR in a network. Contact Technical Assistance for information about previous NN-ISR release support with SBCs.

Supported Hardware/Software

Hardware

This section describes the hardware Oracle has certified for load/capacity. Other hardware platforms may be compatible, but have not been certified for load.

CIS & RSS Certified Hardware

The third-party servers in this section have been certified for use with Oracle's NN-ISR software which is composed of two modular elements:

- **Control and Index Server (CIS)** - The CIS maintains metadata and indices; and provides browser-based administration.
- **Recording and Storage Server (RSS)** - The RSS, under the control of the CIS, records sessions and manages the storage and archival processes. It selects, starts, and stops recordings using Web services APIs.

Note: The specified processor choices and disk sizes of these third-party server recommendations represent the minimal options. Redundant environments require additional servers.

CIS Server

The following third-party servers are certified for use with the NN-ISR and CIS software.

HP DL360 Gen8 Server

Features of this server include:

- CPU0: Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz stepping 07
- CPU1: Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz stepping 07
- HP Smart Array P420i/1GB with FBWC (RAID 0/1/1+0/5/5+0
- Two redundant (652589-B21) HP 300 GB 6G SAS 15K rpm SFF (2.5-inch) SC Enterprise 3yr Warranty Hard Drive in RAID 1 Configuration
- Four Redundant (652611-B21) HP 900GB 6G SAS 10K rpm SFF (2.5-inch) SC Enterprise 3yr Warranty Hard Drive in RAID 1+0 Configuration
- 64GB RAM

HP DL360 G7 Server

Features of this server include:

- Suitable for NN-ISR applications up to 5000 sessions
- Form factor: 8 SFF (Small Form Factor) drive bays total
- Dual Six-Core Intel Xeon® processors, 24 GB RAM
- Two AC power supplies

Configuration Recommendation

The recommended configuration for the HP DL360 G7 Server is:

Hardware	Qty
HP ProLiant® DL360 G7 Server	1
HP DL360 G7 Intel® Xeon® X5660 (2.80GHz/6-core/12MB/95W)	2
HP 4GB memory (1 x 4GB @ 1333MHz)	6
HP 72GB 6G SAS 15K rpm SFF (2.5-inch) Dual Port Enterprise (RAID 1)	2
HP 300 GB 6G SAS 15K rpm SFF (2.5-inch) Dual Port Enterprise (RAID 6 or 1+0)	4
HP Smart Array P410i/1G FBWC Controller – Low profile PCIe	1
HP NC375T PCI Express Quad Port Gigabit Server Adapter	1
HP 750W CS HE Power Supplies	2
HP 1.83m 10A C13-UL US Power Cords (North American variant; acquire applicable power cord for your region)	2

RSS Server

The following third-party servers are certified for use with the NN-ISR and the RSS software.

Note: The RSS certified drive specs call for a second drive to be used for recordings. For a procedure to mount a second drive, see the *Interactive Session Recorder Installation Guide*.

HP DL360 Gen8 Server

Features of this server include:

- CPU0: Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz stepping 07
- CPU1: Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz stepping 07
- HP Smart Array P420i/1GB with FBWC (RAID 0/1/1+0/5/5+0
- Two redundant (652589-B21) HP 300 GB 6G SAS 15K rpm SFF (2.5-inch) SC Enterprise 3yr Warranty Hard Drive in RAID 1 Configuration
- Four Redundant (652611-B21) HP 900GB 6G SAS 10K rpm SFF (2.5-inch) SC Enterprise 3yr Warranty Hard Drive in RAID 1+0 Configuration
- 64GB RAM

HP DL360 G7 Server

Features of this server include:

- Suitable for NN-ISR applications up to 500 sessions
- Form factor: 8 SFF (Small Form Factor) drive bays total
- Dual Quad-Core Intel® Xeon® processors, 8 GB RAM

Configuration Recommendation

The recommended configuration for the HP DL360 G7 Server is:

Hardware	Qty
HP ProLiant® DL360 G7 Server	1
Quad-Core Intel® Xeon® Processor E5620 (2.40GHz/4-core/12MB/80W)	2
HP 4GB memory (2 slots x 4GB @ DDR3-1333MHz)	2
HP 72GB 6G SAS 15K rpm SFF (2.5-inch) Dual Port Enterprise (RAID 1)	2
HP 300 GB 6G SAS 15K rpm SFF (2.5-inch) Dual Port Enterprise (RAID 1)	2
HP Smart Array P410i/1G FBWC Controller – Low profile PCIe	1
HP NC375T PCI Express Quad Port Gigabit Server Adapter	1
HP 750W Common Slot Gold Hot Plug Power Supply Kit (AC)	2
HP 1.83m 10A C13-UL US Power Cords (North American variant; acquire applicable power cord for your region)	2

Software

This section provides a list of the software that installs during the NN-ISR installation process.

NN-ISR Software

The following components are installed during the NN-ISR installation process:

- **Control and Index Server (CIS)** - Installs the following components:
  - VMware Enterprise vSphere™ Hypervisor (ESXi)
  - VMware vSphere™ Client
  - 2 to 4 Virtual Machines running Oracle Linux 6.4
    - NN-ISR Dashboard, Version 5.1.0 M0P0, Build 20130719
    - NN-ISR Index, Version 5.1.0 M0P0 Build, 20130719
    - NN-ISR Remote Archival Webservice, Version 5.1.0 M0P0 Build 20130729
- **Record and Store Server (RSS)**
  - NN-ISR RSS, Version 5.1.0M0P0, Build 20130719
  - NN-ISR API, Version 5.1.0M0P0, Build 20130719
  - Archiver Service

For more information about installing the CIS and RSS software, see *Interactive Session Recorder Installation Guide*.

NN-ISR Dashboard Requirements

The following list recommends third-party applications you can use with the NN-ISR Dashboard.

The recommended third-party applications are:

- Web browser recommendations for NN-ISR Dashboard:
  - Microsoft® Internet Explorer 9 (IE9) with full regression specifically on IE Version 9 and with Quicktime® 7.7.4 Player Plug-in (http://www.apple.com/quicktime/) or Windows Media Player 10/11

  - Mozilla Firefox® 17 with Quicktime® 7.7.4 Player Plug-in or Windows Media Player 10/11
  - Google Chrome™ 28 with Quicktime® 7.7.4 Player Plug-in
  - Other browsers (please contact Oracle Customer Service before using other browsers)
- SIP softphone recommendations for testing:
  - X-lite by CounterPath Corporation - (http://www.counterpath.net/x-lite.html)
  - PhonerLite by Heiko Sommerfeldt - (http://www.phonerlite.de/index_en.htm)

NN-ISR Release Process

The NN-ISR Release process may consist of maintenance (M), and patch (P) information. The numbering scheme for releases is outlined in the table below.

Upgrading from release to release must be done in sequential order (for example, from Release 5.0 to 5.0M1). For any subsequent releases (for example, 5.0M1 to 5.0M2, 5.0M1 to 5.0M2, etc.), you MUST continue to upgrade in sequential order (for example, from 5.0M1 to 5.0M2, 5.0M1 to 5.0M2, 5.0M2 to 5.0M3, etc.). For more information and procedures for upgrading your NN-ISR, see Chapter 2, Upgrading the NN-ISR.

The following table identifies the NN-ISR release process.

Releases	Description
M# (Maintenance Releases)	Maintenance software releases numbered sequentially (for example, M1, M2, M3, etc.). Information in these releases contain maintenance fixes in the NN-ISR. All maintenance release information is documented in the NN-ISR Release Notes for that M# release. All maintenance information is rolled into the next M# release of the NN-ISR documentation set.
P# (Patch Releases)	Patch software releases numbered sequentially (for example, P1, P2, P3, etc.). Information in these releases contain issues fixed in the NN-ISR. All patch release information is documented in the NN-ISR Release Notes for that P# release. All patch information is rolled into the next release of the NN-ISR documentation set.

Net-Net ISR Third-Party Licensing

For commercial and open-source licensing information regarding the RSS components, execute the following command on any RSS host:

- From the OS-E command line, execute the command **show legal**
- From the RSS shell, execute the command **more /cxc_common/ISR/LEGAL.TXT**

Type **q** to exit the legal text display.

For commercial and open-source licensing information regarding the CIS components, execute the following command on any CIS host:

- more /cxc_common/ISR/LEGALTXT

Type **q** to exit the legal text display.

Release 5.1

This section describes the new adaptations added to the NN-ISR in release 5.1, including new features, issues fixed, and known issues.

Features

The following are new features of the NN-ISR 5.1 release:

- Remote Archival Webservice Enhancements
- NN-ISR Monitor Dashboard Enhancements
- Salt Encryption
- SNMP Enhancements
- Security Enhancements
- JBoss Version Upgrade

Remote Archival Webservice Enhancements

Remote Archival allows customers of hosted call recording providers to pull their recordings to a premise location. Utilizing a secure connection between the premise and service provider applications, a Remote Archival client connects to the Remote Archival Webservice and retrieves all recordings for a single account configured on the host platform.

The Remote Archival process includes:

1. Moving recording files to a remote file system. The files may be optionally deleted from the source RSS/NAS/SAN after the client confirms a successful delivery.
2. Moving recording metadata for the configured account, including the standard recording data from the recordings table, SIPREC metadata, and ISR custom fields, to a remote store. If the file has been configured for deletion, the data is also removed from the source Index.

To enable the Remote Archival Webservice, you must configure at least one Remote Archival user and at least one account. This user’s username and password are required in the client requests.

For more information on the Remote Archival Webservice and how to configure it, see Chapter 11 in the *Interactive Session Recorder Administration Guide*.

NN-ISR Monitor Dashboard Enhancements

The NN-ISR Monitor has been enhanced to include an updated Dashboard, affecting the Monitor configuration greatly.

Logging In/Out of the NN-ISR Monitor Dashboard

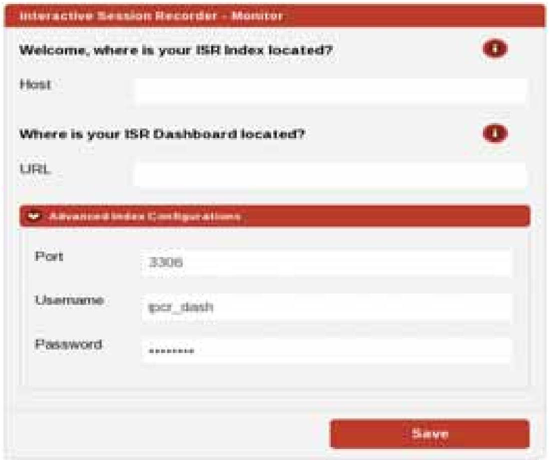
The NN-ISR Monitor Dashboard allows you to access test results, system, and alert configurations, and to import configurations to generate tests for ISR deployments.

> **Note:** You must have Super User privileges to access the NN-ISR Monitor.

The first time you log into the NN-ISR Monitor Dashboard, you must enter and save your Index connection credentials and Dashboard location. These credentials are used to authenticate user login and import data to generate test cases. Once the credentials you entered have been validated, the login screen appears.

You must only enter this information the first time you login to the NN-ISR Monitor. All subsequent login attempts direct you directly to the login page.

The NN-ISR Monitor Dashboard credential page appears.



Interactive Session Recorder - Monitor

Welcome, where is your ISR Index located?

Host

Where is your ISR Dashboard located?

URL

Advanced Index Configurations

Port 3306

Username ipcr_dash

Password ••••••••

Save

1. **Host**—Enter the hostname or IP address of the Index that the NN-ISR Monitor connects to.
2. **Port**—Enter the port number of the Index that the NN-ISR Monitor connects to. The default value is **3306**.
3. **Username**—Enter the Index database username. The default value is **ipcr_dash**.
4. **Password**—Enter the Index database password. The default value is **n3wf0und**.
5. **URL**—Enter the URL of the NN-ISR Dashboard you are monitoring.
6. Click **Save**.

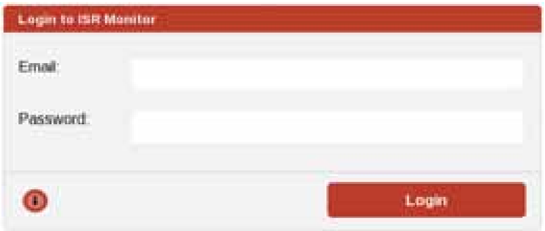
   Note: These Index and Dashboard connection credentials can be updated if need be. For more information, see Setting ISR Index and Dashboard Configurations.

To login to the NN-ISR Monitor Dashboard:

1. Open your Internet Web browser.
2. Enter the following URL in the URL field:

   `http://<IP address>/`

   The Login page appears.



Login to ISR Monitor

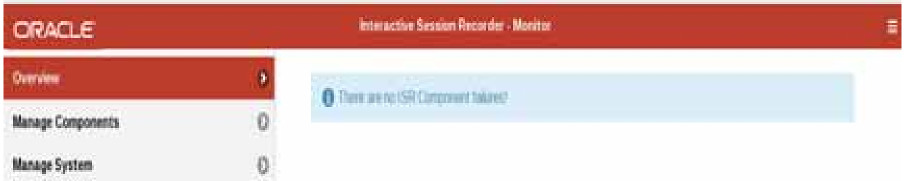
Email:

Password:

Login

3. **Email**—Enter your email address.
4. **Password**—Enter your NN-ISR password.
5. Click **Login**.

The Net-Net ISR Monitor Overview page appears. If there are any ISR component failures, they appear on this page when you log in.



There are no ISR Component failures!

Managing the System

The Manage System tab is where you configure system-wide test and configuration settings. Settings configured here apply to all components tests unless there are test-specific settings configured under the Manage Components tab.

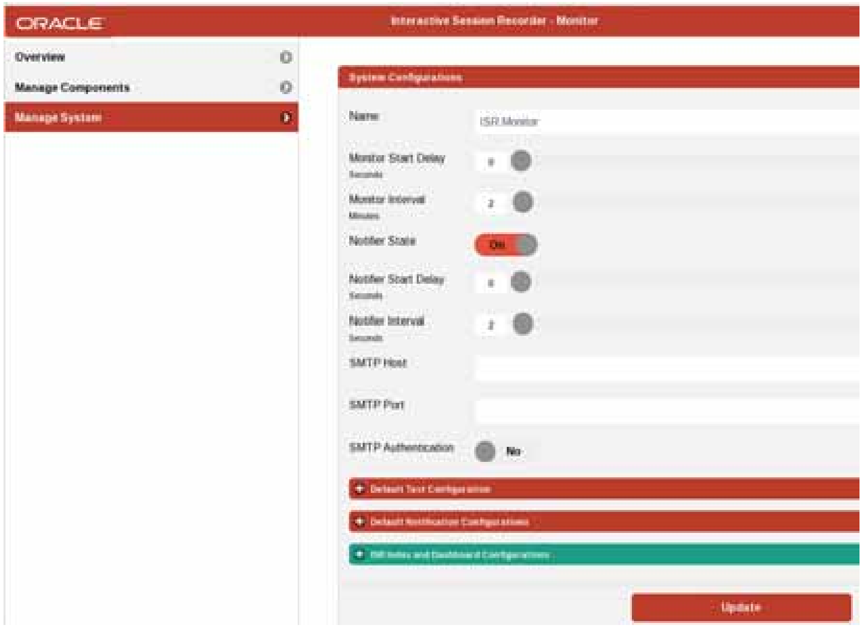
The Manage System tab is divided into four sub-sections.

- System Configurations
- Default Test Configuration
- Default Notification Configurations
- ISR Index and Dashboard Configurations

Setting System Configurations

To configure system configurations settings:

1. Click the **Manage System** tab.


ORACLE
Interactive Session Recorder - Monitor
Overview
Manage Components
Manage System
System Configurations
Default Test Configuration
Default Notification Configurations
ISR Index and Dashboard Configurations
Update

Name: ISR Monitor
Monitor Start Delay (Seconds): 0
Monitor Interval (Minutes): 2
Notifier State: On
Notifier Start Delay (Seconds): 0
Notifier Interval (Seconds): 2
SMTP Host:
SMTP Port:
SMTP Authentication: No

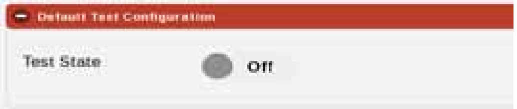
2. **Name**—Enter the name of this NN-ISR Monitor. The default value is **ISR Monitor**.
3. **Monitor Start Delay**—Specify the number of seconds to delay before starting testing at the start of the NN-ISR Monitor service. The minimum value is 0 and the maximum value is 300. The default value is **0**.
4. **Monitor Interval**—Specify the interval, in minutes, that the NN-ISR Monitor performs each test. The minimum value is 0 and the maximum value is 300. The default value is **2** minutes.

5. **Notifier State**—Specify whether the NN-ISR Monitor is enabled to send out notifications. Valid values are **On** and **Off**. The default value is **On**.
6. **Notifier Start Delay**—Specify the number of seconds to wait before sending notifications at the start of the NN-ISR Monitor service. The minimum value is 0 and the maximum value is 300. The default value is **0**.
7. **Notifier Interval**—Specify the interval, in seconds, at which the NN-ISR Monitor sends notifications. The minimum value is 0 and the maximum value is 300. The default value is **2** seconds.
8. **SMTP Host**—Specify the hostname or IP address of the email server. There is no default value.
9. **SMTP Port**—Specify the port number of the email server. There is no default value.
10. **SMTP Authentication**—Enables or disables SMTP authentication. Valid values are **Yes** and **No**. The default value is **No**.
11. **SMTP Username**—When **SMTP Authentication** is set to **Yes**, enter the SMTP username for authentication. There is no default value.
12. **SMTP Password**—When **SMTP Authentication** is set to **Yes**, enter the SMTP password for authentication. There is no default value.
13. Click **Update**.

Setting the Default Test Configuration

To configure the default test configuration setting:

1. Click the **Manage System** tab.
2. Click **Default Test Configuration**.



Test State ● Off

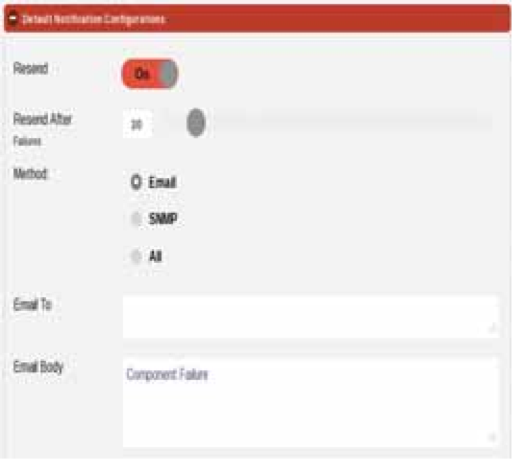
3. **Test State**—Specify whether or not NN-ISR Monitor tests are enabled. Valid values are **On** and **Off**. The default value is **Off**.
4. Click **Update**.

Setting Default Notification Configurations

To configure the default notification configuration settings:

1. Click the **Manage System** tab.

2. Click **Default Notification Configurations**.



Default Notification Configurations

Resend: On

Resend After Failures: 30

Method: ● Email ○ SNMP ○ All

Email To:

Email Body: Component Failure

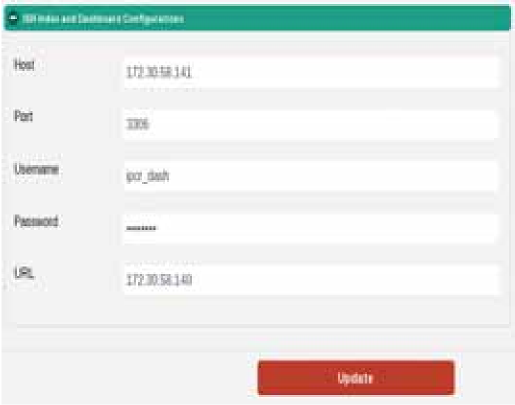
3. **Resend**—Specify whether a notification should be sent for each failure of a test or just after the first in a consecutive string of failures. Valid values are **On** and **Off**. The default value is **On**, meaning notifications will continue to be sent.
4. **Resend After**—Specify the number of consecutive failed tests for the NN-ISR Monitor to wait before it resends a notification. The default value is **30** failures.
5. **Method**—Specify the method to use for notifications when there is a test error. Valid values are **Email**, **SNMP**, or **All**. The default value is **Email**.
6. **Email To**—When the notification method is **Email** or **All**, enter the email address(es) to send the emails to. There is no default setting.
7. **Email Body**—When the notification method is **Email** or **All**, specify the text you want to be included in the email sent when there is a test error. There is no default setting.
8. Click **Update**.

Setting ISR Index and Dashboard Configurations

To configure the ISR Index and Dashboard configuration settings:

1. Click the **Manage System** tab.
2. Click **ISR Index and Dashboard Configurations**.

   Note: These are the same index and database credential you enter and save the first time you log into the NN-ISR Monitor.



ISR Index and Dashboard Configurations

Host: 172.30.58.141

Port: 3306

Username: ipcr_dash

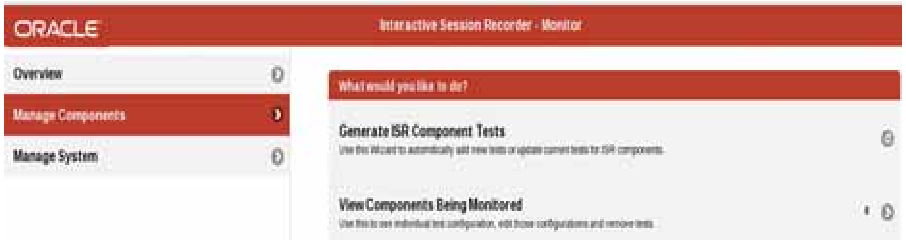
Password: ********

URL: 172.30.58.140

3. **Host**—Enter the hostname or IP address of the index that the NN-ISR Monitor connects to.
4. **Port**—Enter the port number of the index that the NN-ISR Monitor connects to. The default value is **3306**.
5. **Username**—Enter the NN-ISR Monitor username. The default value is **ipcr_dash**.
6. **Password**—Enter the NN-ISR Monitor password. The default value is **n3wf0und**.
7. **URL**—Enter the URL of the NN-ISR you are monitoring.
8. Click **Update**.

Managing Components

The Management Components tab is where you can configure test-specific settings. You can generate new tests, refresh existing tests, view, edit, and remove components being monitored.


ORACLE
Interactive Session Recorder - Monitor
Overview
Manage Components
Manage System
What would you like to do?
Generate ISR Component Tests
View Components Being Monitored

Use this Wizard to automatically add new tests or update current tests for ISR components.

Use this to see individual test configuration, edit those configurations and remove tests.

Generating Component Tests

To generate or refresh NN-ISR component tests:

1. Click the **Manage Components** tab.
2. Click **Generate ISR Component Tests.**

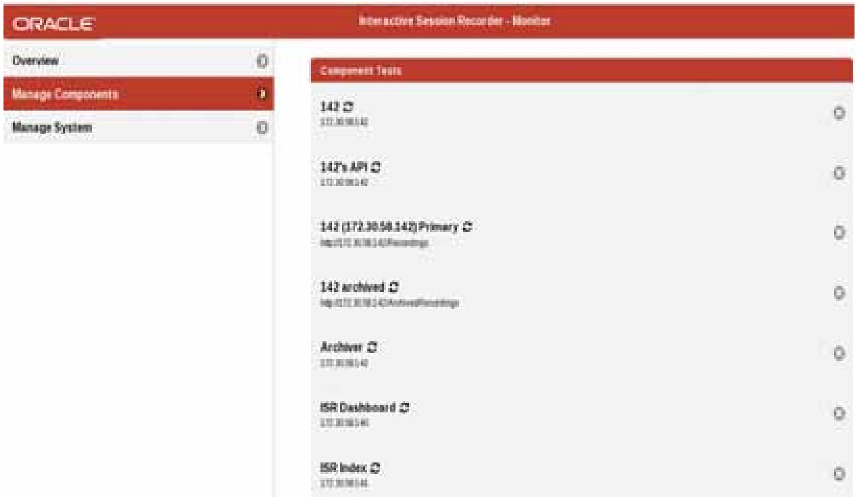
The NN-ISR monitor automatically generates tests with either the system default settings or with test-specific settings you have configured.

Viewing and Editing Monitored Components

To view the components currently being monitored:

1. Click the **Manage Components** tab.
2. Click **View Components Being Monitored**.

All component tests configured on the NN-ISR Monitor appear.\



3. Click a specific test to view its configuration details.

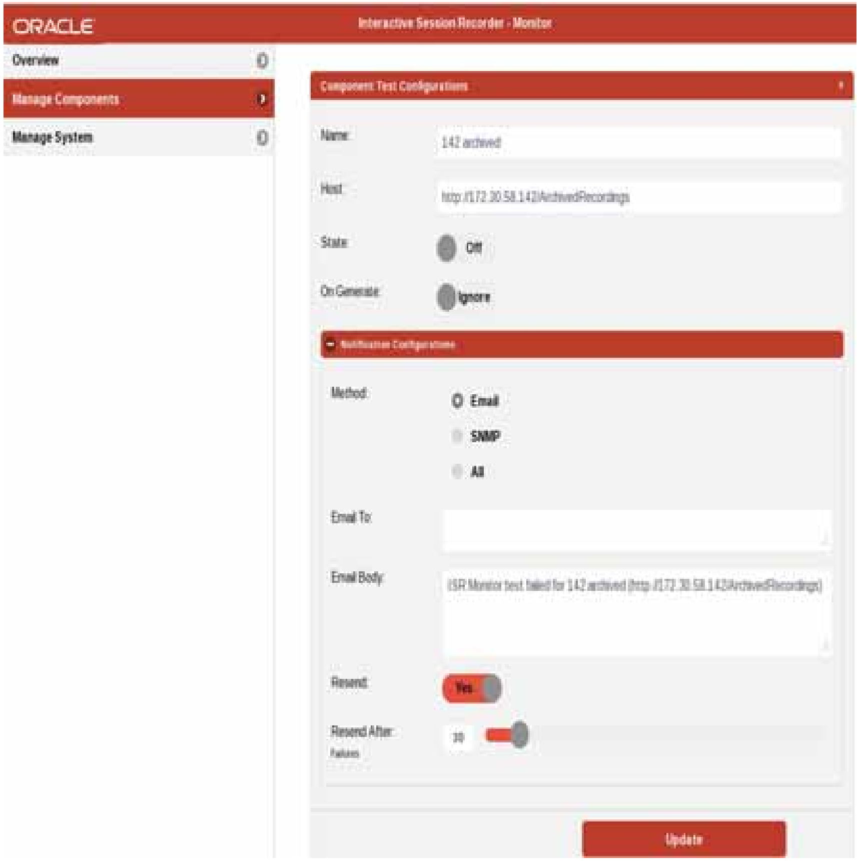
   Note: Click **Notification Configurations** on the Component Test Configurations page to view notification settings for that test.

To edit a component test:

1. Click the **Manage Components** tab.
2. Click **View Components Being Monitored**.

   All component tests configured on the NN-ISR Monitor appear.
3. Click the test you want to edit.

Note: Click **Notification Configurations** to edit notification settings.


ORACLE
Interactive Session Recorder - Monitor
Overview
Manage Components
Manage System
Component Test Configurations
Notification Configurations
Update

Name: 142 archived

Host: http://172.30.58.142/ArchivedRecordings

State: Off

On Generate: Ignore

Method: ○ Email ○ SNMP ○ All

Email To:

Email Body: ISR Monitor test failed for 142 archived (http://172.30.58.142/ArchivedRecordings)

Resend: Yes

Resend After Failures: 30

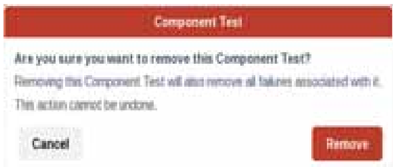
4. **Name**—Enter the name of the test.
5. **Host**—Enter the name or IP address of the host being tested. There is no default setting.
6. **State**—Specify whether this test is active. Valid values are **On** and **Off**. The default value is **Off**.
7. **On Generate**—When set to **Update** and Generate Tests is selected, the NN-ISR configuration overwrites changes to the hostname or IP address. Valid values are **Update** and **Ignore**. The default value is **Ignore**.
8. **Method**—Specify the method to use for notifications when there is a test error. Valid values are **Email**, **SNMP**, or **All**. The default value is **Email**.
9. **Email To**—When the notification method is **Email** or **All**, enter the email address(es) to send the emails to. There is no default setting.
10. **Email Body**—When the notification method is **Email** or **All**, specify the text you want to be included in the email sent when there is a test error. There is no default setting.
11. **Resend**—Specify whether a notification should be sent for each failure of a test or just after the first in a consecutive string of failures. Valid values are **Yes** and **No**. The default value is **Yes**, meaning notifications will continue to be sent.
12. **Resend After**—Specify the number of consecutive failed tests for the NN-ISR monitor to wait before it resends a notification. The minimum value is 0 and the maximum value is 300. The default value is **30**.
13. Click **Update**.

To delete a component test:

1. Click the **Manage Components** tab.
2. Click **View Components Being Monitored**.

   All component tests configured on the NN-ISR Monitor appear.
3. Click the **X** on the test you want to delete.

   A pop-up appears verifying you want to delete the test.

   Are you sure you want to remove this Component Test?

   Removing this Component Test will also remove all failures associated with it.

   This action cannot be undone.
4. Click **Remove**. The test is deleted.

Salt Encryption

The NN-ISR now includes a Salt in its encrypted passwords for enhanced security.

SNMP Enhancements

For improved system monitoring, the CIS hosts are now configured to respond to SNMP requests with a default configuration concentrated on handling queries for disk, memory, and CPU resources.

The NN-ISR supports several versions of SNMP based on component.

The RSS supports:

- SNMP v1
- SNMP v2c

The CIS supports:

- SNMP v3

CIS SNMP Configuration

The CIS is automatically enabled for SNMP and supports SNMPv3 only. The CIS components, Index, Dashboard, Remote Archiver Webservice, and Monitor Service guest operating systems include the standard net-snmp, net-snmp-libs, and net-snmp-utils packages to provide SNMP agent functionality. The CIS hosts expect secure requests that include a username, password, and user security level (“authNoPriv” by default), following version 3 of the SNMP protocol.

The default configuration is located in the following file:

/etc/snmp/snmpd.conf

It has the following contents on deployment:

```
######################################################################
##########
# snmpd.conf:
######################################################################
##########

##### SNMP v3 User #####
createUser isrsnmp MD5 n3wf0und
rouser isrsnmp auth .1.3.6.1.4.1.2021
```

```
disk / 500000 (or)
load 20
```

The default SNMP agent configuration for each CIS host consists of a user and password specific to the SNMPv3 protocol. The default username is “isrsnmp” and the default password is “n3wf0und”. These two parameters must be included in any Get requests to the CIS agent.

RSS SNMP Configuration

You must configure the RSS to enable the SNMP agent service on a specific network interface. The RSS supports SNMP v1 and SNMP v2c only, so SNMP Get requests must follow a slightly different version of the protocol than the CIS.

You must use the NN-ISR CLI to configure SNMP on the RSS.

Use the following CLI command sequence to enable SNMP on the RSS.

```
config box> config interface eth0
config interface eth0> config ip a
config ip local> config snmp
config snmp> set admin enabled
config snmp> set port 161
config snmp> set version 2c
config snmp> set community private
config snmp>exit
Do you want to commit your changes before you exit (y or n)? y
Do you want to update the startup configuration (y or n)? y
```

Note: If you set the **community** name to anything other than **isr**, make note of it because you must use this value for management configuration of the Get requests.

SNMP Agent MIBs

The latest MIB for the CIS OID table, UCD-SNMP-MIB, can be found at the following URL:

http://www.net-snmp.org/docs/mibs/ucdavis.html

It is also available at the following path on each CIS host:

/usr/share/snmp/mibs/UCD-SNMP-MIB.txt

All MIBs included as part of the net-snmp are found at the following URL:

http://www.net-snmp.org/docs/mibs

The MIB or the RSS OID table, cxc.mib, may be found at the following path on each RSS host:

/cxc_rel/app_slot_1/web/cxc.mib

To view the MIB in its entirety, see Appendix C in the *Interactive Session Recorder Monitor Guide*.

For more information on the NN-ISR’s SNMP support, see Chapter 4, Configuring NN-ISR SNMP Agents in the *Interactive Session Recorder Monitor Guide*.

Security Enhancements

You can now configure the Remote Archival Webservice to handle HTTP requests over SSL.

To enable SSL on the Remote Archival Webservice

1. Create a keystore on server. To do this, on the rWebservice host, generate the keystore by executing the following command (and follow the instructions).

   ```
   /opt/jdk1.6.0_24/bin/keytool-genkey-alias<alias_of_choice>-keyalg RSA
   -keystore/cxc_common/ISR/RemoteArchival/server.keystore
   ```

2. Import the certificate into the client’s trustore. To do this, on the Remote Archival Webservice host export the certificate by executing the following command (and follow the instructions).

   ```
   /opt/jdk1.6.0_24/bin/keytool-export -
   keystore/cxc_common/ISR/RemoteArchival/server.keystore-
   alias<alias_of_choice>-file.raws.crt
   ```

   Transfer the newly-created file, raws.crt, from the rWebservice host to the Remote Archival Client host.

   If the Remote Archival Client is a Java-based application, execute the following command (and follow the instructions).

   ```
   keytool-import-alias<alias_of_choice>-file faws.crt-
   keystore<JAVA_HOME>\jre\lib\security\cacerts
   ```

   Note: The password for the keystore is required and, by default, is “changeit”. To change the password, execute the following command:

   ```
   keytool-storepasswd-new<new_storepass>-
   keystore<JAVA_HOME>\jre\lib\security\cacerts
   ```

3. Edit and verify the RA Client’s run.sh or run.bat files so that the -k parameter matches the keystore path.

   Note: Some troubleshooting tips on the keystore:

   – Exception:org.apache.axis2.AxisFault:java.lang.RuntimeException:Unexpected error: java.security.InvalidAlgorithmParameterException: the trustAnchors parameter cannot be left empty.

     – Your client keystore path is not valid.

   – org.apache.axis2.AxisFault:sun.security.validator.ValidatorException:PKIX path building failed:sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certificate path to requested target.

     – Your keystore path is valid, but the keystore has not been updated with the RA WS exported certificate.

4. Configure the Remote Archival Webservice for SSL-only requests. To do this edit /opt/jboss/standalone/configuration/standalone.xml.

   Within the following tag:

   ```
   <subsystem xmlns=”urn:jboss:domain:web:1.1”
   ```

   add:

   ```
   <connector name=”https” protocol=”HTTP/1.1”socket-
   binding=”https”scheme=”https”secure=”true”
   <ssl-name=”ssl”password=”<key_password>”key-
   alias=”<alias>”certificate-key-
   file=”/cxc_common/ISR/RemoteArchival/server.keystore”/>
   </connector>
   ```

   Note:<key_password> refers to the password provided during the instructions to generate, export, and import the key.

   For JBoss to stop listening on port 8080, remove the following lines in standalone xml:

```
<connector name=”http”protocol=”HTTP/1.1”scheme=”scheme=”http”socket-binding=”http”/>
<socket-binding=”http”port=”8080”/>
```

Modify the Linux firewall to allow port 8443 instead of 8080 by editing:

```
/etc/sysconfig/iptables
```

Change the following line:

```
-A INPUT -m state --state NEW -m tcp - tcp --dport 8080 -j ACCEPT
```

To:

```
-a INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
```

Restart the iptables service with the following command:

```
service iptables restart
```

Restart Jboss with the following command:

```
service jboss restart
```

5. To confirm the configuration point the Remote Archival Webservice JBoss root URL to:

```
https://<RA Webservice IP>:8443/
```

JBoss Version Upgrade

The JBoss application server has been upgraded from 4.0.2 to 7.1.1. This upgrade impacts the RSS, Monitor, and rWebservice hosts, more specifically the API (deployed on the RSS), the REST API, the Remote Archival Webservice, and the Monitor service applications.

JBoss 7.1.1 cannot be configured to serve static content from arbitrary directories on the server. The NN-ISR used this feature in JBoss 4.0.2 to serve recorded files, but each RSS now serves recording files from an existing Tomcat 7.0.34 instance.

This leads to an important change with some important ramifications. In previous versions, Dashboard, API, and Remote Archival Webservice hosts, by default, accessed recordings with HTTP fetches over port 9000. These hosts now access recordings via port 80. Firewall settings may have to change if the ISR-host-to-ISR-host communications have been locked down. Also, since the default RSS recording Location setting is set im prior versions as port 9000, the upgrade process includes a SQL script that updates existing locations with port 9000 to port 80.

Issues Fixed

This section describes the issues fixed in each component of the NN-ISR, Version 5.1.

NN-ISR Dashboard

The following Dashboard component fixed issues in NN-ISR, Version 5.1.

Release	Description
5.1	• The Dashboard no longer allows white space in the Session Agent field.
5.1	• An Administrator is now able to add users with equal privileges.
5.1	• When adding a new location, the “Source Directory” field has been renamed to “Recordings Directory” to eliminate confusion.
5.1	• In the reset the password page, the Dashboard brings you to the correct field to confirm the password.
5.1	• Configuration scripts which are automatically included in every distributed ISR component have replaced manually editing configuration files.

NN-ISR Index

The following Index component issues were fixed in NN-ISR, Version 5.1.

Release	Description
5.1	• The NN-ISR Route warning message now specifies what data is being removed from the Index.
5.1	• The MySQL database no longer contains two default users with blank user names in the NN-ISR Index installations.
5.1	• Configuration scripts which are automatically included in every distributed ISR component have replaced manually editing configuration files.

NN-ISR RSS

The following RSS component issues were fixed in NN-ISR, Version 5.1.

Release	Description
5.1	• The RSS now includes a check to prevent a second instance of the RSS service, resulting in the loss of session historical data in the Index.
5.1	• The RSS and API are now in agreement on what value should be contained within all parameters.
5.1	• The RSS now includes the filename it is using for ad hoc recording in its response to the API.
5.1	• Configuration scripts which are automatically included in every distributed ISR component have replaced manually editing configuration files.

NN-ISR RSS Installation

The following RSS Installation component issues were fixed in NN-ISR, Version 5.1.

Release	Description
5.1	• The USB installer now supports 3GB-16GB USB keys.
5.1	• The contributing RTP sources count are now updated accurately for the alternative file objects.

NN-ISR RSS OS-E CLI

The following RSS OS-E CLI component issues were fixed in NN-ISR, Version 5.1.

Release	Description
5.1	• The show interfaces command from the OS-E shell displays the correct output now.

NN-ISR API

The following API component issues were fixed in NN-ISR, Version 5.1.

Release	Description
5.1	• The updateFileInfo commands are now able to update custom data field values regardless of whether the names are set at the route or account level.
5.1	• Configuration scripts which are automatically included in every distributed ISR component have replaced manually editing configuration files.

NN-ISR Remote Archival Web Service

The following Remote Archival Web Service component issues were fixed in NN-ISR, Version 5.1:

Release	Description
5.1	• Configuration scripts which are automatically included in every distributed ISR component have replaced manually editing configuration files.

NN-ISR Monitor

The following Monitor VAM component issues were fixed in NN-ISR, Version 5.1:

Release	Description
5.1	• The Monitor service now immediately makes a second attempt that ignores certificate errors if the test fails the first attempt due to not having a trusted certificate.
5.1	• SNMP agents are now included on each host and documented for configuration instructions, recommended OIDs, and recommended requests.
5.1	• Configuration scripts which are automatically included in every distributed ISR component have replaced manually editing configuration files.

NN-ISR Archiver

The following NN-ISR Archiver component issues were fixed in NN-ISR, Version 5.1:

Release	Description
5.1	• Configuration scripts which are automatically included in every distributed ISR component have replaced manually editing configuration files.

Known Issues

This section describes the known issues in each component of the NN-ISR, Version 5.1.

NN-ISR Dashboard

The following are known issues in the Dashboard for NN-ISR, Version 5.1:

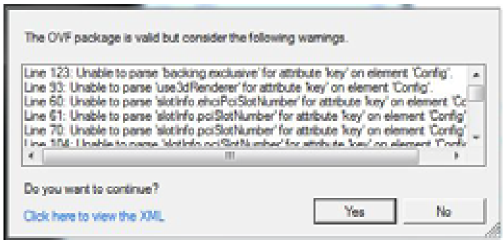
- The Dashboard help message log file location is not correct.
- The Dashboard Database failover limitation requires manual configuration of the NN-ISR Dashboard and Monitor Dashboard upon database failure.
- The Dashboard presents historical DTMF entries with granularity only to one second.
- The Dashboard change of user email limits enforcement of previous passwords.

  Note: Dashboard Third-Party Authorization integration for this release is tested for Broadworks release 19sp1.

NN-ISR RSS

The following are known issues in the RSS for NN-ISR, Version 5.1:

- In certain versions of vSphere, deployment of the RSS VM may show a Warning dialog box concerned with parsing certain OVF attributes and looks like the following:

  The OVF package is valid but consider the following warnings.

  ```
  Line 123: Unable to parse 'backing.exclusive' for attribute 'key' on element 'Config'.
  Line 93: Unable to parse 'use3dRenderer' for attribute 'key' on element 'Config'.
  Line 60: Unable to parse 'slotInfo.ehciPciSlotNumber' for attribute 'key' on element 'Cc
  Line 61: Unable to parse 'slotInfo.pciSlotNumber' for attribute 'key' on element 'Config'
  Line 70: Unable to parse 'slotInfo.pciSlotNumber' for attribute 'key' on element 'Config'
  Line 104: Unable to parse 'slotInfo.pciSlotNumber' for attribute 'key' on element 'Confi
  ```

  Do you want to continue?

  You may ignore this warning.
- Mounted drives do not persist through the RSS upgrade process.
- Filesystems are not properly managed in the OS-E shell and must be managed in the Linux shell.
- The NN-ISR Archiver version is unavailable via the log file wiht the following error reported:

  7/18/13 19:16:00[WARN] error getting build number /usr/local/jboss-4.0.2/server/default/deploy/IPCRArchival.sar/build-timestamp.properties (Not a directory)

  7/18/13 19:16:00[INFO] ISR Archiver - null

NN-ISR CIS

There are no known issues in the CIS component for NN-ISR, Version 5.1.

NN-ISR API

The following is a known issue in the API for NN-ISR, Version 5.1:

- The API does not honor the waitTime parameter.

NN-ISR Remote Archival Webservice

The following are known issues in the Remote Archival Webservice for NN-ISR, Version 5.1:

- Single quote in a recording file name causes Archival failure. Recordings are not deleted or moved.

2 Upgrading the NN-ISR

Introduction

This chapter provides information and procedures for upgrading the NN-ISR when required. Upgrading your NN-ISR software is required between major releases (4.0, 5.0, etc.) and are also required for maintenance (M1, M2, etc.) and/or patch releases (P1, P2, etc.).

Upgrading Your NN-ISR

This section provides the information and procedures required for upgrading the NN-ISR from the current release to subsequent releases (feature, maintenance, and/or patch releases). In Chapter 1, the sections, Features, Issues Fixed, and Known Issues describe specific information for this release.

Each CIS host displays its version in the “Annotation” element in the VM’s .ovf file. This may also be viewed in the summary tab of the virtual host using the vSphere client. The RSS version can be viewed by executing the command **tail /cxc_common/ISR/ISRLogs/ISRService.log** and searching for a line similar to the following:

```
2013-06-23 15:22:04 >> VoIP Media Gateway v5.1.0 (M0P0 built on
30130718.134705) starting
```

Note: Before performing the procedures in this section, verify your current operating release of the NN-ISR. You must upgrade the NN-ISR in subsequent order (for example, 5.0 to 5.0M1, 5.0M1 to 5.0M2, etc.)

To upgrade your NN-ISR, you need to perform the upgrade in the following order:

- CIS
- RSS

Control and Index Server (CIS)

Use the procedures in this section to upgrade the Control and Index Server (CIS). Upgrade procedures include:

- Before You Begin
- Updating the Index VM Database
- Importing the New Dashboard VM
- Deleting the Prior Dashboard VM
- Verifying the CIS Upgrade

Before you Begin

Before you begin the upgrade of the CIS, the following must be met:

- NN-ISR must have the latest CIS software (prior to this upgrade) currently installed and working properly.

- New Virtual Machine (VM) files (unzipped) for the Index must be resident on your Windows host machine that is managing the VM with the VSphere Client. This file is:
  - *ISR Index Version <#> build <#> OVF Template.zip*
- Find and make note of the Dashboard public IP addresses. You enter these addresses when performing the procedures in Importing the New Dashboard VM.

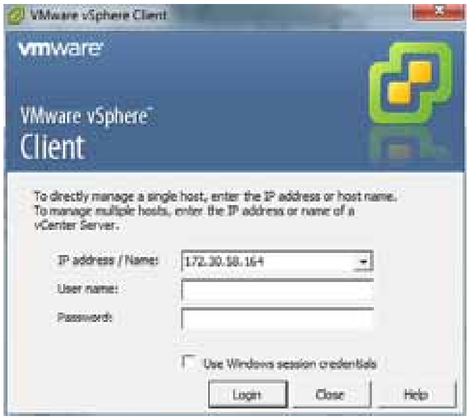
Updating the Index VM Database

When upgrading the CIS, you must replace each Dashboard, Monitor, and Remote Archival Webservice CIS VM with a new one.The Index host upgrade requires additional steps to be taken when existing recordings and configuratioin information must be maintained.

When upgrading a CIS Index from 5.0M1P1 or 5.0M1P2 to 5.1, you must run the latest 5.1 Index host on the same hypervisor (either ESXi 4.1 or vSphere) server as the Index host being replaced. Once the 5.1 Index VM is deployed and powered on, you must connect to it using the vSphere console and log in.

To log into the vSphere server:

1. Double-click the VMware vSphere Client icon. The following screen displays.



To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 172.30.58.164

User name:

Password:

□ Use Windows session credentials

2. In the "**IP address / Name**" text box, enter the IP address or the domain name of the ESXi host. For example:

   `IP address / Name: **172.30.58.164**`

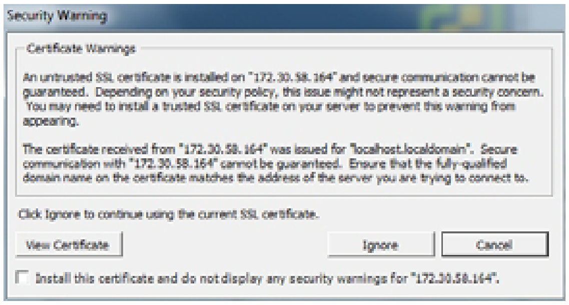
3. In the "**User name**" text box, enter the user name assigned to you by the system administrator of the ESXi host. For example:

   `User name: **root**`

4. In the Password text box, enter the password assigned to you by the system administrator of the ESXi host. For example:

   `Password: **jre453i**`

5. Click <**Login**>. The following Security Warning displays:



Security Warning

Certificate Warnings

An untrusted SSL certificate is installed on "172.30.58.164" and secure communication cannot be guaranteed. Depending on your security policy, this issue might not represent a security concern. You may need to install a trusted SSL certificate on your server to prevent this warning from appearing.

The certificate received from "172.30.58.164" was issued for "localhost.localdomain". Secure communication with "172.30.58.164" cannot be guaranteed. Ensure that the fully-qualified domain name on the certificate matches the address of the server you are trying to connect to.

Click Ignore to continue using the current SSL certificate.

View Certificate | Ignore | Cancel

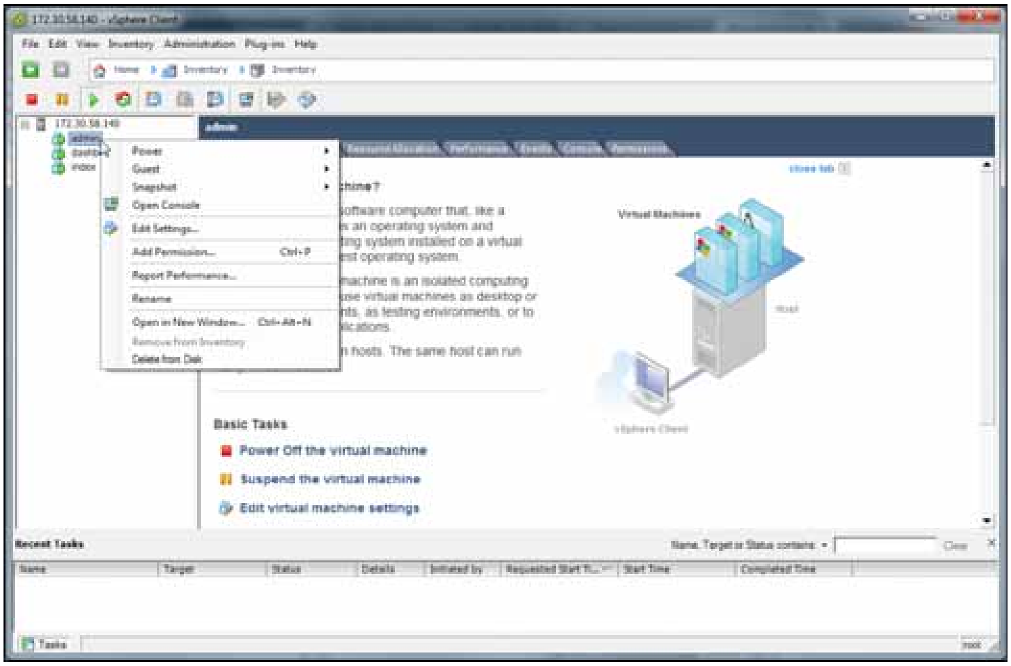
□ Install this certificate and do not display any security warnings for "172.30.58.164".

6. Place a check mark in the box that indicates:

   "*Install this certificate and do not display any security warnings for <ip_address>"*.

   The IP address is the address of the ESXi host.

7. Press <**Ignore**>. The following window displays.

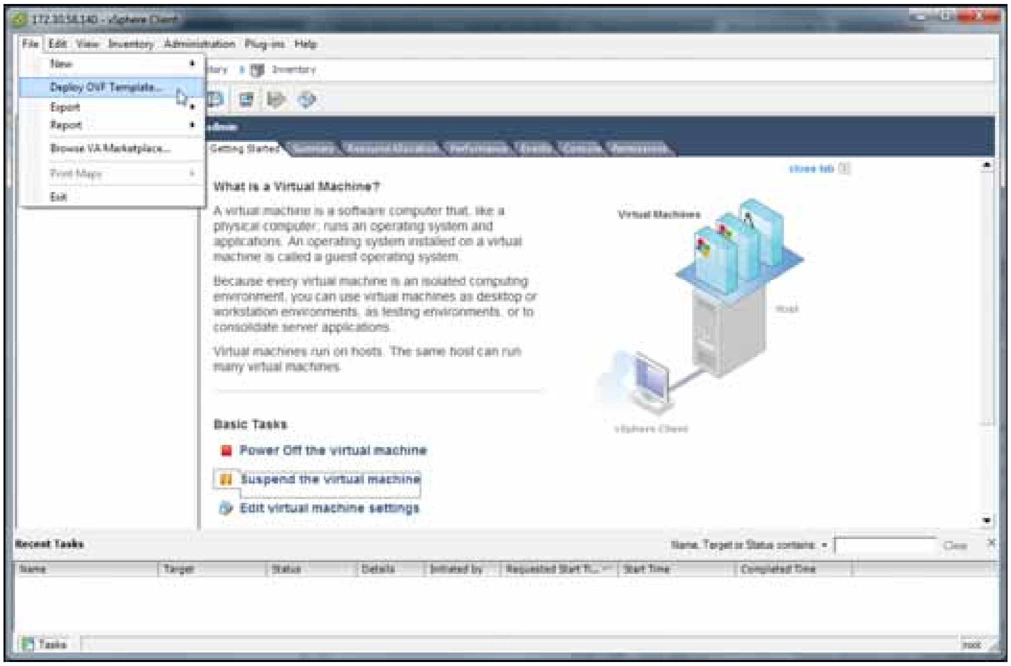


8. In the left column, click the IP address to display the VMs.

Importing the New Index VM

To import the new Index VM:

1. In the VMware vSphere Client, select "**File->Deploy OVF Template....**"



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

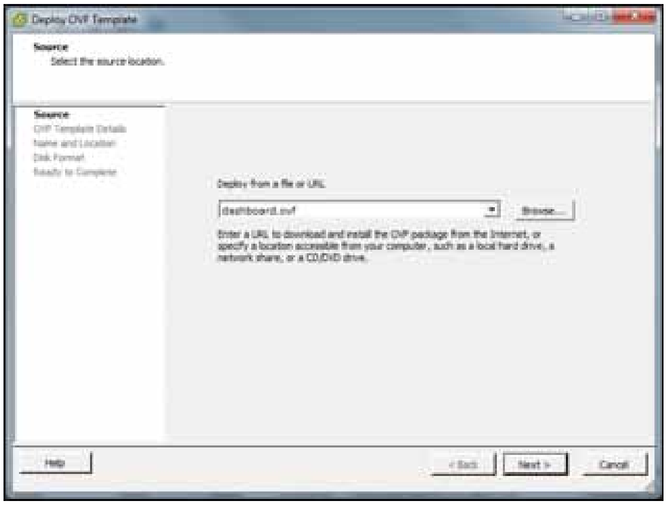
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

- Power Off the virtual machine
- Suspend the virtual machine
- Edit virtual machine settings

The following window displays.



Source

Select the source location.

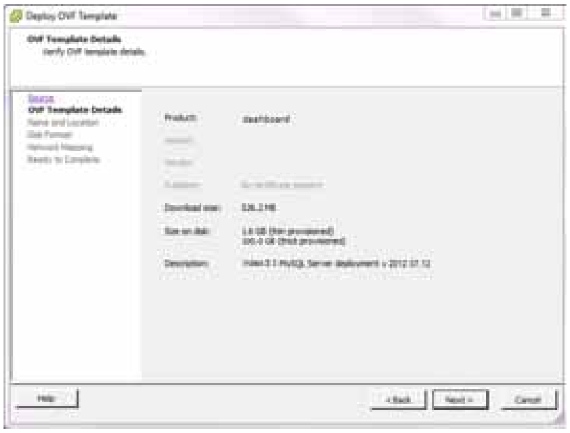
Deploy from a file or URL: dashboard.ovf

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

2. In the "**Deploy from a file or URL**" field, browse to the directory that contains the files you unzipped from the file , "*ISR Index Version <#> build <#>.zip"* on your Windows host machine.

   Note: For more information about transferring the required new files to your Windows host machine, see Control and Index Server (CIS).

3. Select the "**index.ovf**" file and click <**Open**>.
4. Click <**Next**>. The following window displays.



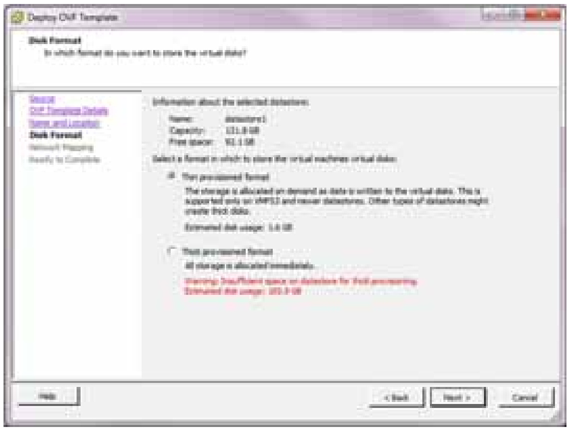
OVF Template Details
Verify OVF template details.

Product: dashboard
Version:
Vendor:
Publisher: No certificate present
Download size: 526.2 MB
Size on disk: 1.6 GB (thin provisioned)
100.0 GB (thick provisioned)
Description: Index 5.1 MySQL Server deployment v 2012.07.12

5. Click <**Next**> in the “OVF Template Details” window. The “Name and Location” window displays. This field is automatically populated with the name and location of the virtual machine you selected in Step 3.

   Note: The old Index VM may already have the name “index” and the vSphere wizard automatically names the new VM the same name. You have the choice to either rename the old VM or choose a new name for this VM.

6. Click <**Next**>. The “Disk Format” window displays.



Disk Format
In which format do you want to store the virtual disks?

Information about the selected datastore:
Name: datastore1
Capacity: 131.8 GB
Free space: 92.1 GB

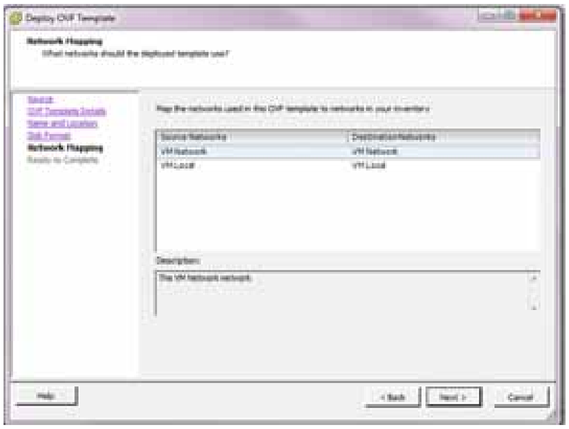
Select a format in which to store the virtual machines virtual disks:

● Thin provisioned format
The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks.
Estimated disk usage: 1.6 GB

○ Thick provisioned format
All storage is allocated immediately.
Warning: Insufficient space on datastore for thick provisioning.
Estimated disk usage: 100.0 GB

Note: If using CIS certified hardware, verify the datastore name is correct.

7. Select "**Thin provisioned format**" with disk usage of **3.2 GB** (default) and click <**Next**>. The “Network Mapping” window displays.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

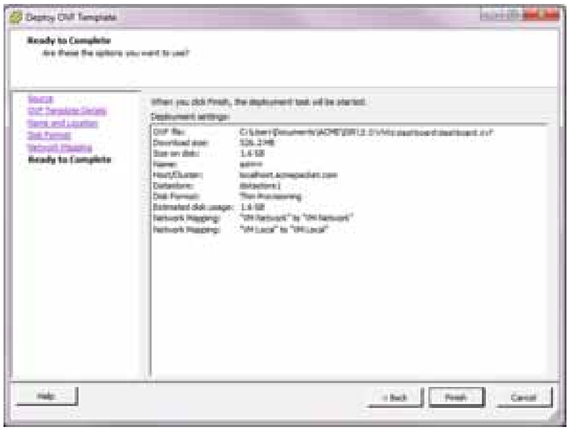
Source Networks	Destination Networks
VM Network	VM Network
VM Local	VM Local

Description:

The VM Network network.

8. Verify that “VM Network” and the “VM Local” are in both the Source Network column and the Destination Network column.

9. Click <**Next**>. The following window displays.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

```
OVF file:              C:\Users\[illegible]\Documents\ACME\ISR\12.3\VMs\dashboard\dashboard.ovf
Download size:         526.2 MB
Size on disk:          1.6 GB
Name:                  admin
Host/Cluster:          localhost.acmepacket.com
Datastore:             datastore1
Disk Format:           Thin Provisioning
Estimated disk usage:  1.6 GB
Network Mapping:       "VM Network" to "VM Network"
Network Mapping:       "VM Local" to "VM Local"
```

10. Verify all selections in the “Ready to Complete” window are correct and click <**Finish**>.

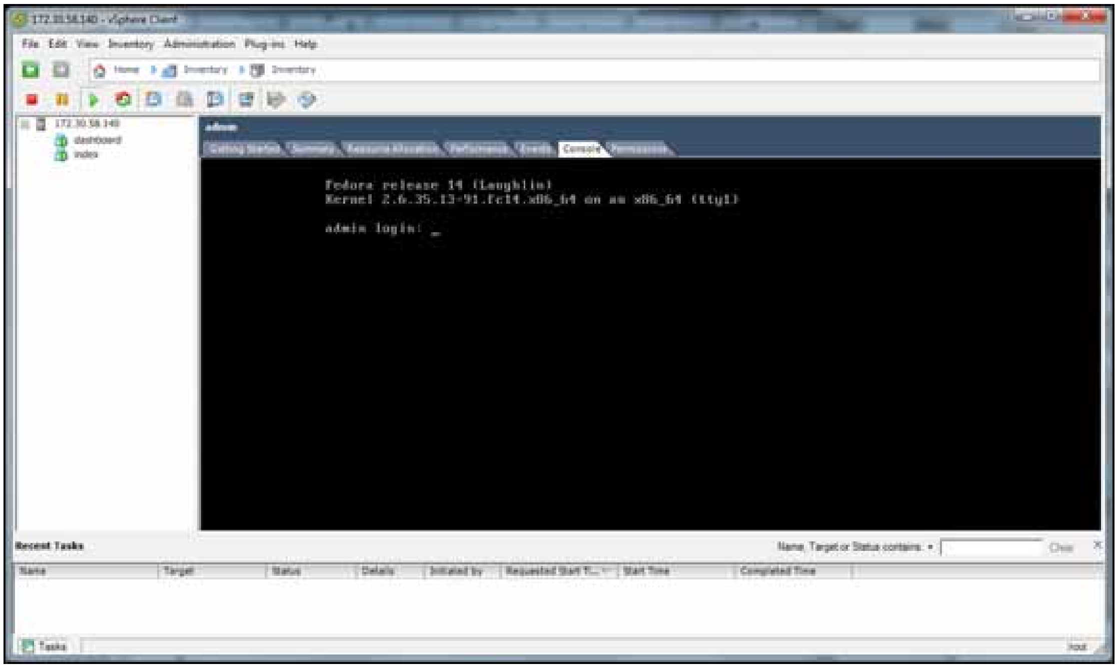
11. When the deployment of the *index.ovf* is complete, close the “Deploy OVF Template” window by clicking the “X” in the upper right corner.

12. In the VMware vSphere Client window, select the “**index**” VM from the left column.

13. Click the Power on button.

14. Click on the **Console** tab.

    Note: During the remaining procedures using the Console window, the mouse may be confined to the console pane. Press <**Alt**><**Ctrl**> to release it at any time. The following window displays.



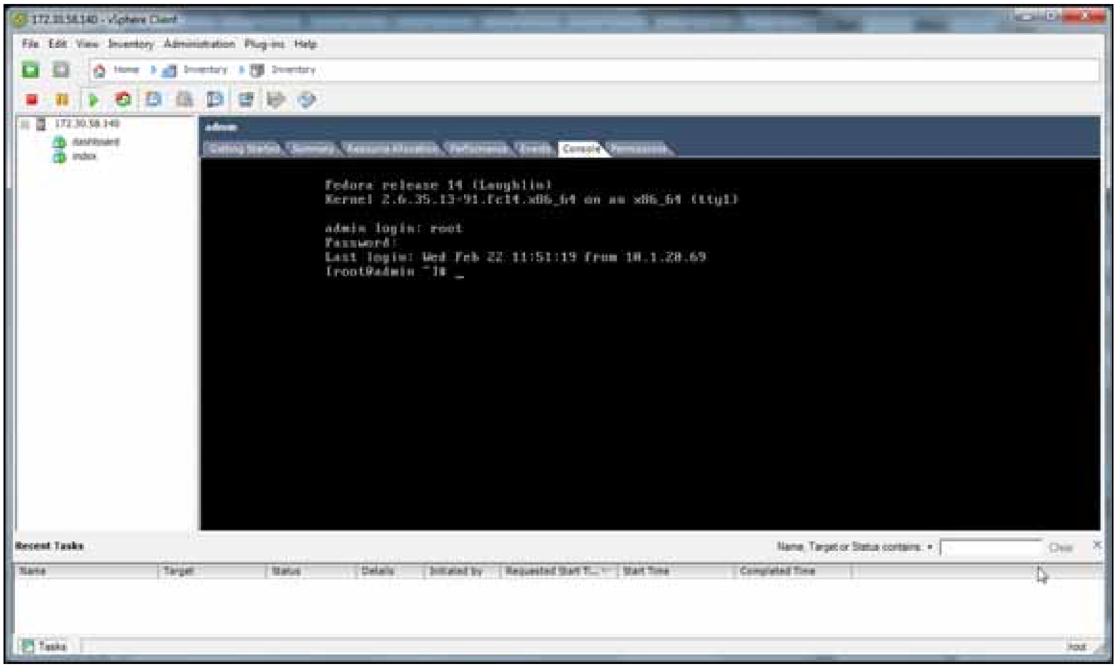
```
Fedora release 14 (Laughlin)
Kernel 2.6.35.13-91.fc14.x86_64 on an x86_64 (tty1)

admin login: _
```

15. Login using ID “**root**” and password “**64^5377**”.

    ```
    Index login: root
    Password: 64^5377
    ```

    The following screen displays.



```
Fedora release 14 (Laughlin)
Kernel 2.6.35.13-91.fc14.x86_64 on an x86_64 (tty1)

admin login: root
Password:
Last login: Wed Feb 22 11:51:19 from 10.1.20.69
[root@admin ~]# _
```

16. Enter **upgradeCis.sh** and press <*Enter*>.

    Note: In some upgrade situations, the old Index VM may not have the openssh package you need for the secure copying portion of the upgrade. If the old Index VM was originally installed wiht an older version, you must ensure the package is included. To do this, execute the **yum list openssh-clients** command and confirm the openssh-clients package appears under “Installed Packages”.

17. Press <*Enter*> to begin the Index upgrade process.

    The upgrade application displays the MySQL server service shutting down and the following prompt is displayed:

    ```
    The authenticity of host ‘169.254.1.50 (169.254.1.50)’ can’t be
    established. RSA key fingerprint is
    a2:19:ea:b2:6f:58:41:d5:89:63:56:88:94:8d:80:74. Are you sure you want
    to continue connecting (yes/no)?
    ```

18. Type **yes** and press <*Enter*>.

    The upgrade application then displays the following message:

    ```
    Warning: Permanently added ‘169.254.1.50’ (RSA) to the list of known
    hosts.
    ```

19. Enter the old CIS host **root** password.

    Note: By default this is **64^5377**. However, your password may have been changed.

    The upgrade application displays the secure copying of several MySQL InnoDB files.

20. Enter the old CIS host **root** password again.

    The upgrade application displays the secure copying of several “ipcr_db” database files.

21. In vSphere power off the old (5.0M1P1 or 5.0M1P2) Index VM database.

22. Within the new Index VM upgradeCis.sh script press <*Enter*>.

    The upgrade application does the following:

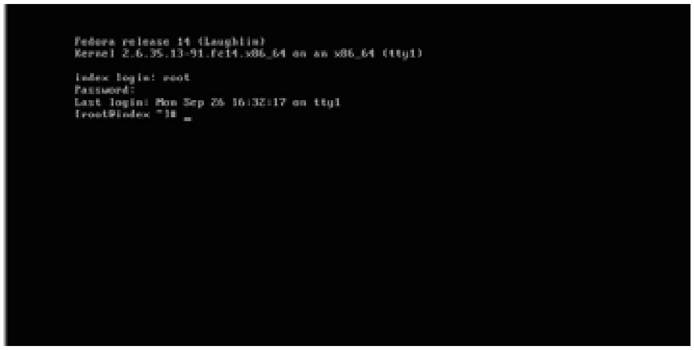
    - Displays the MySQL server service starting up
    - Upgrades the imported “ipcr_db” schema to reflect changes to 5.1
    - Displays “Index upgrade complete”

To configure the IP address:

1. From the vSphere client console, log into the Index VM with the following and press <Enter>:

   ```
   <VM> Login: root
   Password: 64^5377
   ```

The following screen displays.



```
Fedora release 14 (Laughlin)
Kernel 2.6.35.13-91.fc14.x86_64 on an x86_64 (tty1)

Index login: root
Password:
Last login: Mon Sep 26 16:32:17 on tty1
[root@Index ~]# _
```

2. Execute the **configCis.sh** script. The following menu displays:

- s <*Enter*>—Show the current configuration

- q <*Enter*>—Quit the application
- m <*Enter*>—Modifies the current RSS configuration. The following fields appear:
  - Enter Host IP: [*Host IP*]
    - Eth0 interface IPv4 address of the CIS host
  - Enter prefix: [16]
    - The routing prefix, e.g., 192.168.1.1/16
  - Enter gateway IP: [*Gateway IP*]
    - The IPv4 address of the network gateway or router.
  - Enter DNS1 IP: [<*DNS1 IP* | none>]
    - The IPv4 address of the first DNS, which may be skipped (set to **none**) and ignored.
  - Enter DNS2 IP: [<*DNS2 IP* | none>]
    - The IPv4 address of the second DNS, which may be skipped (set to **none**) and ignored.

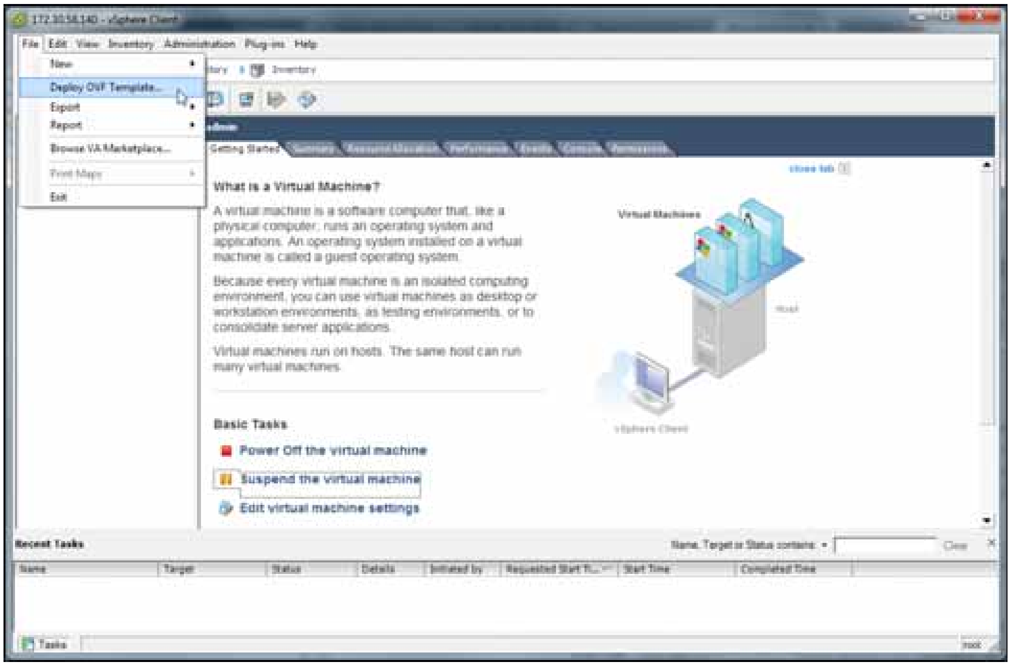
  Note: To skip to the next field, hit <*Enter*>.

Enter valid values for any fields that require updating. Once all necessary information has been properly entered, the message “Configuration updated.” appears while the CIS host restarts the network service to apply the changes. Any failures that may have occured are displayed at this time.

Importing the New Dashboard VM

To import the new Dashboard VM:

1. In the VMware vSphere Client, select “**File->Deploy OVF Template....**”



What is a Virtual Machine?

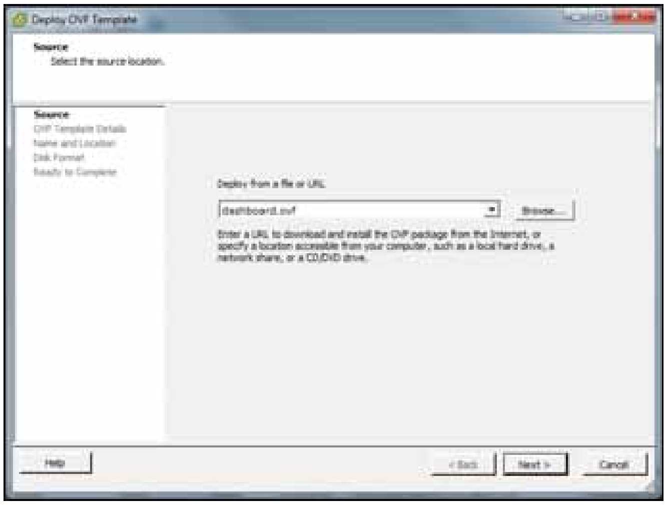
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

The following window displays.



Deploy from a file or URL

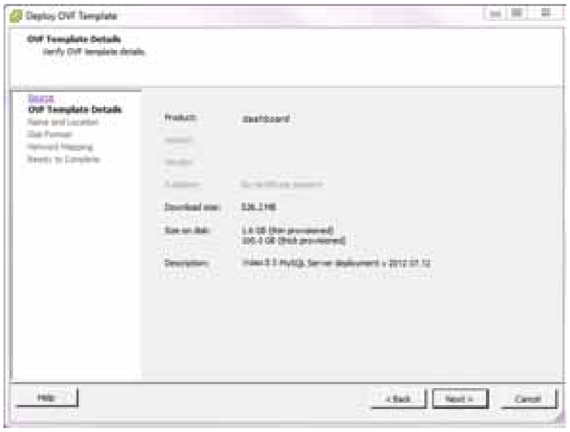
dashboard.ovf

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

2. In the “**Deploy from a file or URL**” field, browse to the directory that contains the files you unzipped from the file , “*ISR Dashboard Version <#> build <#>.zip”* on your Windows host machine.

   Note: For more information about transferring the required new files to your Windows host machine, see Control and Index Server (CIS).

3. Select the “**dashboard.ovf**” file and click <**Open**>.
4. Click <**Next**>. The following window displays.



Product: dashboard

Version:

Vendor:

Publisher: No certificate present

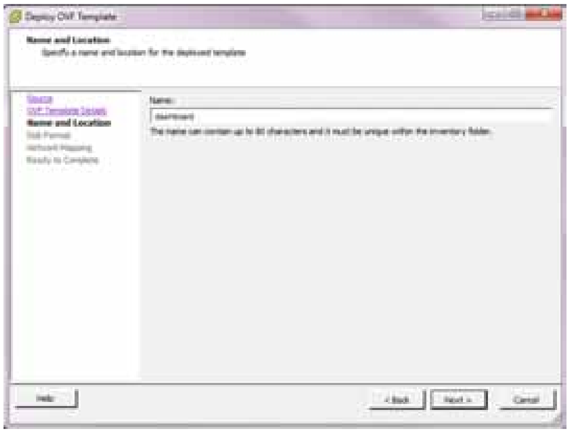
Download size: 526.2 MB

Size on disk: 1.6 GB (thin provisioned)
100.0 GB (thick provisioned)

Description: Video 5.5 MySQL Server deployment v 2012.07.12

5. Click <**Next**> in the “OVF Template Details” window. The “Name and Location” window displays. This field is automatically populated with the name and location of the virtual machine you selected in Step 3.

   Note: The old Dashboard VM may already have the name “dashboard” and the vSphere wizard automatically names the new VM the same name. You have the choice to either rename the old VM or choose a new name for this VM.

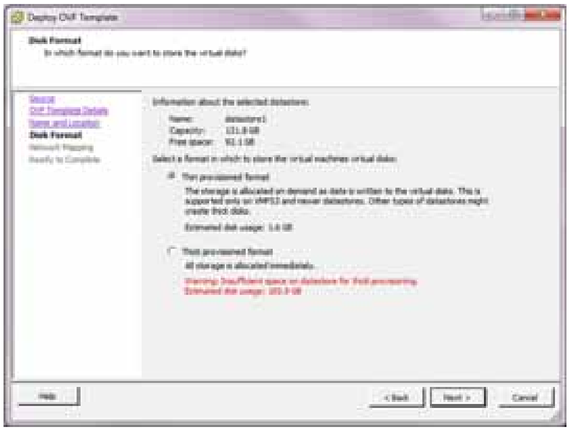


Name and Location
Specify a name and location for the deployed template

Name:
dashboard

The name can contain up to 80 characters and it must be unique within the inventory folder.

6. Click <**Next**>. The “Disk Format” window displays.



Disk Format
In which format do you want to store the virtual disks?

Information about the selected datastore:

Name:	datastore1
Capacity:	131.8 GB
Free space:	92.1 GB

Select a format in which to store the virtual machines virtual disks:

● Thin provisioned format

The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks.

Estimated disk usage: 1.6 GB

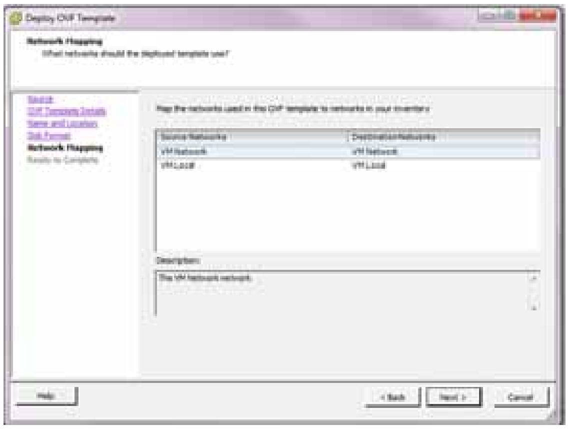
○ Thick provisioned format

All storage is allocated immediately.

Warning: Insufficient space on datastore for thick provisioning.
Estimated disk usage: 103.9 GB

Note: If using CIS certified hardware, verify the datastore name is correct.

7. Select "**Thin provisioned format**" with disk usage of **3.2 GB** (default) and click <**Next**>. The “Network Mapping” window displays.



Network Mapping
What networks should the deployed template use?

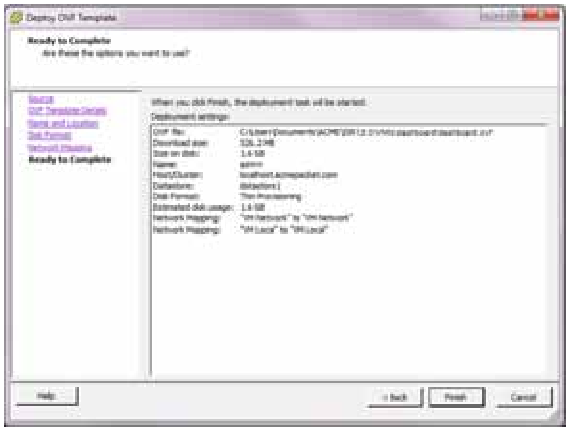
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	VM Network
VM Local	VM Local

Description:
The VM Network network.

8. Verify that “VM Network” and the “VM Local” are in both the Source Network column and the Destination Network column.

9. Click <**Next**>. The following window displays.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\Documents\ACME\ISR\2.0\VMs\dashboard\dashboard.ovf
Download size:	526.2 MB
Size on disk:	1.6 GB
Name:	admin
Host/Cluster:	localhost.acmepacket.com
Datastore:	datastore1
Disk Format:	Thin Provisioning
Estimated disk usage:	1.6 GB
Network Mapping:	"VM Network" to "VM Network"
Network Mapping:	"VM Local" to "VM Local"

10. Verify all selections in the “Ready to Complete” window are correct and click <**Finish**>.

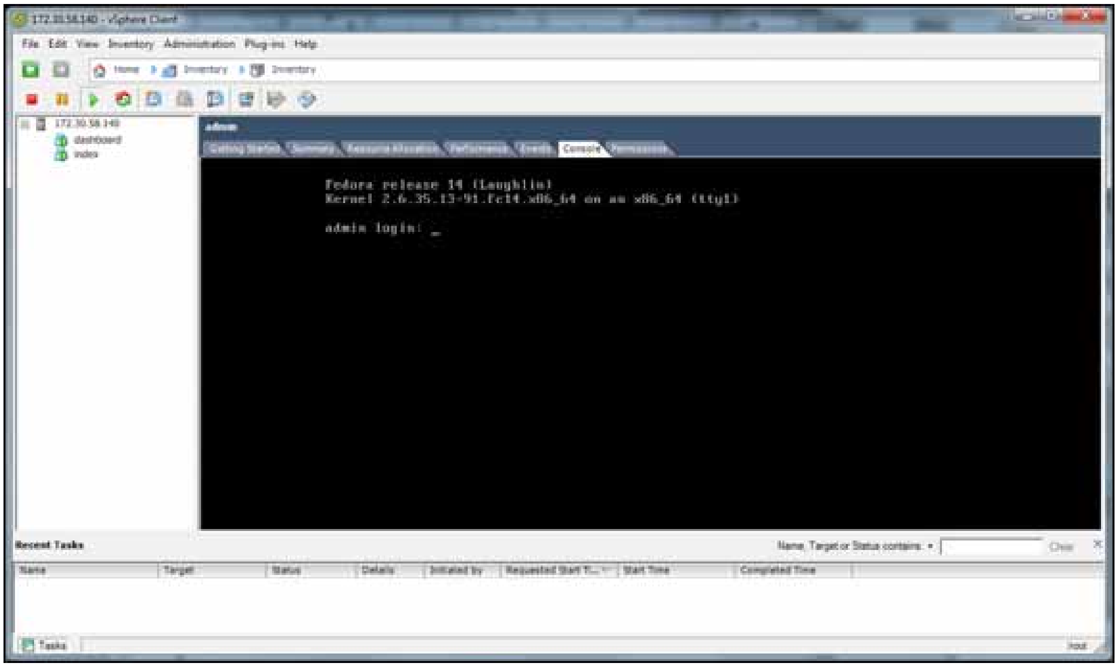
11. When the deployment of the *dashboard.ovf* is complete, close the “Deploy OVF Template” window by clicking the “X” in the upper right corner.

12. In the VMware vSphere Client window, select the “**dashboard**” VM from the left column.

13. Click the Power on button.

14. Click on the **Console** tab.

    Note: During the remaining procedures using the Console window, the mouse may be confined to the console pane. Press <**Alt**><**Ctrl**> to release it at any time. The following window displays.



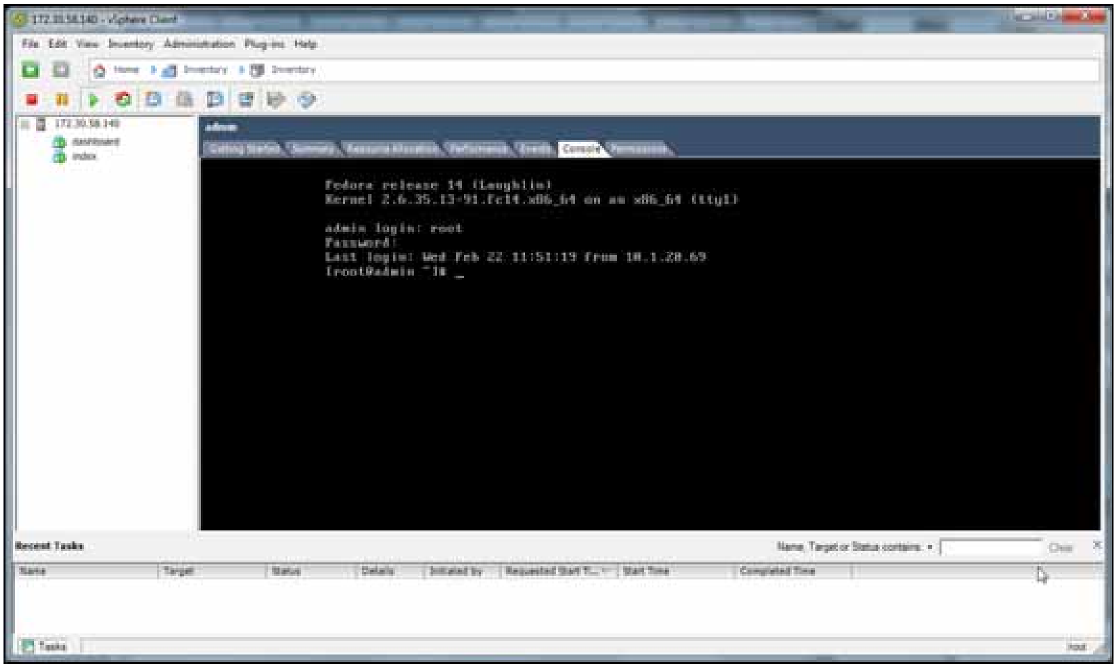
```
Fedora release 14 (Laughlin)
Kernel 2.6.35.13-91.fc14.x86_64 on an x86_64 (tty1)

admin login: _
```

15. Login using ID “**root**” and password “**64^5377**”.

```
admin login: root
Password: 64^5377
```

The following screen displays.



172.30.58.140 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
172.30.58.140
dashboard
index
admin
Getting Started Summary Resource Allocation Performance Events Console Permissions
Recent Tasks
Name, Target or Status contains: Clear
Name Target Status Details Initiated by Requested Start Ti... Start Time Completed Time
Tasks
root

```
Fedora release 14 (Laughlin)
Kernel 2.6.35.13-91.fc14.x86_64 on an x86_64 (tty1)

admin login: root
Password:
Last login: Wed Feb 22 11:51:19 from 10.1.20.69
[root@admin ~]# _
```

16. Execute the **configCis.sh** script. The following menu displays:

- s <*Enter*>—Show the current configuration
- q <*Enter*>—Quit the application
- m <*Enter*>—Modifies the current RSS configuration. The following fields appear:
  - Enter Host IP: [*Host IP*]
    - Eth0 interface IPv4 address of the CIS host
  - Enter prefix: [16]
    - The routing prefix, e.g., 192.168.1.1/16
  - Enter gateway IP: [*Gateway IP*]
    - The IPv4 address of the network gateway or router.
  - Enter DNS1 IP: [<*DNS1 IP* | none>]
    - The IPv4 address of the first DNS, which may be skipped (set to **none**) and ignored.
  - Enter DNS2 IP: [<*DNS2 IP* | none>]
    - The IPv4 address of the second DNS, which may be skipped (set to **none**) and ignored.

    Note: To skip to the next field, hit <*Enter*>.

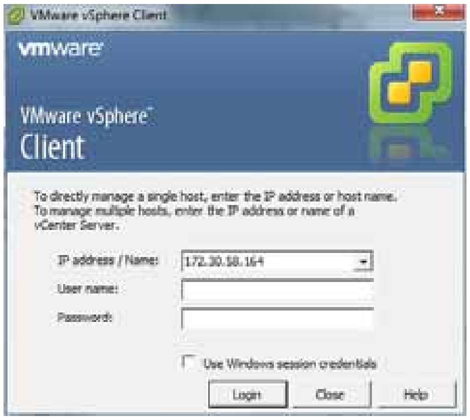
Enter valid values for any fields that require updating. Once all necessary information has been properly entered, the message “Configuration updated.” appears while the CIS host restarts the network service to apply the changes. Any failures that may have occured are displayed at this time.

Importing the new Dashboard VM is complete.

Deleting the Prior Dashboard VMs

To delete the prior Dashboard VMs:

1. Double-click the VMware vSphere Client icon. The following screen displays.



To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 172.30.58.164

User name:

Password:

□ Use Windows session credentials

2. In the “**IP address / Name**” text box, enter the IP address or the domain name of the ESXi host. For example:

```
IP address / Name: 172.30.58.164
```

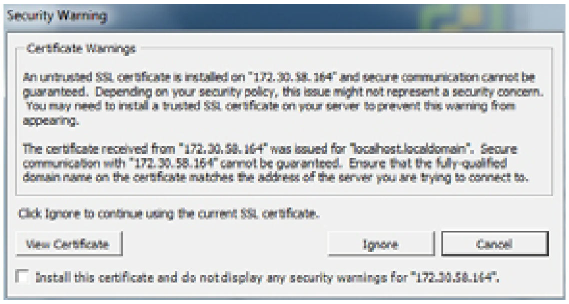
3. In the “**User name**” text box, enter the user name assigned to you by the system administrator of the ESXi host. For example:

```
User name: root
```

4. In the Password text box, enter the password assigned to you by the system administrator of the ESXi host. For example:

```
Password: jre453i
```

5. Click <**Login**>. The following Security Warning displays:



An untrusted SSL certificate is installed on "172.30.58.164" and secure communication cannot be guaranteed. Depending on your security policy, this issue might not represent a security concern. You may need to install a trusted SSL certificate on your server to prevent this warning from appearing.

The certificate received from "172.30.58.164" was issued for "localhost.localdomain". Secure communication with "172.30.58.164" cannot be guaranteed. Ensure that the fully-qualified domain name on the certificate matches the address of the server you are trying to connect to.

Click Ignore to continue using the current SSL certificate.

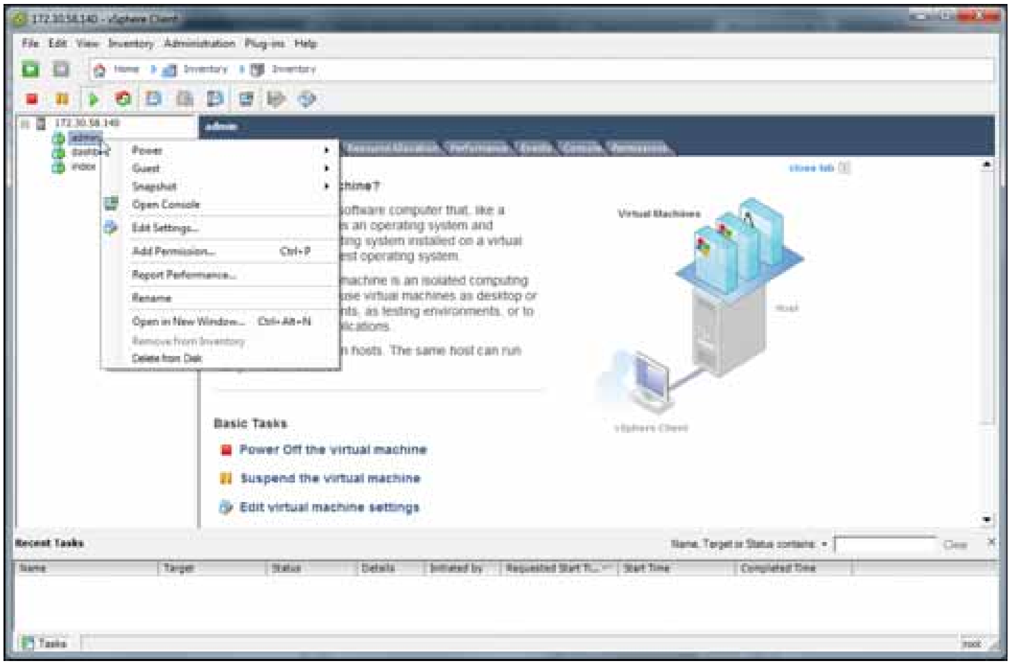
□ Install this certificate and do not display any security warnings for "172.30.58.164".

6. Place a check mark in the box that indicates:

   "*Install this certificate and do not display any security warnings for <ip_address>".*

   The IP address is the address of the ESXi host.

7. Press <**Ignore**>. The following window displays.

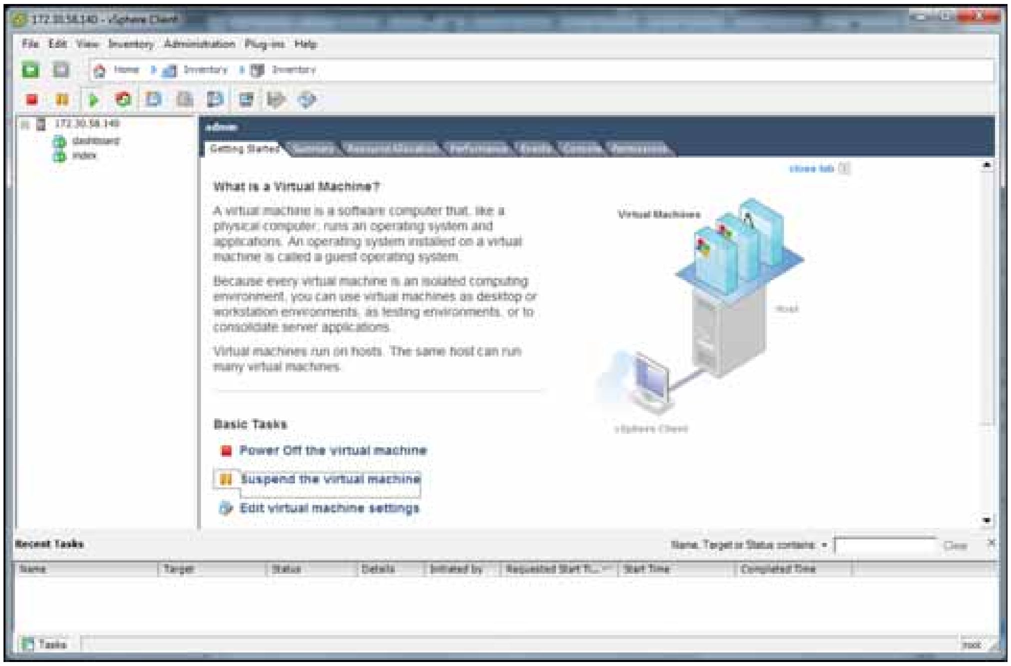


8. In the left column, click the IP address to display the VMs.

9. Using your mouse, right click the “**dashboard**” VM, and then select “**Delete from Disk**”. A prompt displays for you to verify the deletion of the dashboard VM.

   “Delete the virtual machine ‘dashboard’?”

10. Click <**Yes**>. The prior User Dashboard deletes from the CIS.



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

Power Off the virtual machine

Suspend the virtual machine

Edit virtual machine settings

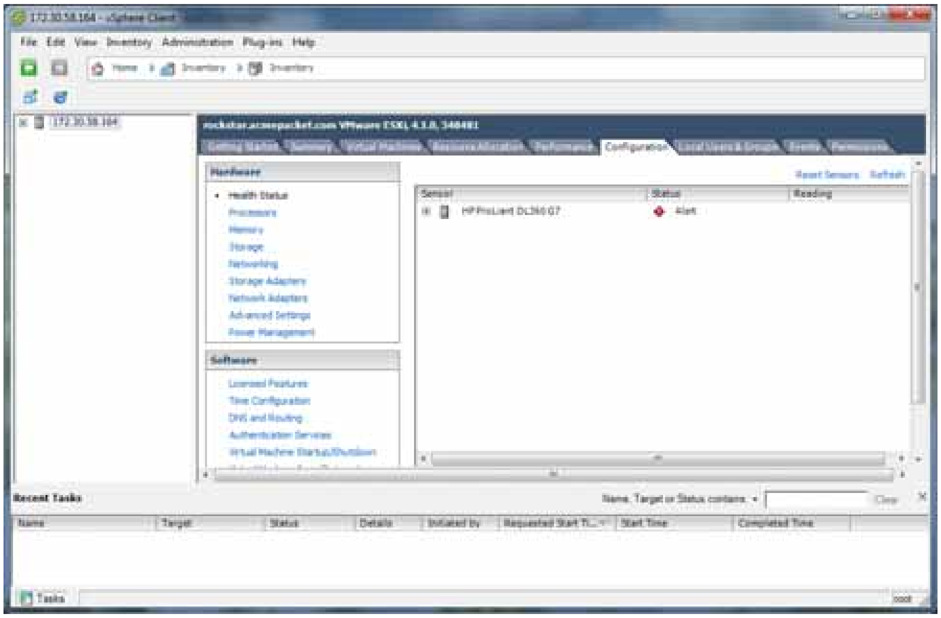
Configuring Automatic Start of the Upgraded VMs

When all updated CIS components are installed, you must configure the VMs to start automatically.

Use the following procedure to configure the virtual machines to start automatically.

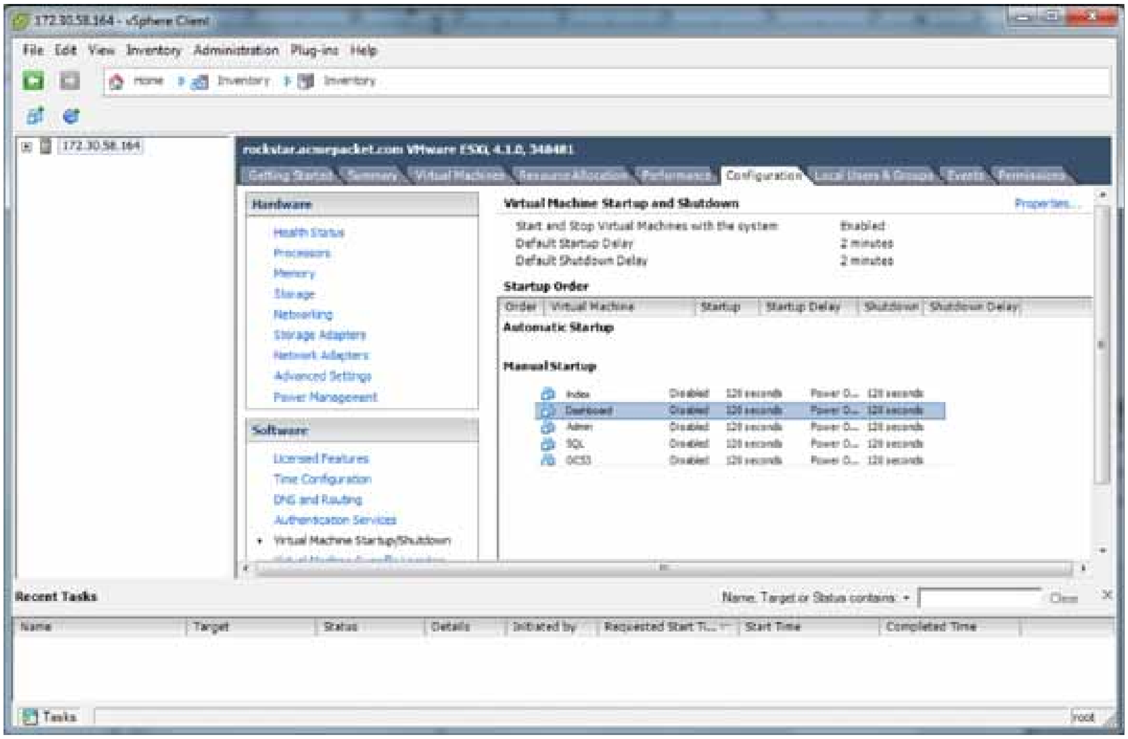
To configure the VMs to start automatically:

1. Open the vSphere Client application to the Home page.
2. Click on the **Configuration** tab.



Sensor	Status	Reading
HP ProLiant DL360 G7	Alert	

3. In the left column, under the Software category, click on **Virtual Machine Startup/Shutdown**. The following screen displays.



172.30.58.164 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
rockstar.acmepacket.com VMware ESXi, 4.1.0, 348481
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions
Hardware
Health Status
Processors
Memory
Storage
Networking
Storage Adapters
Network Adapters
Advanced Settings
Power Management
Software
Licensed Features
Time Configuration
DNS and Routing
Authentication Services
Virtual Machine Startup/Shutdown
Properties...
Recent Tasks
Name, Target or Status contains:
Clear
Tasks
root

Virtual Machine Startup and Shutdown

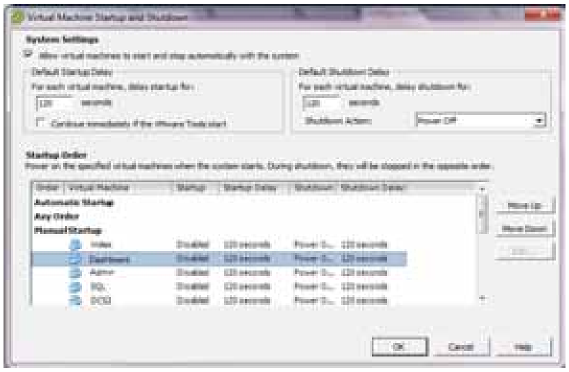
Start and Stop Virtual Machines with the system Enabled
Default Startup Delay 2 minutes
Default Shutdown Delay 2 minutes

Startup Order

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup					
Manual Startup					
	Index	Disabled	120 seconds	Power O...	120 seconds
	Dashboard	Disabled	120 seconds	Power O...	120 seconds
	Admin	Disabled	120 seconds	Power O...	120 seconds
	SQL	Disabled	120 seconds	Power O...	120 seconds
	OCSI	Disabled	120 seconds	Power O...	120 seconds

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time

4. In the upper right corner of the window, click **Properties**. The following window displays:



System Settings

☑ Allow virtual machines to start and stop automatically with the system

Default Startup Delay
For each virtual machine, delay startup for:
120 seconds
☐ Continue immediately if the VMware Tools start

Default Shutdown Delay
For each virtual machine, delay shutdown for:
120 seconds
Shutdown Action: Power Off

Startup Order
Power on the specified virtual machines when the system starts. During shutdown, they will be stopped in the opposite order.

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup					
Any Order					
Manual Startup					
	Index	Disabled	120 seconds	Power O...	120 seconds
	Dashboard	Disabled	120 seconds	Power O...	120 seconds
	Admin	Disabled	120 seconds	Power O...	120 seconds
	SQL	Disabled	120 seconds	Power O...	120 seconds
	OCSI	Disabled	120 seconds	Power O...	120 seconds

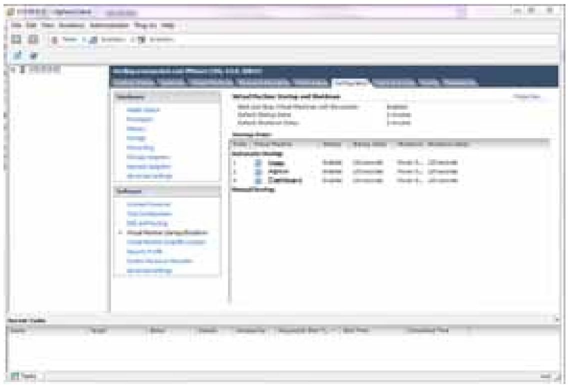
5. In System Settings section, enable the **Allow virtual machines to start and stop automatically with the system** by placing a check mark in the box.

6. In the Startup Order section, select the **Index** entry and then click <**Move Up>** to include the index virtual machine in the Automatic Startup group.

   Note: When moving the entry up in the window, continue to click <Move Up> until the entry is in the appropriate category.

7. Select the **Dashboard** entry and then click <**Move Up>** to place the Dashboard VM just below the Index entry in the Automatic Startup group.

8. Click **OK**. The window should displays as follows.



Verifying the CIS Upgrade

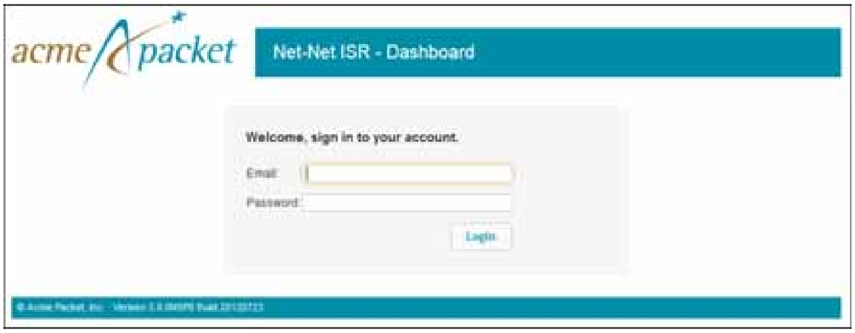
You can log into the NN-ISR Dashboard to verify that the upgrade was successful.

To log into the NN-ISR dashboard:

1. Open your Internet Web browser (see compatible browser requirements in Net-Net ISR Dashboard Requirements).
2. Enter the following IP address of your NN-ISR in your network:

   `http://<Dashboard IP address>`

   The Login page displays.



3. In the "**Email**" and "**Password**" fields, enter the applicable email and password, respectively. The default email and password are:

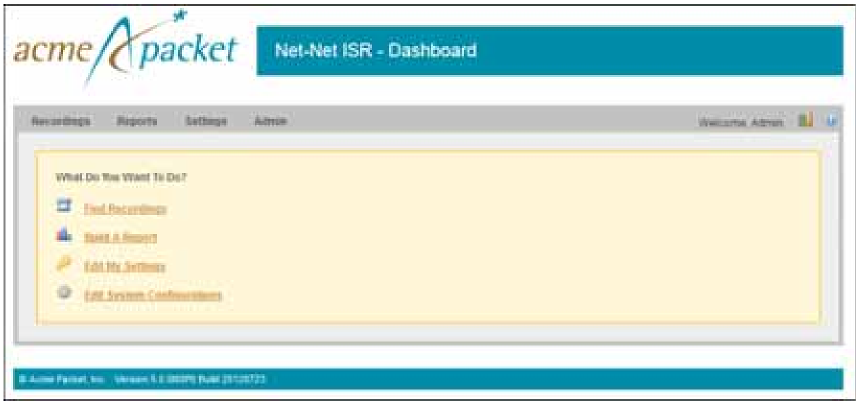
   Email: isradmin@acmepacket.com

   Password: Admin123

   Note: If you changed your password from the default in your prior software, then enter that password in the "Password" field. The password from the prior software has been saved to your new version software. You can skip Step 4 and proceed to Step 5.

   If you did not change the default password in your prior software, then you have the option of changing it in the new version of software. On your initial login, you are prompted to change your password.
4. Respond to the prompts as applicable to change your password.
5. Verify that the NN-ISR version number is visible in the blue bar at the bottom of the window.

The following page displays after logging in.



You can now use the Dashboard as required.

Record and Store Server (RSS)

Use the procedures in this section to upgrade the Record and Store Server (RSS). Upgrade procedures include:

- Before You Begin
- Determining the RSS System Partitions
- (optional) Mounting a Different Partition
- Upgrading the RSS
- Reverting Your Installation to the Previous Version

Note: Configuration scripts, which are automatically included in every distributed NN-ISR component, have replaced manually editing configuration files.

Before you Begin

Before you begin the upgrade of the RSS, the following must be met:

- NN-ISR must have the latest RSS software (prior to this upgrade) currently installed and working properly.
- New RSS file (supertar upgrade file) must be resident on your RSS host machine in the directory */cxc_common/releases/*. This file is:
  - *nnRSS-<version>-<build_date>.upgrade-a.tar.gz*
- Determine the system partition for which the RSS is currently running on. For a procedure, see Determining the RSS System Partition.

Determining the RSS System Partitions

Before beginning the upgrade, you must determine the RSS system partition on which the NN-ISR is currently running.

To determine the RSS partition:

1. Startup the NN-ISR system.
2. At the “Login as” prompt, enter “**root**” and press <Enter>.

   ```
   Login as: root
   ```

   The password prompt displays.
3. At the “Password” prompt, enter “**sips**” and press <Enter>.

```
root@<hostname>’s password> sips
The following prompt and message display.
Net-Net OS-E
Copyright (c) 2004-2012 Acme Packet Inc.
Username:
```

Note: The login input shown is the default security settings and may be different on your NN-ISR if it has been changed.

4. No username is required so press <Enter>.

```
Username: (leave blank)
The password prompt displays.
```

5. No password is required so press <Enter>.

```
Password: (leave blank)
The following message displays followed by the NN-ISR hostname prompt.
“Access granted since there are no configured users.”
NN-ISR>
```

6. Enter “**show chassis-config**” and press <Enter>.

```
NN-ISR> show chassis-config
The following is an example of the output that displays.
    boot-partition: system-2
 system-partitions: 2
management-console: vga
        ipmi-admin: enabled
```

The boot-partition field should indicate “**system-1**” or “**system-2**”.

7. If you want to mount the partition other than the partition that displays in the output, see Mounting a Different Partition.

(optional) Mounting a Different Partition

You can mount another partition to use for the upgrade of the RSS if required.

To mount another partition:

1. At the NN-ISR prompt, enter “**show mounts**”, and press <Enter>.

```
NN-ISR> show mounts
The following is an example of the output that displays.
```

```
drive     mount-point    drive-name     filesystem     drive-size percent-free
-----     -----------    ----------     ----------     ---------- ------------
system-1  /mnt/backup                                  0          0
system-2  /              /dev/root      reiserfs       7164       66
```

The output above shows the active mounted system to be the “**system-2**” partition.

2. Enter “**mount system-#**”, and press <Enter>.

```
NN-ISR> mount system-1
```

where “system-#” is the system you want to mount. If “system-1” is the active mounted system, then enter “system-2” for Step 2.

This mounts the other partition to */mnt/backup/*. You can access the available RSS files on the newly mounted partition as required (for example, */mnt/backup/cxc/isrl.elf*).

Upgrading the RSS

After determining the RSS partition (or mounting another partition), you can upgrade the RSS as required.

Note: This upgrade procedure installs the new version of software to the inactive partition and then makes the partition active.

To upgrade the RSS:

1. At the NN-ISR prompt, enter a shell session by entering “**shell**” and press <Enter>.

```
NN-ISR> shell
The hostname prompt displays.
<hostname> #
```

2. Copy the RSS supertar upgrade file to the RSS host’s filesystem by entering the following:

```
<hostname> # cp nnSE-a.tar.gz /cxc_common/releases/
```

3. Enter “**exit**” to exit the shell and display the NN-ISR> prompt.

```
<hostname> # exit
NN-ISR>
```

4. At the NN-ISR prompt, enter “**install file /releases/nnSE-a.tar.gz**”, and press <Enter>.

```
NN-ISR> install file /releases/nnSE-a.tar.gz
The upgrade process proceeds on the RSS using the file you specified.
When the upgrade is complete, the RSS server reboots.
```

5. At the “Login as” prompt, enter “**root**” and press <Enter>.

```
Login as: root
The password prompt displays.
```

6. At the “Password” prompt, enter “**sips**” and press <Enter>.

```
root@<hostname>’s password> sips
The following prompt and message display.
Net-Net OS-E
Copyright (c) 2004-2012 Acme Packet Inc.
Username:
```

7. No username is required so press <Enter>.

```
Username: (leave blank)
The password prompt displays.
```

8. No password is required so press <Enter>.

```
Password: (leave blank)
The following message displays followed by the NN-ISR hostname prompt.
“Access granted since there are no configured users."
NN-ISR>
```

9. Verify the active partition is correct by entering “**show chassis-config**”, and press <Enter>.

10. The following is an example of the output that displays.

```
    boot-partition: system-1
 system-partitions: 2
management-console: vga
        ipmi-admin: enabled
```

The RSS upgrade is complete.

(optional) Reverting Your Installation to the Previous Version

During the upgrade process, the RSS installs the new version of software, as well as copies of the current configuration, to the non-active partition. You have the ability to revert back to the last version that was installed.

Note: For more information on determining which partition is active, see the section Determining the RSS System Partitions.

To revert your installation to the previous version:

At the NN-ISR prompt, enter “**set-chassis-config-boot system-#**”, and press <Enter>.

```
NN-ISR> set-chassis-config-boot system-2
```

where “system-#” is the inactive partition you want to access.