Interactive Session Recorder

Installation Guide

Release 6.4
F29534-06
January 2022

ORACLE

Interactive Session Recorder Installation Guide, Release 6.4

F29534-06

Contents

B Public Cloud Platforms

C Configuring an NFS Share For Archival

D Configuring Circular Replication

E ISR RMC

F ISR Troubleshooting and Customizations

G Selective Call Recording SIPREC

About This Guide

The Interactive Session Recorder Installation Guide provides information including:

- Overview of the Interactive Session Recorder (ISR)
- Hardware/Software Requirements/Recommendations
- ISR Software Installation Procedures
- Post-install and Verification Procedures
- Making the First Call
- FACE API Installation Procedures
- Additional Advanced Topics (Appendices)

Related Documentation

The following table describes the documentation set for this release.

Document Name	Document Description
ISR Release Notes	Contains information about new ISR features, fixes, and known issues.
ISR Installation Guide	Provides an overview of the ISR, hardware/ software requirements and recommendations, storage considerations, pre-installation information, installation procedures, post-install verification procedures, making the first call, and additional advanced topics about the ISR.
ISR User Guide	Contains information about using the ISR Dashboard for all levels of users. Provides information about viewing, playing, deleting recordings, running reports, and managing user profiles.
ISR Administrator Guide	Contains information about using the ISR Dashboard for the Administrator level user (Super User, Account Administrator, Tenant Administrator). Provides information about creating and managing accounts, routes, and users. Also provides information about configuring the ISR, running reports, viewing active calls, and securing the ISR deployment.
ISR API Reference Guide	Contains information about ISR FACE API, Recording File Types/Formats Supported, Return Codes, and Troubleshooting.
ISR Monitoring Guide	Provides provisioning, configuration and test instructions for the NET-SNMP implementation to monitor all ISR component hosts.

Document Name	Document Description
ISR Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the ISR product.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select `2` for New Service Request.
2. Select `3` for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select `1`.
   - For non-technical issues such as registration or assistance with My Oracle Support, select `2`.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Revision History

This section provides a revision history for this document.

Date	Description
March 2020	• Initial release of ISR 6.4 software.
July 2020	• Adds "Public Cloud Platforms" appendix.
November 2020	• Updates the supported tomcat version in "Third-Party Dependencies for Offline Installation". • Updates the supported MySQL version number in "Installing the ISR Index and "Index Virtual Machine" in the Troubleshooting appendix.
February 2021	• Updates the supported tomcat version to tomcat-7.0.76-15.el7.noarch. • Adds note to "Installing the ISR Components" and "Upgrade Prerequisites" regarding tomcat.
April 2021	• Updates the supported Oracle Linux version to 7.2 - 7.7.
January 2022	• Updates the supported MySQL version to 5.7.36.

1 Overview

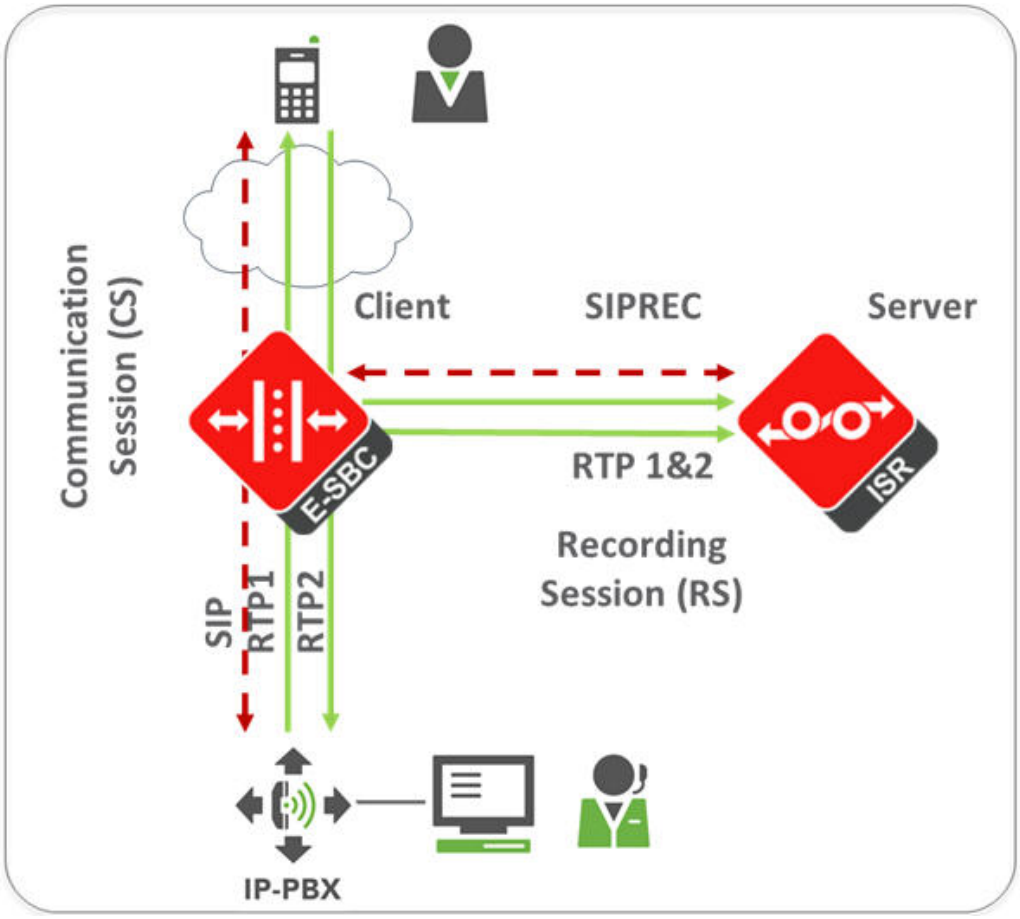
This section provides an overview of the ISR.

About the ISR

Driven by a profusion of government and industry regulations, enterprises are required to record and store an increasing quantity of communications sessions in order to maintain compliance. Conventional call recording solutions, designed for capturing contact center agent exchanges for training or quality assurance purposes, are not well suited to compliance recording applications. They are difficult to integrate with business applications, offer limited scalability, and can be costly to deploy.

The Oracle Communications Interactive Session Recorder (ISR) is specifically designed to eliminate enterprise compliance recording cost and complexity. The solution features an open, standards-based architecture that dramatically simplifies the capture and storage of real-time IP communications sessions throughout the enterprise. Ideal for a wide range of compliance applications, ISR leverages a modular design for superior scalability and economics, offers an extensive API set for ultimate extensibility and flexibility, and includes integrated support for screen recording using an industry leading user monitoring solution.

The ISR leverages SIPREC and a modular architecture for ease of deployment and scale. SIPREC uses a client/server architecture, where the SIPREC client (the Oracle Enterprise Session Border Controller in the image below) initiates SIPREC sessions with the SIPREC server (the Oracle ISR).



For an introduction to SIPREC and its configuration on the Oracle Session Border Controller, see the "Selective Call Recording/SIPREC" appendix in this guide or .

Session Recording Client Support

The ISR has been tested with the following SIPREC Session Recording Platforms:

- Oracle communications Session Border Controller
- Oracle Enterprise Session Border Controller
- Broadworks Application Server R21

2
Hardware/Software Requirements

This section provides the hardware and software pre-requisites for installing the ISR. It provides the recommended hardware and VM configurations you can use in your network.

Hardware

The ISR components are distributed as applications running on Oracle Linux Releases 7.2 - 7.7, which abstracts the ISR application from the physical hardware. As such, ISR can be deployed on any hardware platforms that support Oracle Linux Releases 7.2 - 7.7. For a comprehensive list of the hardware platforms currently certified, see the Oracle Linux and Oracle VM Hardware Certification List (HCL).

ISR testing is predominantly done on Oracle Server X5-2 and Oracle Server X6-2 systems with the following resource configurations:

Hardware Description	Quantity
Intel® Xeon® E5-2630 v3 8-core 2.4 GHz processor	2
One 16 GB DDR4-2133 DIMM	8
One 1.2 TB 10000 rpm 2.5-inch SAS-3 HDD with marlin bracket in RAID 10 configuration using 12Gb SAS RAID HBA	4

> **Note:**
>
> RAID must be configured BEFORE performing the ISR component installation.

Each of the ISR components must be installed on their own server/VM instance.

Minimum Virtual Machine Resource Configurations

The ISR virtual hosts have the following default VM configurations:

Configuration Type	RSS	Index	Dashboard	FACE API
VM Version	8	8	8	8
CPU	4 vCPU	4 vCPU	1 vCPU	1 vCPU
Memory	16GB	8GB	2GB	2GB
Disk Provisioning Type	Thin	Thin	Thin	Thin
Disk Provisioned Size	256GB*	256GB*	12GB	12GB
Network Adapter 1	Admin	Admin	Admin	Admin

Configuration Type	RSS	Index	Dashboard	FACE API
Network Adapter 2	Local	Local	Local	Local
Network Adapter 3	Voice	Voice	Voice	Voice
Network Adapter 4	Data	Data	Data	Data

WARNING:

The values in the table above reflect the minimum resources required to run the ISR components in a lab/trial environment. For information on your ISR production deployment sizing needs, contact your Oracle representative.

Networking Considerations

The ISR expects four separate network interfaces for the following functions:

Network	Expected Use
Admin	Management Interface, used for accessing consoles and SNMP traffic
Local (169.254.1.x)	Used for internal communications between the various ISR components
Voice	SIP and Media traffic
Data	Recording Archival and all FACE API traffic

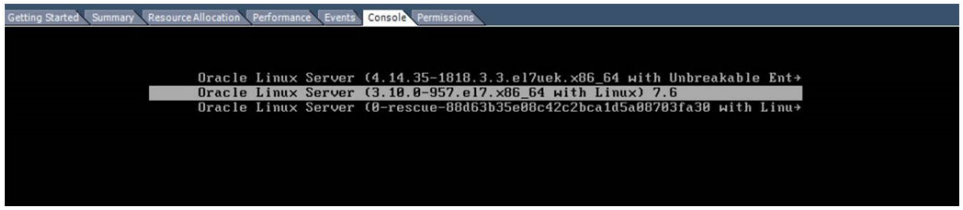
The *Interactive Session Recorder Security Guide* covers the ISR networking considerations in depth. Oracle recommends reviewing that document before proceeding with the installation.

Red Hat Kernel Compatible Support

ISR has been successfully tested and is compatible with the Red Hat kernel compatible with Oracle Linux 7.6. Red Hat Compatible Kernel is configured at boot time selections.

To enable RHEL:

1. Open a terminal for the ISR components.
2. Enter **reboot**.
3. Select **Oracle Linux server with Linux 7.6** and press Enter.



Installation Prerequisites

Before beginning your ISR installation, ensure you have completed the following prerequisites:

1. Have at least three servers (physical or virtual) with Oracle Linux Release 7.2 - 7.7 installed.
2. Have access to the ISR rpms:
   - `isr-Index-<release#>.x86_64.rpm`
   - `isr-Dashboard-<release#>.x86_64.rpm`
   - `isr-rss-<release#>.x86_64.rpm`
   - `isr-Face-<release#>.x86_64.rpm` (optional)

   > **Note:**
   >
   > You may access these files via https://edelivery.oracle.com..

3. Have access to the Ruby 2.6 rpm (ruby-2.6.4-1.el7.centos.x86_64.rpm). Ruby is the framework the ISR Dashboard uses and must be installed as part of the ISR Dashboard installation.
4. Configure a Linux User named **isradm** on each of the Linux instances created in step 1 to allow you to automatically gain access to config and log files. Once you have configured the **isradm** Linux user, you must add the user to the "sudoers" group.
5. Verify that the hosts you are installing the ISR components on are connected to the internet.

   > **Note:**
   >
   > If your ISR hosts do not have internet connectivity, see "Installing ISR In an Isolated Lab".

6. Oracle Linux 7 has the yum package management utility configured by default with access to the "public-yum.oracle.com" repositories in the file located at `/etc/yum.repos.d/public-yum-ol7.repo`. If, for some reason, this file needs to be created, see the Appendix, "Oracle Public Yum Repository Configuration File" in the *Oracle Communications Interactive Session Recorder Installation Guide*, which contains the specific repository entries.
7. Configure interfaces; ISR expects network configuration to include 4 interfaces, connecting to separate Administration, Local, Data, and Voice networks. Refer to the Oracle Communications Interactive Session Recorder Security Guide for more information on networking and trusted boundaries.
   For more information on configuring networking in Oracle Linux 7, see the *man nmtui* guide and http://www.unixarena.com/2015/04/rhel-7-network-management-nmcli-or-nmtui.html.

8. If access to the external yum repository is gated by a proxy, ensure the **proxy** parameter in the `/etc/yum.conf` file is set to:

   ```
   proxy=http://<your_proxy_host>
   ```

> **Note:**
>
> During the installation process, you will be asked to provide and/or verify the users, passwords and interfaces you created during the Oracle Linux installation. Ensure you have that information before you begin the installation process.

ISR Dashboard Requirements

The ISR Dashboard is a web portal that is used for recording configuration and playback. As web technologies advance, some functionality may not be available on older browser versions. The ISR has been tested with the following web browsers and versions:

- Google Chrome (Version 63.0.3239.84 64-bit)
- Mozilla Firefox (Version 52.5.2 32-bit)
- Microsoft Edge (Version 40.15063.674.0)

> **Note:**
>
> Browser playback support for recording codecs changes frequently. Refer to the *Oracle Communications Interactive Session Recorder Release Notes* for current details.

Supported Codecs

The ISR supports the following transmission codecs:

- g.711 mulaw
- g.711 alaw
- g.729
- g.722 and g.722.2 (excluding g.722.1)
- H.264
- AMR-WB

The audio transmission codecs can be mapped to the following recording formats:

Header Raw	Header WAVE	Format	Bit Rate	Sample Rate (KHz)	Channels Mono	Channels Stereo
YES	YES	ulaw	8	8	YES	YES
YES	YES	alaw	8	8	YES	YES

Header Raw	Header WAVE	Format	Bit Rate	Sample Rate (KHz)	Channels Mono	Channels Stereo
YES	YES	Linear PCM	8	8	YES	YES
NO	YES	Linear PCM	16	8	YES	YES
NO	YES	Linear PCM	16	1	YES	NO
NO	YES	Linear PCM	16	16	NO	YES
NO	YES	ADPCM	4	8	YES	YES

H.264 video content is stored and replayed in MP4 format.

Sample Implementation Diagrams

The following are sample ISR/SBC implementation diagrams.

Figure 2-1 Single Site-Single Server ISR/SBC Implementation

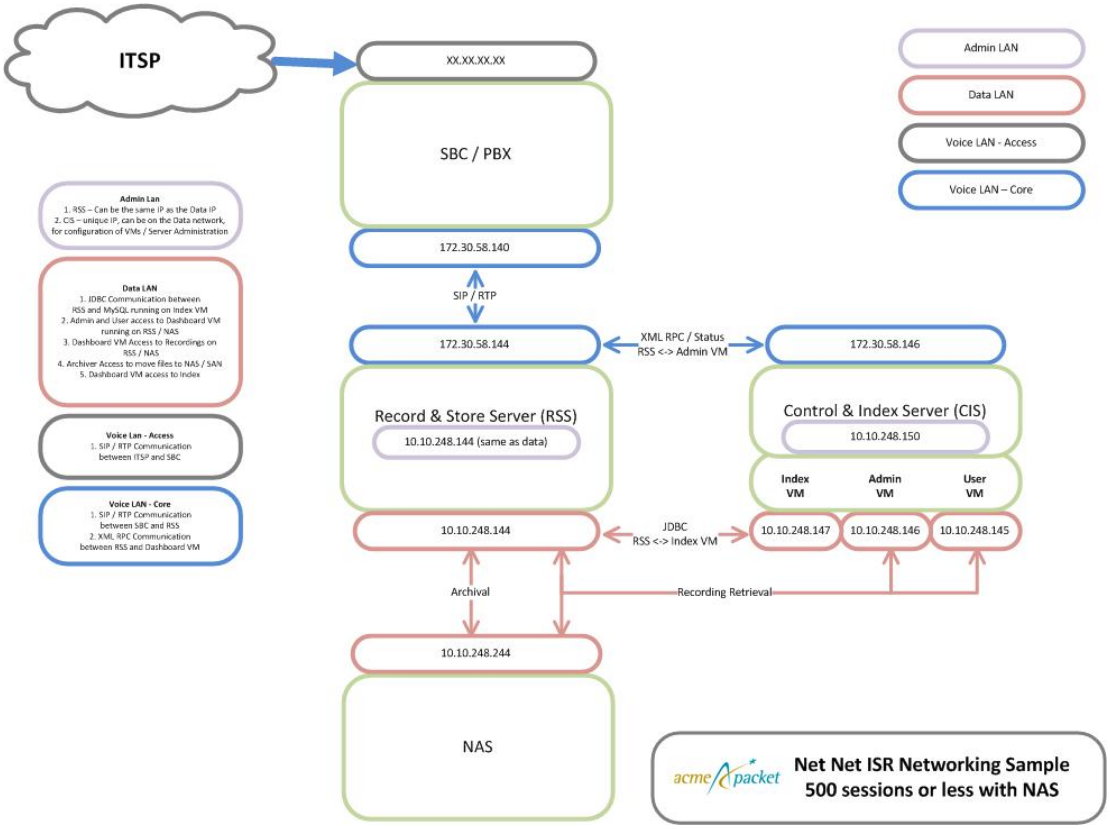


Figure 2-2 Single Site-2RSS ISR/SBC Implementation

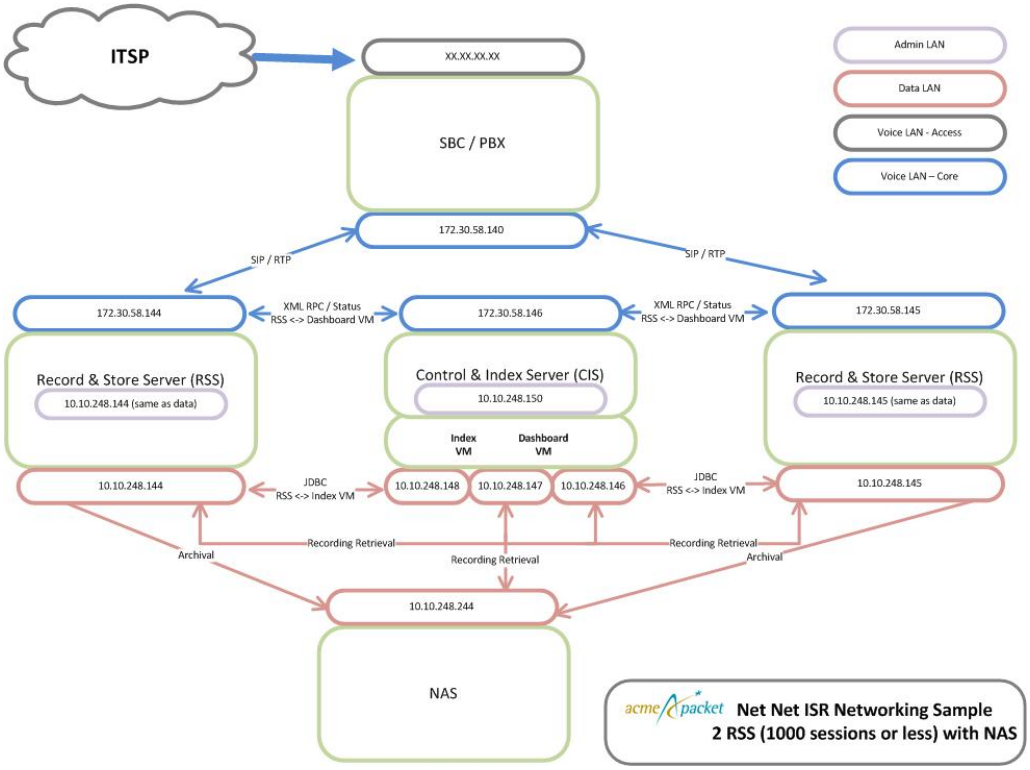
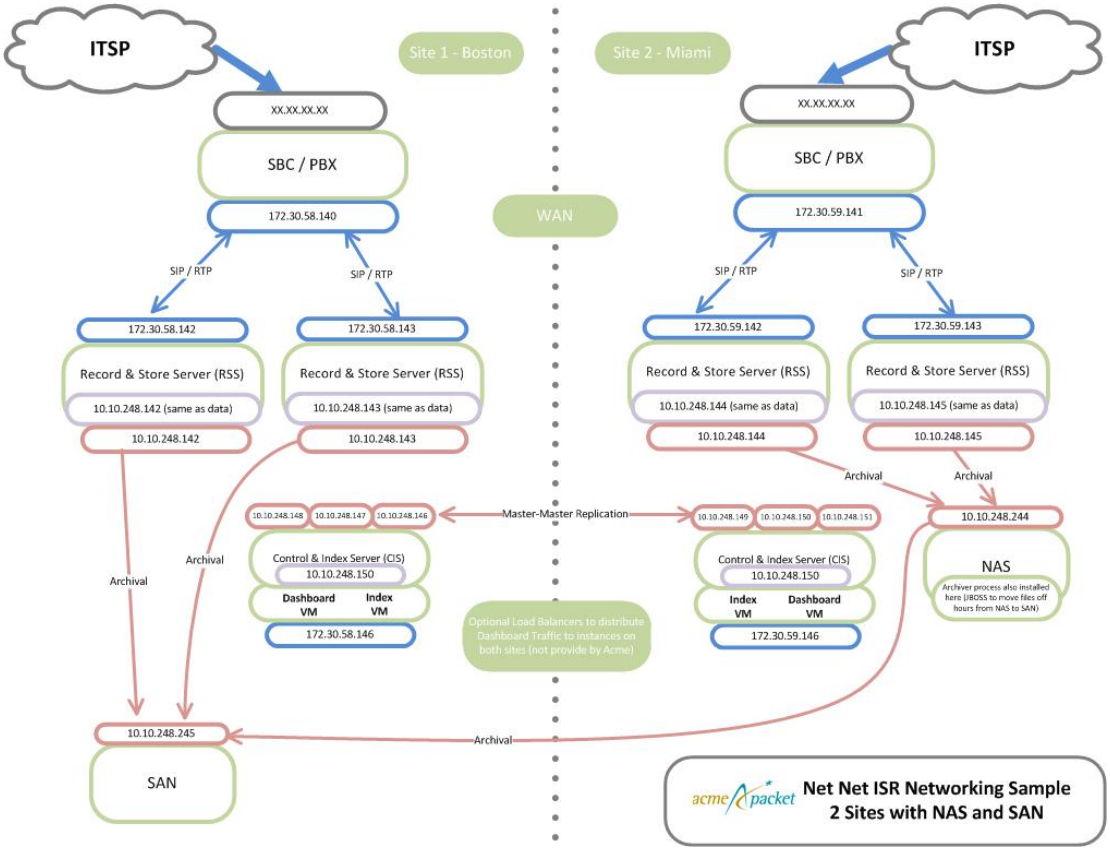


Figure 2-3 Dual Site Redundant ISR/SBC Implementation



3

Installing the ISR Software

This chapter provides the information and procedures you need to install the ISR components.

The ISR runs on Oracle Linux 7 and uses yum to install and update RPM files.

> **Note:**
>
> The ISR has been tested with Oracle Linux only. Other Linux distributions have not been tested or verified.

You must have Oracle Linux Releases 7.2 - 7.7 installed on your hardware prior to installing the ISR. Refer to the "Installation Prerequisites" section of this guide before proceeding.

You must install the ISR components in the following order:

1. Index
2. RSS
3. Dashboard
4. FACE API (optional)

> **Note:**
>
> The order in which you install the ISR components is very important. The installation does not work if you install the components in any order other than the order listed above.

ISR Software

The following components are installed during the ISR installation process:

- Index
- RSS
- Dashboard
- FACE API (optional)

Installing the ISR Components

This section describes how to install the ISR components, including the Index, Dashboard, and RSS. Note that when you install RSS and FACE, the ISR picks up the latest available tomcat version from the OL 7 repository.

> **Note:**
>
> During the installation process, you will be asked to provide and/or verify the users, passwords, and interfaces you created during the Oracle Linux installation.

Installing the ISR Index

This section describes how to install the ISR Index.
The ISR requires installations of both MySQL Server and the MySQL client application, which are included in the Index RPM. The ISR includes MySQL Enterprise Commercial (Advanced) Edition Version 5.7.36. For more information, see Oracle's MySQL Products page to learn more about the MySQL platform.

> **Note:**
>
> During the installation process, you will be asked to provide and/or verify the users, passwords, and interfaces you created during the Oracle Linux installation, including:
>
> - OS root passwords of all ISR component hosts
> - MySQL root password in the case of an existing MySQL deployment (otherwise the temporary password is replaced during initial configuration)
> - An understanding of how to map your four network interfaces to ISR's 'Admin', 'Local', 'VoIP', and 'Data'.

To install the ISR Index:

1. Log into the Oracle Linux CLI using an SSH client.

   > **Note:**
   >
   > The Oracle Linux CLI is case-sensitive.

2. Verify that the Index is connected to the Internet and that yum.conf is properly configured with the proxy. For more information, see "Installation Prerequisites".
3. Most ISR installation environments do not have access to a repository with the RPM required to install the isr-Index RPM itself. The best way to manage this issue is to (secure) copy the following file onto the Index host:

   - isr-Index-<*release#*>.x86_64.rpm

   Once the file is properly copied, connect to the Index host with an SSH client and in the directory (for example, /tmp) containing the file, execute the following command:

   ```
   # sudo yum localinstall /tmp/isr-Index-<release#>.x86_64.rpm
   ```

> **Note:**
>
> Upon initial installation, the Index's configISR.sh does not pull the temporary mysql password. Before proceeding with the ISR Index installation, run the following command:
>
> ```
> yum remove mariadb-libs
> ```

4. Verify the installation when prompted.

   ```
   Is this ok [y/d/N]:y
   ```

   The Index application is installed.

5. To configure the Index server:

   ```
   sudo /opt/isr/configIsr.sh
   ```

6. Follow the script's instructions closely.

> **Note:**
>
> In order to install MySQL successfully, you must update the MySQL password provided to you during the MySQL installation. When prompted by the script with, "If you have not changed the MySQL root user password, you will not be able to continue. Would you like to change it now?", answer **yes** and follow the instructions closely if the temporary MySQL root password has not been updated, otherwise answer **no**. MySQL User Passwords must be:
>
> - At least 8 characters long
> - Contain at least 1 uppercase and 1 lower case letter
> - Contain at least 1 number
> - Contain at least 1 special character

Installing the ISR RSS

This section describes how to install the ISR RSS.

> **Note:**
>
> During the installation process, you will be asked to provide and/or verify the users, passwords, and interfaces you created during the Oracle Linux installation.

To install the ISR RSS:

1. Log into the Oracle Linux CLI using an SSH client.

> **Note:**
>
> The Oracle Linux CLI is case-sensitive.

2. Most ISR installation environments do not have access to a repository with the RPMs required to install the isr-rss package and the isr-rss RPM itself. The simplest way to manage this is to (secure) copy or FTP the following file onto the Index host:

   - isr-rss-<*release#*>.x86_64.rpm

   Once the file is properly copied, connect to the Index host with an SSH client and in the directory (for example, /tmp) containing the file, execute the following command:

   ```
   # sudo yum localinstall /tmp/isr-rss-<release#>.x86_64.rpm
   ```

3. Verify the installation when prompted.

   ```
   Is this ok [y/d/N]:Y
   ```

   The RSS application is installed.

4. To configure the RSS, enter the following:

   ```
   sudo /opt/isr/configIsr.sh
   ```

5. Follow the configIsr.sh script instructions closely.

Installing the ISR Dashboard

This section describes how to install the ISR Dashboard.

> **Note:**
>
> During the installation process, you will be asked to provide and/or verify the users, passwords, and interfaces you created during the Oracle Linux installation.

To install the ISR Dashboard:

1. Log into the Oracle Linux CLI using an SSH client.

> **Note:**
>
> The Oracle Linux CLI is case-sensitive.

2. Install Ruby by coping the Ruby RPM, `ruby-2.6.4-1.el7.centos.x86_64.rpm`, to your working directory (for example, `/tmp`) and executing the **yum localinstall** command. For example:

   ```
   sudo yum localinstall /tmp/ruby-2.6.4-1.el7.centos.x86_64.rpm
   ```

3. Most ISR installation environments do not have access to a repository with the RPMs required to install the ISR Dashboard. The simplest way to manage this issue is to (secure) copy or FTP the following file onto the Dashboard host:

   - isr-Dashboard-<*release#*>.x86_64.rpm

   Once the files are properly copied, connect to the Index host with an SSH client and in the directory (for example, /tmp) containing the files, execute the following command:

   ```
   # sudo yum localinstall /tmp/isr-Dashboard-<release#>.x86_64.rpm
   ```

4. Verify the installation when prompted.

   ```
   Is this ok [y/d/N]:Y
   ```

   The ISR Dashboard is installed.

5. Enter the following to configure the ISR Dashboard.

   ```
   sudo /opt/isr/configIsr.sh
   ```

6. Follow the script's instructions closely.

Configuring Recording Capacity

Recording capacity is configured via the ISR Dashboard. Navigate to **Admin**, **Sites**, **RSS** to add any RSS hosts, configure their **VoIP IP**, **Admin IP**, and **Data IP**, and set the Recorder capacity in the **Advanced Configurations - Session Capacity** field.

> **Note:**
>
> The **Sessions Capacity** value is the number of concurrent sessions allowed for this RSS host. This number must comply with your Oracle contract. For more information regarding your ISR software contract, contact your Oracle representative.

Configuring the Timezone on an ISR

The timezone of each ISR component has a default setting of America/New_York, also known as the Eastern Time Zone. To change the timezone on the ISR, the administrator must set all hosts to the timezone of choice and the RSS hosts must be set to the same timezone as all ISRs.

> **Note:**
>
> It is important that your ISR component hosts are assigned the same timezone, except the Index host, which must be set to UTC.

To configure the timezone of an ISR component:

1. Connect to the ISR component console with an SSH client.
2. Execute the **rm -f /etc/localtime** command to remove the previous timezone setting.
3. Execute the following command to link the updated timezone.

   ```
   ln -s    /usr/share/zoneinfo/<region>/<timezone> /etc/localtime
   ```

   Note: When you enter the /usr/share/zoneinfo/<region> and /usr/share/zoneinfo/<region>/<timezone> commands the CLI provides options for both the <region> and <timezone> arguments.

4

Post-Install Verification and Configuration

This section provides information and procedures for post-install verification and configuration. It includes verifying connectivity between the components and testing the call recording functionality of the ISR. It also includes required ISR configuration that must be performed before making the first call.

Verifying Connectivity Between the RSS and the Index

When installation of the RSS and Index are complete, you can test the connectivity between these components to verify they are working properly. Procedures in this section include:

- Testing connectivity between the RSS and Index
- Logging into the dashboard

Testing Connectivity

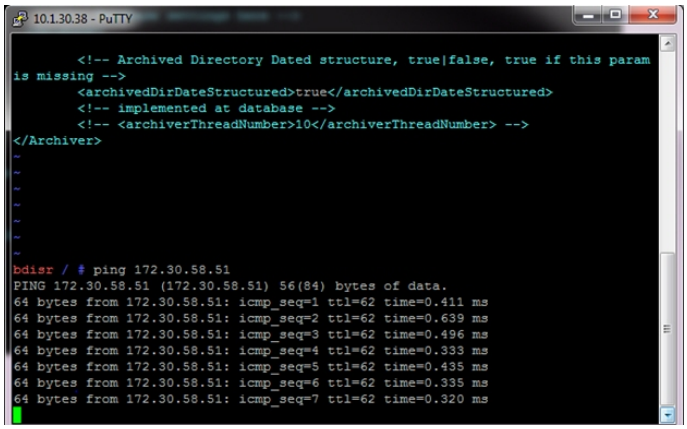
Use the following procedure to test connectivity between the RSS and Index VM.

To test connectivity:

1. Log in to the RSS host using an SSH client.
2. Enter **ping index_host_ip** and press Enter.

   ```
   hostname# ping <your_index_host_ip>
   ```

   The following is an example of the screen that displays.



You can complete the connectivity verification by logging into the dashboard using the procedures in, "Logging Into ISR Dashboard".

Logging Into ISR Dashboard

Use the following procedures to verify the administrator dashboard is working properly.

To log into the Dashboard:

1. Open your Internet Web browser.
2. Enter the IP address of the ISR Dashboard. For example:

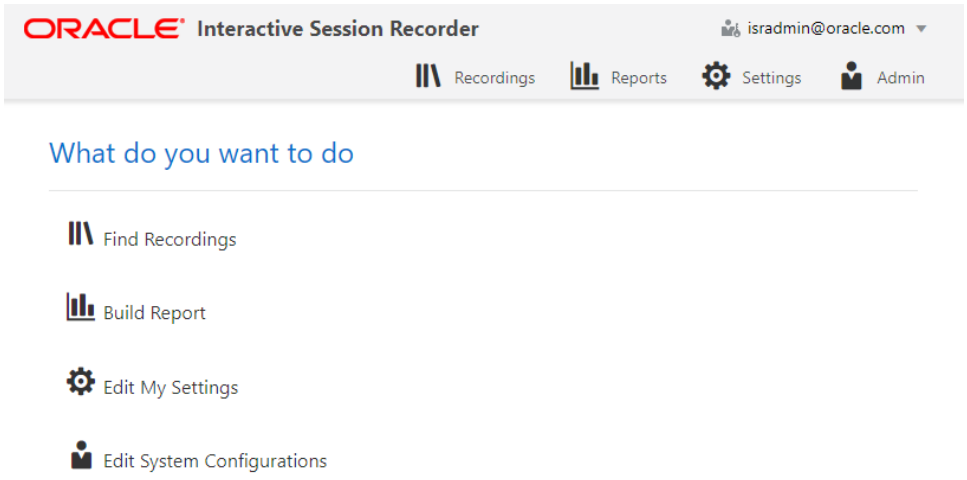
   ```
   https://172.54.66.7
   ```

   The initial Login page displays.
3. Enter your email and password respectively, in the **Email** and **Password** fields.

   The initial temporary user name and password are:
   User name: isradmin@acmepacket.com **Password**: admin123.

> **Note:**
>
> You are required to change the default email and password upon initial login and then the password again every 90 days.

4. After logging in, the following page displays.



Configuring the ISR for Recording a Call

You can place a call to verify that the ISR call recording functionality is working properly. Before you can place a call, you must configure the following on the ISR:

- Add a new site for the RSS server
- Add a new RSS to the site
- Add a Route

Add Site for RSS Server

To verify that the RSS and the dashboard are communicating, you must add a new site for the RSS server. Use the following procedure to add a new site.

To add a site:

1. From the Main Menu, click **Admin**.
2. Click **Sites**.
3. Click **Create**.
4. **Name**—Enter a name for the Site and click **Create**. The new site displays on the Sites page.

   For more information about creating Sites, see the *Oracle Communications Interactive Session Recorder Administrator Guide*.

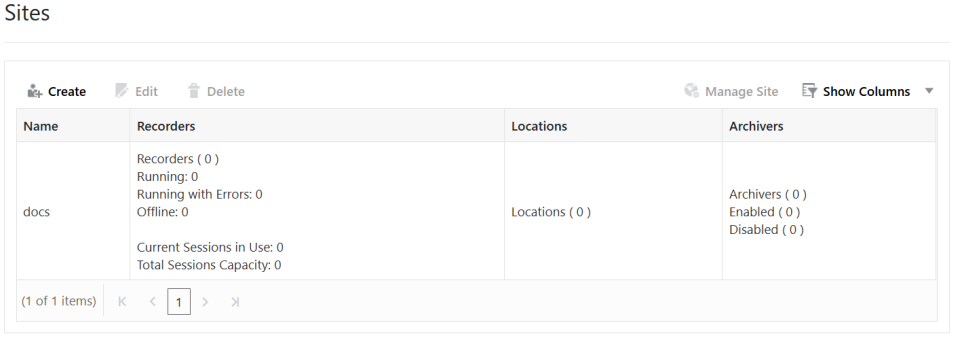
Add the RSS to a Site

To enable connectivity between the RSS and the Index, you must add the new RSS to a site. Use the following procedure to add the new RSS.

To add the new RSS to the site:

1. From the Admin page, click **Sites**.

   The Sites page appears.

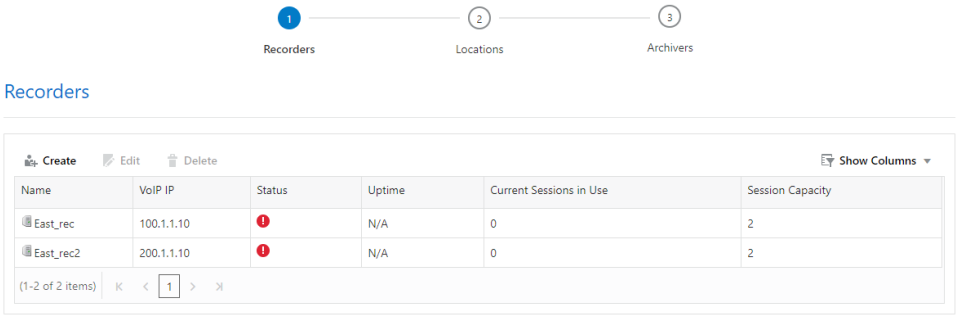


   The Sites page displays the following:

Field	Description
Name	The name of the site.
Recorders	Provides information about the Site's Recorders including the number or recorders, their status, current sessions in use, and total sessions capacity.
Locations	Provides the number of Locations associated with this Site.
Archivers	Provides information about the Site's Archivers, including the number of Archivers and their status.

2. Select a site for which you want to add the RSS, and click **Manage Site**.

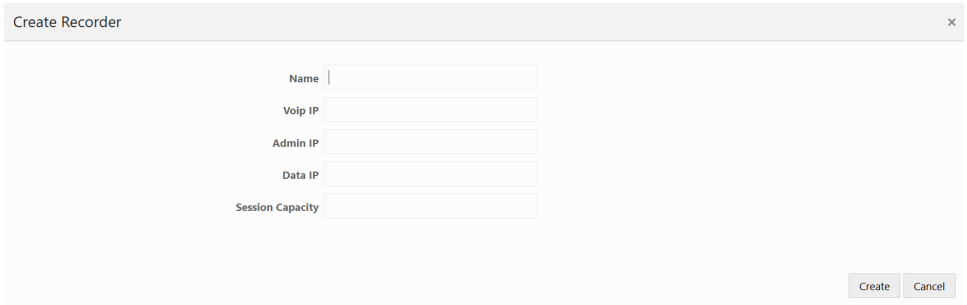
   The following page displays.



The Recorders page displays the following about each RSS.

Column	Description
Name	Name of the RSS.
VoIP IP	IP Address of the VoIP interface of the RSS.
Status	Current status of the RSS . Status can be: Enabled (active) Disabled (inactive) Active with errors
Uptime	Time elapsed since the last RSS process restart.
Current Sessions in Use	Total number of licensed sessions currently being used on the RSS.
Sessions Capacity	Total number of licensed sessions on the RSS.

3. Click **Create**. The Create Recorder page displays.



4. In the **Name** field, enter a name for the RSS you are adding.
5. In the **VoIP IP** field, enter the IP address (in dotted decimal format) on which the RSS is listening for SIP traffic.
6. In the **Admin IP** field, enter the IP address at which to connect to the RSS host over the Administrator network.

7. In the **Data IP** field, enter the IP address at which ISR components communicate with the RSS host over the Data network.
8. In the **Sessions Capacity** field, enter the value of the number of concurrent sessions allowed for this RSS host.

> **Note:**
>
> This number must comply with your Oracle license agreement.

9. Click **Create**.

   For additional information about RSS, see the *Interactive Session Recorder Administrator Guide*.

5
Setting up a Test Call

This chapter provides information and procedures for configuring the first route to use for placing a test call to the ISR. It also includes information for setting up a Softphone for making the first call procedures for verifying that the recording was made and that the Dashboard works properly.

Configuring a Route

Route configuration is important to the flexibility of your ISR installation. A route defines the parameters to evaluate and invoke recording, as well as the recording rules to apply for all calls received by the ISR. Users are given access to recordings based on routes.

Use the following test procedure to make your first recording. This procedure uses a wildcard route that applies the same recording rules to every call received. Please note that this is not the recommended configuration to deploy in a production system, as it eliminates the ability to assign users access to specific recordings.

> **Note:**
>
> Use the new Route you configure in this section for call verification purposes only.

To configure a route:

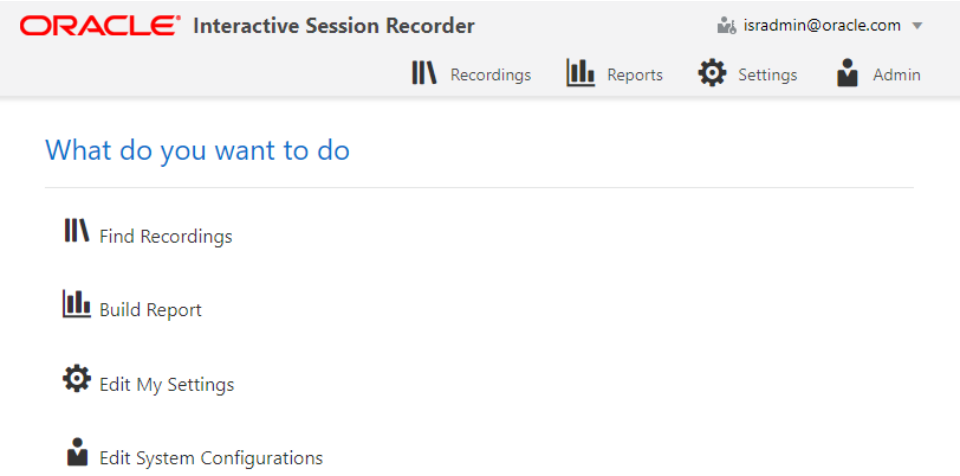
1. Open your Internet Web browser.
2. Enter the IP address of the ISR. For example:

   ```
   https://172.54.66.7
   ```

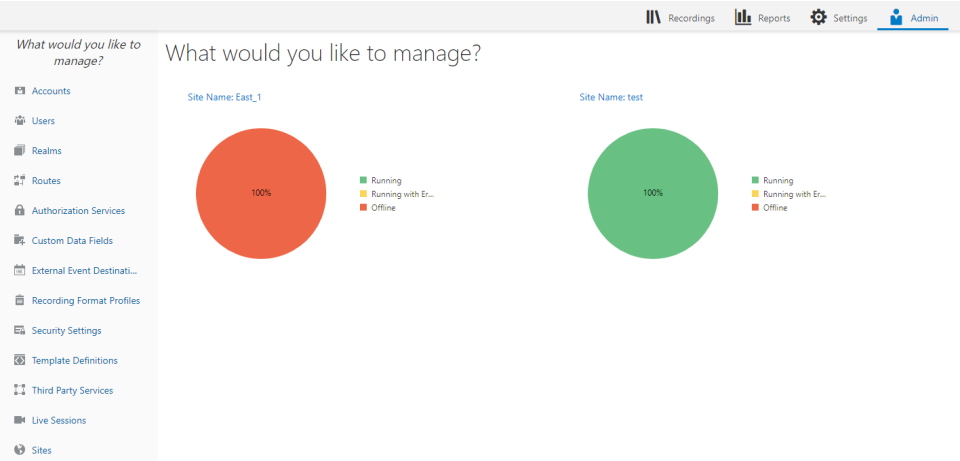
   The Login page displays.
3. Enter your credentials in the **Email** and **Password** fields.

   Note: Upon initial login, you are required to change the email and password login credentials, and then you must update the password again every 90 days.

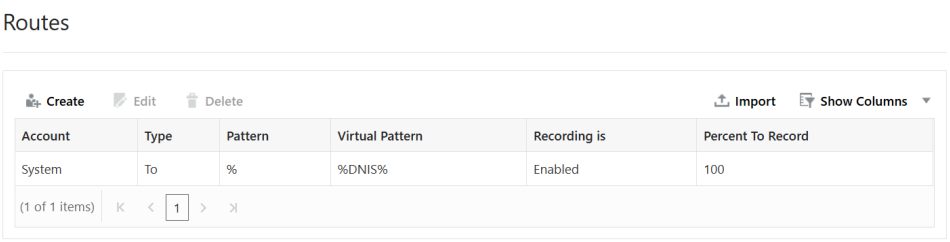
   The following page displays.



4. From the Main Menu, click **Admin**. The following page displays.



5. Click the **Routes** . The following page displays.



The Route page displays the following about each Route.

Column	Description
Account	Name of the Account assigned to the current route.
Type	Type of route associated with this account (DNIS - To, ANI - From, or Both - To/From)
Pattern	Pattern that is matched in the incoming INVITE.

Column	Description
Virtual Pattern	Not supported.
Recording is	Specifies whether or not recording is enabled on this account/route.
Percent to Record	Indicates the percentage of calls currently being recorded on this account/route.

This route can also be used to test SIPREC traffic without any changes.

Setting Up a Softphone

In order to make calls to the RSS, you must have phone hardware or a softphone. If you have phone hardware with a configured route to the ISR, you can skip the procedure in this section and go directly to the procedure Verifying Call Recording/Playback Using the Dashboard to verify connectivity to the RSS.

A softphone is software that allows you to talk using VoIP without having a physical phone set. It acts as an interface allowing you to dial numbers and carry out other phone functions using your computer screen and your mouse, keyboard or keypad.

If you would like to make a call to the RSS using a softphone, use the procedures in this section to install a SIP Softphone onto your computer. You can use any SIP Softphone application that supports G.711a/u. The following example installs the PhonerLite SIP Softphone application.

Installing the Softphone

Use the following procedure to install the Softphone.

To install the softphone:

> **Note:**
>
> You must install the Softphone onto a computer with network access to the RSS server and the computer must have audio input/output (microphone/speakers).

1. Open a Web browser and enter the following URL in the URL field to access the download page for the PhonerLite application: http://www.phonerlite.de/download_en.htm
2. Click on the PhonerLiteSetup.exe file in the download box to download the application to your PC.
3. Double-click the application and follow the instructions to install PhonerLite to your PC.

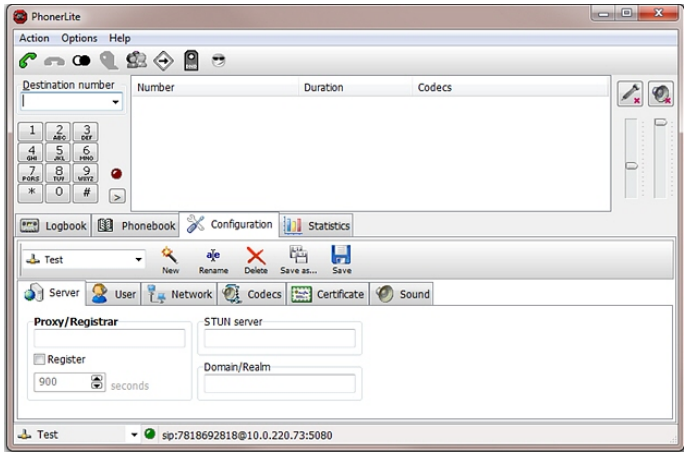
Configuring the Softphone

Use the following procedure to configure the Softphone.

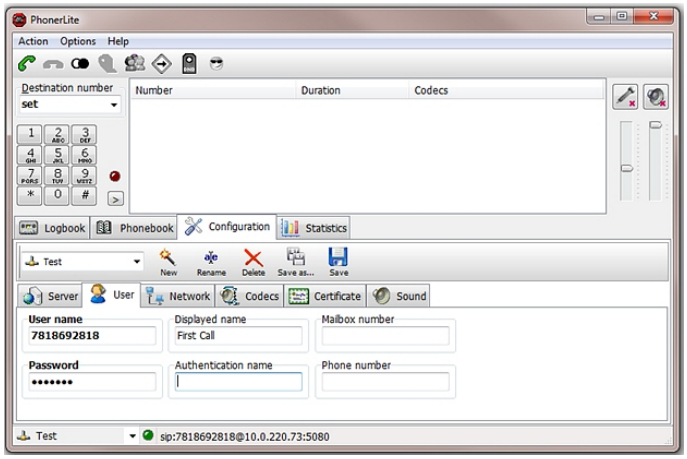
To configure the softphone:

1. When PhonerLite is installed, double-click the PhonerLite icon on your desktop to open the application.

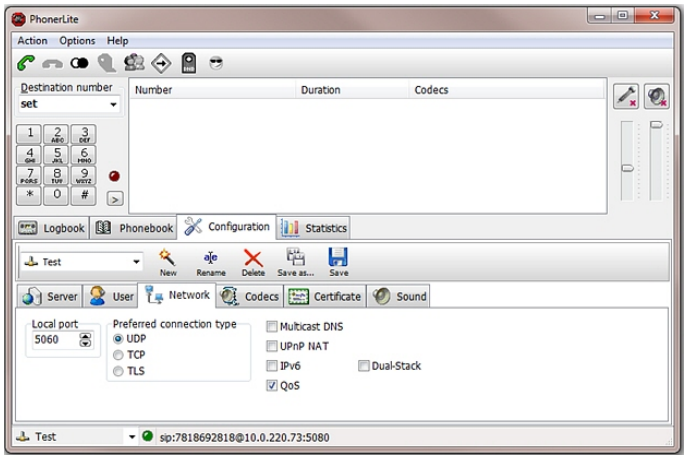
2. In the PhonerLite window, click the Configuration tab.
3. Click the Server tab.



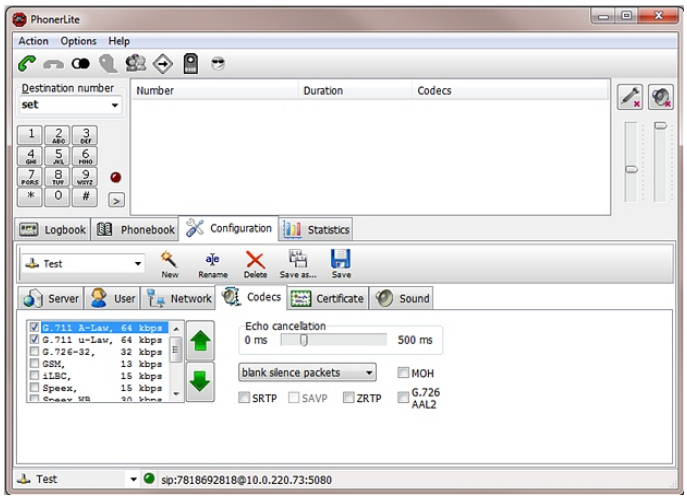
4. Verify that the Register box is disabled (unchecked).
5. Click the User tab.



6. In the User name box, enter your user name. Your user name is your outgoing caller ID (SIP URI).
7. In the Displayed name box, enter a name to display to the recipient of a call. Valid values are alpha-numerical characters.
8. Click on the Network tab.



9. In the Local Port box, enter the value for an open port on your computer. Default SIP port is **5060**. This port value should be available if you have no other SIP devices running on your computer.
10. In the Preferred connection type field, click **UDP** to enable it. The RSS requires the UDP transport protocol. All other network parameters can remain at default values.
11. Click the Codecs tab.



12. In the codec list, select "**G.711 A-Law, 64 kbps**" and/or G.711 u-Law, 64 kbps. At least one of these codecs must be selected.
13. In the drop-down box, select blank silence packets.
14. Click the <**Save**> icon. Do not close this Softphone application as you will be using it to make your first call. Go to Making the First Call to make the first test call to the RSS.

Making the First Call

After installing the Softphone Client, you can use it to place your first call to the RSS. Initiating a session directly with the RSS is purely for testing purposes, and production use of ISR requires SIPREC and includes an SBC or similar Session Recording Client (SRC) application.

Before You Begin

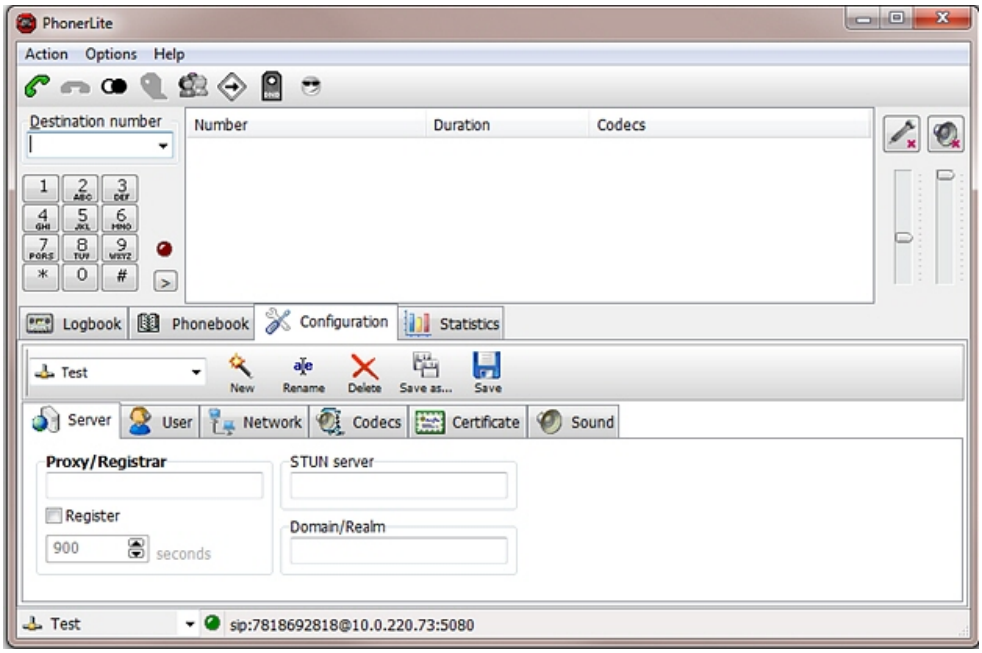
Before you make your first call to the RSS, open the /opt/isr/logs/recorder/recorder.log file to observe the cache refresh and see your test call display in the log as it happens.

To open the ISR.log file:

1. Enter tail -f /opt/isr/logs/recorder/recorder.log and press Enter.

```
<hostname> # tail -f /opt/isr/logs/recorder/recorder.log
```

2. In your Softphone client (PhonerLite), enter a test phone number in the "**Destination Number**" field. The destination number must be a full SIP URI of the format sip:<User>@<your_rss_ip>. The following window uses an example destination number of sip:test@10.1.30.38.



3. Click the telephone iicon  icon in the Main Menu or Press Enter.

   The output in the /opt/isr/logs/recorder/recorder.log displayed in your RSS tail should look similar to the following:

```
08/30/2011 07:31:54[ INFO] sipProxy: (SIP INVITE received - new
call!!! [cid = 1, did = 2])
08/30/2011 07:31:54[ INFO] sipProxy: [Channel 1] Looking up call w/
ANI: 7818692818 DNIS: test
08/30/2011 07:31:54[ INFO]callManager: [Channel 1] Enqueueing
SipCall, callId: 800D645C-5CD2-E011-9026-F0DEF154AD05@10.1.30.38
08/30/2011 07:31:54[ INFO]callManager: [Channel 1] Dequeueing
SipCall, callId: 800D645C-5CD2-E011-9026-
F0DEF154AD05@10.221.100.147, queueSize: 1
08/30/2011 07:31:54[ INFO]callManager: [Channel 1] Looking up call
w/ ANI: 7818692818 DNIS: test
```

```
08/30/2011 07:31:54[ INFO] RouteMap: Call route with ANI:7818692818 DNIS:
test returned CALL_TYPE_CONFERENCE accountName: System
08/30/2011 07:31:54[ INFO] RouteMap: [Channel 1] getRouteInfo returned
with vDNIS: test, isRecordable: true
08/30/2011 07:31:54[ INFO]xmlRpcQueryAgent: XmlRpcQueryAgent::execute:
method addDirectVmgEntry (_connectionState 0).
08/30/2011 07:31:54[ INFO]xmlRpcQueryAgent: XmlRpcQueryAgent::execute:
method addDirectVmgEntry completed.
08/30/2011 07:31:54[ INFO]callManager: [Channel 1] addDirectVmgEntry
return with ACK.
08/30/2011 07:31:54[ INFO]callManager: [Channel 1] addDirectVmgEntry is
successful with ANI: 7818692818 DNIS: test channelId 1
08/30/2011 07:31:54[ INFO]callManager: [Channel 1] routeId 1 adjusted
limit is 24, adjusted burst ports is 6, acct limit is 100, acct burst
port is -1.
08/30/2011 07:31:54[ INFO]callManager: [Channel 1] Current route (1)
usage: 1, account (1) usage: 1.
08/30/2011 07:31:54[ INFO] sipProxy: [Channel 1] Call State Transition:
Idle -> Called
08/30/2011 07:31:54[ INFO] sipProxy: [Channel 1] Got rtp port 22000 for
Caller->Mixer RTP Stream.
08/30/2011 07:31:54[ INFO] sipProxy: [Channel 1] Got RTP Port 22002 for
3Party->Mixer RTP Stream.
```

4. When the RSS answers the call, leave a voice recording.
5. Click  to hang up the phone.
6. Verify that no errors appear in the recorder.log file on your RSS tail output. Go to Verifying Call Recording/Playback Using the Dashboard to verify the call recording was successful.

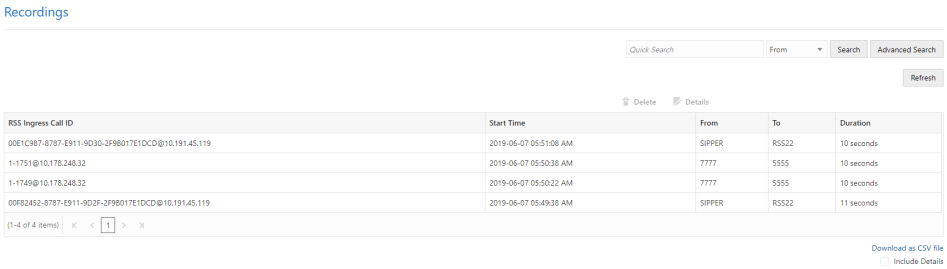
Verifying Call Recording/Playback Using the Dashboard

After making a call with your phone equipment or softphone, you can verify that the call recording was successful by playing back the call using the ISR Dashboard. Use this procedure to verify that the RSS has stored your recording.

> **Note:**
>
> Before playing recordings, ensure your browser has a default media application that plays audio files with a .wav format and that your speaker/microphone is turned ON. For more information about the software requirements and recommendations for playing recordings, see ISR Dashboard Requirements.

To verify the call recording/playback:

- From the Main Menu, click **Recordings**. The following page displays.



This page displays the test recording you just made on the first call to the RSS.

Click on the recording entry to bring up the Recording Details page. This displays details about the recorded session and its recorded segment(s) and allows you to select the Play icon at the top of the Segment 1 tab to play the recording from the details page.

If the recording does not appear in the dashboard, review the RSS recorder.log.

If the recording appears in the Dashboard but does not play, ensure your media application is installed. Dashboard logging can be found on the Dashboard VM in /opt/isr/logs/dashboard/production.log.

6
Deploying and Configuring ISR FACE API

Deploying ISR FACE API

The ISR FACE API is deployed the same way as the other ISR components. The ISR FACE API is commonly deployed on an Oracle Linux 7 VM and has the same prerequisites as the other ISR components, described in "Installation Prerequisites".

Installing ISR FACE API

By default, FACE API is configured to handle HTTP requests over SSL, but you must perform the following steps to complete the initial configuration.

> **Note:**
>
> During the installation process, you will be asked to provide and/or verify the users, passwords, and interfaces you created during the Oracle Linux installation.

To install the ISR FACE API:

1. Log into the Oracle Linux CLI using an SSH client.

   > **Note:**
   >
   > The Oracle Linux CLI is case-sensitive.

2. Enter the following command into the CLI:

   ```
   sudo yum install isr-Face
   ```

> **Note:**
>
> Most ISR installation environments do not have access to a repository with the RPM required to install the isr-Face RPM itself. The simplest way to manage this issue is to (secure) copy the following file onto the Index host:
>
> - isr-Face-<release#>.x86_64.rpm
>
> Once the file is properly copied, connect to the Index host with an SSH client and in the directory (for example, /tmp) containing the file, execute the following command:
>
> ```
> # sudo yum localinstall /tmp/isr-Face-<release#>.x86_64.rpm
> ```

3. Verify the installation when prompted.

   ```
   Is this ok [y/d/N]:Y
   ```

   Oracle Linux downloads the FACE API installation packages.

4. Enter the following command into the CLI once Oracle Linux indicates the installation packages have finished downloading.

   ```
   sudo /opt/isr/configIsr.sh
   ```

5. Follow the script's instructions closely.

Configuring FACE API Reduced Security

The ISR's FACE API functionality may be run with reduced security. You can use the configIsr.sh script to loosen security settings on the FACE API host.

- To disable HTTPS in FACE API, run the configCis.sh script and select HTTP for FACE API.

  ```
  [root@face ~]# configIsr.sh
  ----------------------------------------
  Please select from the following menu:
  ----------------------------------------

  s) Show the current configuration
  m) Modify the current configuration
  i) Add/modify a second network interface
  f) Set FACE default configuration in DB
  q) Quit

  Choice: f

  WARNING, this action will reset the FACE to its default
  configuration.
    ** All customization of FACE configured will be lost.
  ```

```
Continue? (yes|no) [yes] yes
You have been warned.

Enter Face Host IP: [] 1.2.3.4
Protocol to use for FACE connections? (http|https) [https] http

FACE connection protocol set to http
Enter ObserveIT Server IP: [] 2.3.4.5
Protocol to use for ObserveIT Server connections? (http|https) [https]
ObserveIT connection protocol set to https
Attempting to restore backup SQL
Backing up FACE Config (to /opt/isr/faceSetupTemplate.sql.bak).
Updating FACE IP in SQL Script.
Updating FACE HTTP/S in SQL Script.
Updating ObserveIT IP in SQL Script.
```

7

Upgrading the ISR

The ISR includes a "yum-style" approach to upgrading all ISR applications on each ISR component host. The upgrade feature is limited to upgrades within the 5.2Mx and later release sets. Upgrading from release 5.1 or earlier is not currently automated. Contact your Oracle representative for more information.

You must upgrade the ISR components in the following order:

- Index
- RSS
- Dashboard
- FACE API (if present)

Upgrade Prerequisites

To upgrade the ISR components, you must complete the following prerequisites:

1. The ISR component hosts are properly running on the Oracle Linux Release 7.2 - 7.7 OS
2. Access to the following upgrade tar files from the ISR component hosts:
   - isr-Index-<*release#*>-upgrade.tgz
   - isr-Dashboard-<*release#*>-upgrade.tgz
   - isr-rss-<*release#*>-upgrade.tgz
   - isr-Face-<*release#*>-upgrade.tgz
3. Have access to the Ruby 2.6 rpm (ruby-2.6.4-1.el7.centos.x86_64.rpm).
4. For the duration of the maintenance window, all call traffic is stopped on all sites and outside client access to the Dashboard and API services is prohibited.

> **Note:**
>
> When you install RSS and FACE, the ISR picks up the latest available tomcat version from the OL 7 repository.

The following instructions assume the recommended "isradm" Linux user has sudo permissions.

WARNING: The upgrade process for each component includes a critical backup step that copies important host configuration, ISR application configuration, ISR application platform configuration, ISR application data, encrypted keys, keystores, and log files to a temporary directory before consolidating these copies into a compressed set of files for a potential rollback situation. This backup step requires additional disk space to successfully write the files, and a warning prompt is displayed to detail concerns and recommend an option to mount an additional drive if disk space may be an issue. Oracle strongly recommends you

consider these details and the recommended option carefully before continuing with the upgrade. For more information about mounting remote storage, see Chapter 22, Shared File System Administration from the Oracle Linux Administrators Guide Release 7.

Upgrading the ISR Index

This section describes the ISR Index upgrade process.

> **Note:**
>
> The following examples use <release#> as a placeholder for the appropriate file name you are upgrading to.

1. Log into the Index host using the recommended "isradm" user.
2. Copy the Index upgrade file "isr-Index-<*release*#>-upgrade.tgz into the `/opt/isr/releases` directory.
3. Switch to the `root` directory by executing the **cd /** command.
4. Delete prior ISR RPM packages to avoid confusion with the current version by executing the following command:

   ```
   $ sudo rm /opt/isr/releases/isr-*.rpm
   ```

5. Unpack the upgrade file from the `root` directory by executing the following command:

   ```
   sudo tar xzf /opt/isr/releases/isr-Index-<release #>-upgrade.tgz -
   C /
   ```

6. Run the upgrade script by executing the following command:

   ```
   sudo /opt/isr/releases/upgradeIsr.sh
   ```

7. Follow the script's prompts and instructions closely.
8. Verify the updated build upon completion by executing the following command.

   ```
   yum info isr-Index
   ```

   If the upgrade is successful, the following information displays:

   ```
   Repo        : installed
   Summary     : <release#> <build_date>        Index for ISR
   ```

Upgrading the ISR RSS

This section describes the ISR RSS upgrade process.

> **Note:**
>
> The following examples use <release#> as a placeholder for the appropriate file name you are upgrading to.

1. Log into the RSS host using the recommended "isradm" user.
2. Copy the RSS upgrade file "isr-rss-<*release#*>-upgrade.tgz into the `/opt/isr/releases` directory.
3. Switch to the `root` directory by executing the **cd /** command.
4. Delete prior ISR RPM packages to avoid confusion with the current version by executing the following command:

   ```
   $ sudo rm /opt/isr/releases/isr-*.rpm
   ```

5. Unpack the upgrade file from the `root` directory by executing the following command:

   ```
   sudo tar xzf /opt/isr/releases/isr-rss-<release #>-upgrade.tgz -C /
   ```

6. Run the upgrade script by executing the following command:

   ```
   sudo /opt/isr/releases/upgradeIsr.sh
   ```

7. Follow the script's prompts and instructions closely.
8. Verify the updated build upon completion by executing the following command.

   ```
   yum info isr-rss
   ```

   If the upgrade is successful, the following information displays.

   ```
   Repo        : installed
   Summary     : 6.0 20161234-567890        RSS for ISR
   ```

9. Run the configuration script by executing the following command:

   ```
   sudo /opt/isr/configIsr.sh
   ```

10. Follow any configuration script's prompts and instructions closely to ensure all component configurations are verified and select the **q** option to finish.

Upgrading the ISR Dashboard

This section describes the ISR Dashboard upgrade process.

> **Note:**
>
> The following examples use <release#> as a placeholder for the appropriate file name you are upgrading to.

1. Log into the Dashboard host using the recommended "isradm" user.
2. Copy the Dashboard upgrade file "isr-Dashboard-<*release#*>-upgrade.tgz into the `/opt/isr/releases` directory.
3. Copy the Ruby 2.6 RPM to the /opt/isr/releases directory. You can download the Ruby 2.6 RPM package, ruby-2.6.4-1.el7.centos.x86_64.rpm, using the https://github.com/feedforce/ruby-rpm/releases/tag/2.6.4 link.
4. Switch to the `root` directory by executing the **cd /** command.
5. Delete prior ISR RPM packages to avoid confusion with the current version by executing the following command:

   ```
   $ sudo rm /opt/isr/releases/isr-*.rpm
   ```

6. Unpack the upgrade file from the `root` directory by executing the following command:

   ```
   sudo tar xzf /opt/isr/releases/isr-Dashboard-<release #>-
   upgrade.tgz -C /
   ```

7. Run the upgrade script by executing the following command:

   ```
   sudo /opt/isr/releases/upgradeIsr.sh
   ```

8. Follow the script's prompts and instructions closely.
9. Verify the updated build upon completion by executing the following command.

   ```
   yum info isr-Dashboard
   ```

   If the upgrade is successful, the following information displays:

   ```
   Repo        : installed
   Summary     : <release#> <build_date>        Dashboard for ISR
   ```

10. Run the configuration script with the following command:

    ```
    sudo /opt/isr/configIsr.sh
    ```

11. Follow the configuration script's prompts and instructions closely to import public keys from all RSS hosts.

> **Note:**
>
> For the Recorder and Converter processes to update their configurations and record successfully after upgrading from 5.2 to 6.x, you must log into the Dashboard, access the **Admin**, **Sites**, **Recorders** page, and edit each Recorder, updating their network IPs, Sessions Capacity, Primary and Failover Locations, and confirm the remaining configuration settings. The Primary Location may already be set. Typically, the Failover Location is configured to the Destination Location set for the Archival process for this Recorder.

Upgrading the ISR FACE API

This section describes the ISR FACE API upgrade process.

> **Note:**
>
> The following examples use <release#> as a placeholder for the appropriate file name you are upgrading to.

1. Log into the FACE API host using the recommended "isradm" user.
2. Copy the FACE API upgrade file "isr-Face-<*release#*>-upgrade.tgz into the `/opt/isr/releases` directory.
3. Switch to the `root` directory by executing the **cd /** command.
4. Delete prior ISR RPM packages to avoid confusion with the current version by executing the following command:

   ```
   $ sudo rm /opt/isr/releases/isr-*.rpm
   ```

5. Unpack the upgrade file from the `root` directory by executing the following command:

   ```
   sudo tar xzf /opt/isr/releases/isr-Face-<release #>-upgrade.tgz -C /
   ```

6. Run the upgrade script by executing the following command:

   ```
   sudo /opt/isr/releases/upgradeIsr.sh
   ```

7. Follow the script's prompts and instructions closely.
8. Verify the updated build upon completion by executing the following command.

   ```
   yum info isr-Face
   ```

   If the upgrade is successful, the following information displays:

   ```
   Repo        : installed
   Summary     : <release#> <build_date>        Face for ISR
   ```

9. Run the configuration script with the following command:

   ```
   sudo /opt/isr/configIsr.sh
   ```

10. Follow the configuration script's prompts and instructions closely to import public keys from all RSS hosts.

A

Oracle Public Yum Repository Configuration and Offline Installation Pre-Requisites

The repositories specified in the `/etc/yum.repos.d/public-yum-ol7.repo` file, usually found by default in Oracle Linux 7, must be accessible during ISR software installations. The repository entries are the following:

```
[ol7_latest]
name=Oracle Linux $releasever Latest ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/latest/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=1


[ol7_u0_base]
name=Oracle Linux $releasever GA installation media copy ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/0/base/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0


[ol7_u1_base]
name=Oracle Linux $releasever Update 1 installation media copy ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/1/base/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0


[ol7_u2_base]
name=Oracle Linux $releasever Update 2 installation media copy ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/2/base/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0


[ol7_UEKR3]
name=Latest Unbreakable Enterprise Kernel Release 3 for Oracle
Linux $releasever ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/UEKR3/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
```

```
gpgcheck=1
enabled=1


[ol7_optional_latest]
name=Oracle Linux $releasever Optional Latest ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/optional/
latest/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0


[ol7_addons]
name=Oracle Linux $releasever Add ons ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/
addons/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0


[ol7_UEKR3_OFED20]
name=OFED supporting tool packages for Unbreakable Enterprise Kernel
on Oracle Linux 7 ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/
UEKR3_OFED20/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
priority=20


[ol7_MySQL56]
name=MySQL 5.6 for Oracle Linux 7 ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/
MySQL56/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0


[ol7_MySQL55]
name=MySQL 5.5 for Oracle Linux 7 ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/
MySQL55/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0


[ol7_spacewalk22_client]
name=Spacewalk Client 2.2 for Oracle Linux 7 ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/spacewalk22/
client/$basearch/
```

```
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
```

Third-Party Dependencies for Offline Installation

ISR expects internet access to allow yum access to install all dependent third-party packages. For installations that do not have internet access, a local repository of dependent packages can be created.

> **Note:**
>
> ISR components are installed on Oracle Linux Server 7.7.

The following is a list of packages the ISR expects to be installed for a proper, fully-functional installation.

Dashboard

- ruby-0:2.6.4-1.el7.centos.x86_64
- zlib-devel-0:1.2.7-13.el7.x86_64
- bash-0:4.2.46-12.el7.x86_64
- java-1.8.0-openjdk-1:1.8.0.242.b08-0.el7_7.x86_64
- gcc-0:4.8.5-39.0.3.el7.x86_64
- patch-0:2.7.1-12.el7_7.x86_64
- openssl-devel-1:1.0.2k-19.0.1.el7.x86_64
- gcc-c++-0:4.8.5-39.0.3.el7.x86_64
- libxml2-0:2.9.1-6.0.1.el7_2.3.x86_64

FACE

- tomcat-7.0.76-15.el7.noarch (Latest available from OL 7 yum repo)
- bash-0:4.2.46-33.el7.x86_64
- java-1.8.0-openjdk-1:1.8.0.242.b08-0.el7_7.x86_64

Index

- bash-0:4.2.46-33.el7.x86_64

RSS

- bzip2-libs-0:1.0.6-13.el7.x86_64
- c-ares-0:1.10.0-3.el7.x86_64
- java-1.8.0-openjdk-1:1.8.0.242.b08-0.el7_7.x86_64
- libgcc-0:4.8.5-39.0.1.el7.x86_64
- bash-0:4.2.46-33.el7.x86_64

- libstdc++-0:4.8.5-39.0.1.el7.x86_64
- zlib-0:1.2.7-18.el7.x86_64
- glibc-0:2.17-292.0.1.el7.x86_64
- tomcat-7.0.76-15.el7.noarch (Latest available from OL 7 yum repo)
- openssl-libs-1:1.0.2k-19.0.1.el7.x86_64

To verify the required components for your installation version, run the following command on each ISR host:

```
$ repoquery --requires --resolve isr-<component>
```

where component is either Dashboard, FACE, Index, or RSS.

Distributed MySQL RPMs

Each component host includes the following MySQL dependencies in the ISR distribution:

- Dashboard
  - mysql-commercial-common.x86_64
  - mysql-commercial-devel.x86_64
  - mysql-commercial-libs.x86_64
  - mysql-commercial-libs-compat.x86_64
- FACE
  - mysql-commercial-client.x86_64
  - mysql-commercial-common.x86_64
  - mysql-commercial-libs.x86_64
  - mysql-commercial-libs-compat.x86_64
- Index
  - mysql-commercial-client.x86_64
  - mysql-commercial-common.x86_64
  - mysql-commercial-libs.x86_64
  - mysql-commercial-libs-compat.x86_64
  - mysql-commercial-server.x86_64
- RSS
  - mysql-commercial-client.x86_64
  - mysql-commercial-common.x86_64
  - mysql-commercial-libs.x86_64
  - mysql-commercial-libs-compat.x86_64

In certain instances the Linux host may contain MySQL packages that are not appropriate for ISR applications and therefore must be uninstalled (for example, yum

removed, for proper ISR component installations). The currently deployed packages can be displayed using the **yum list installed mysql** command.

Configuring ISR Recordings For Encryption Using Third-Party Software

The ISR supports encryption capabilities, as well as restriction of access to recording files, using the Oracle ZFS Storage Appliance.

For information on mounting the ISRto a NFS, see "Configuring an NFS Share For Archival".

For more information on the Oracle ZFS Storage Appliance and instructions on how to configure this functionality, see https://docs.oracle.com/cd/E27998_01/html/E48433/.

B

Public Cloud Platforms

The Oracle Communications Interactive Session Recorder (ISR) may be run on certain public cloud platforms. The following platforms are currently supported

- OCI
- Azure
- AWS

> **Note:**
>
> Refer to the ISR Release Notes to confirm the public clouds supported and important detail on that software version's support.

This section addresses requirements associated with running the ISR as public cloud instances. It also provides basic instructions on deploying machine instances.

Public Cloud providers maintain extensive product documentation. You must use those vendors' documentation for specifications, requirements, caveats, known issues, deployment details, and operation detail prior to deploying the **ISR**.

Create and Deploy ISR on OCI

You can deploy all nodes of Oracle Communications Interactive Session Recorder (ISR) on Oracle Cloud Infrastructure (OCI) .When deployed on this platform, you configure and operate the ISR as you would on any other platform. You can deploy the ISR to use the environment's IP infrastructure, including the private and public addressing scheme.

Before installing ISR components, SSH keys must be generated to access the ISR VM instances.

For more information, see https://docs.oracle.com/en/cloud/paas/event-hub-cloud/admin-guide/generate-ssh-key-pair-using-puttygen.html.

Prerequisites to Deploying an OCI Instance

The Oracle Cloud Infrastructure (OCI) deployment infrastructure provides a flexible management system that allows you to create objects required during the instance deployment procedure prior to or during that deployment. When created prior to deployment, these objects become selectable, typically from drop-down lists in the appropriate deployment dialogs. You may use these objects for a single deployment or for multiple deployments.

Deployment prerequisites tasks:

- Identify and deploy to the correct OCI Region. This is typically a default component of your OCI Account.

- Identify and deploy to the correct OCI Availability Domain
- Identify and deploy to the correct OCI Fault Domain
- Create an Oracle Virtual Cloud Network (VCN). Required VCN configuration includes:
  - Security list—These access control lists provide traffic control at the packet level.
  - Subnet configuration—The ISR has 4 types of interfaces: Admin, Local, VoIP, and Data. To maintain traffic separation, each of the vNICs should be connected to a separate subnet within the VCN.
  - Internet Gateway—Create a default internet gateway for the compartment and give it an appropriate name.
  - Route table (Use Default)—Create a route table to route appropriate Subnet(s) through the Internet Gateway.
- Security Groups—Security lists specify the type of traffic allowed on a particular type of subnet. Rules set on security lists can be either stateful or stateless. Stateful rules employ connection tracking and have the benefit of not requiring exit rules. However, there is a limit to the number of connections allowed over stateful connections and there is a performance hit. Oracle, therefore, recommends stateless lists for media interfaces.
  The security list for management ports can be stateful. Ports you should consider opening for management interfaces include:
  - SSH—TCP port 22
  - NTP—UDP port 123

  The security list for media ports should be stateless. Ports you should consider opening for VoIP/media interfaces include:
  - SIP—UDP or TCP port 5060
  - SIP TLS—TCP port 5061

  You can add rules to allow inter-component traffic for VoIP, data, admin interfaces. For more information about specific ports to be allowed, see the *ISR Security Guide*.
- Create Networks and Subnet—OCI interface types include those hidden from the internet and those that are not. Oracle recommends creating regional subnets, which means the subnet can span across availability domains within the region. Refer to OCI's Regional Subnets documentation for further information about using these objects.

Deploying the OCI Instance

The OCI instance configuration procedure includes a multi-dialog wizard that presents configuration options in the preferred sequence. The ISR has four components to be installed: Index, RSS, Dashboard, and FACE.

1. Create a VM instance by logging into the OCI console and selecting the appropriate region.
2. Click **Create a VM instance**. The Create Computer Instance page appears.
3. Enter appropriate information in the following fields:
   - **Name your instance**—Provide a component name

- **Choose an operating system**—Select Oracle Linux 7.x from Platform image
- **Availability Domain**—Select the domain to use
- **Instance Type**—Select Virtual Machine
- **Instance Shape**—Select either **VM.Standard.E2.4** (8 CPUs, 32 GB memory, 4 VNICs) or **VM.Standard2.4** (8 CPUs, 60 GB memory, 4 VNICs)
- **Virtual cloud network compartment**—Select a virtual cloud network compartment
- **Virtual cloud network**—Select a virtual cloud network
- **Subnet compartment**—Select a subnet compartment
- **Subnet**—Select a subnet and choose **Assign a public IP address**.
- **Boot volume**—Leave as the default value.

4. In the **Show Advanced Options**, **Management** tab, enter appropriate information in the following fields: (Leave Networking, Image, and Host tabs as default values)
   - **Choose a compartment for your instance**—Select a compartment for your instance
   - **Choose a fault domain**—Select a fault domain
5. Click **Create** to create the instance. The public and private IP of the instance displays.
6. **Selecting Networks and Subnets**—Use the following steps to select your networks and subnets. The minium ISR deployment typically has four interfaces.
   - Navigate to **Computer**, **Instances**, and open your instance.
   - Click **Stop** to stop your instance. The infrastructure cannot add interfaces to an instance when it is running.
   - Scroll down to the Attached VNICs section of the instance dialog and click **Create VNIC**. The Create VNIC dialog box appears.
   - Name your VNICs and select the subnets you created for them in the Create VNIC dialog box.
   - Click the **Start** button to restart your instance.
7. After configuring all of your VM instances, install the ISR components. See the *ISR Installation Guide* for more information.

Create and Deploy ISR on Azure

You can deploy the Oracle Communications Interactive Session Recorder (ISR) on Azure public clouds. Azure provides multiple ways of managing your environment(s), including via its web portal, using its powershell, and its CLI interfaces. This document focuses on the portal. The portal provides navigation via a web-page pane with links to specified functions on the left side of portal pages. These procedures also assume you have reviewed Azure documentation, and can access portal pages and navigation.

Prerequisites to Deploying an Azure Instance

You can create some of the objects required during the instance deployment procedure prior to or during that deployment. When created prior to instance deployment, these objects become selectable, typically from drop-down lists in the appropriate deployment dialogs. You may use these objects for a single deployment or for multiple deployments.

Tasks denoted here as ISR instance deployment prerequisites include:

- You have identified and are deploying to or via the correct Azure:
  - Subscription
  - Region
  - Location
- You have created the virtual networks you need for ISR (Admin, Local, VoIP, Data) interfaces. Within the context of interface creation, you also need to create:
  - Subnets—To maintain traffic separation, each of the vNICs must be connected to a separate subnet within the virtual network.
  - Security Groups—These define the inbound and outbound traffic allowed through that interface
- During the instance interface creation procedure, you must have the appropriate image, subnets, and security groups available.
  For more information on creating your network elements, see Azure's online documentation.

Deploying the Azure Instance

This is the main instance configuration procedure. It includes a multi-dialog wizard that presents configuration options in the preferred sequence. The result of this wizard is an installed Oracle Linux image on instance. You can add interfaces after deployment.

The following are important requirements:

- Management subnets must be public to allow access from outside the cloud. Addressing within these subnets should include Public IP addresses.
- All Media interfaces addresses that must be reachable through the internet must reside on public subnets; all others can reside on private subnets.

The Oracle Communications Interactive Session Recorder (ISR) is comprised of four components, the Index, RSS, Dashboard, and FACE. The Azure instance configuration procedure's multi-dialog wizard presents configuration options in the preferred sequence.

Basics

The Azure instance deployment allows you to configure a VM instance using the **Basics** configuration.

- Create a VM by associating it to a **Resource group** and choosing the right **Size**.
- Enter details for the **Administrator account**: **Username** with **Authentication Type** (either **Password** or **SSH public key**). For more information, see https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys.
- Configure the Inbound port rules to allow SSH.

Disks

The Azure instance deployment allows you to configure disk size using the **Disk** configuration.

- Select the **OS disk type** based on the VM size.

- Set **OS disk type** to `Standard HDD`.
  Despite the initial boot disk size provided by Oracle, you are free to create a boot disk that is a different size, as supported by Azure. Specifically, consider whether you need a disk that is larger than the initial size to allow for storing log files and other data. When creating disks, refer to both Azure and this *Installation Guide's* instructions and guidelines on creating, formatting and mounting your disks.

Networking

The Azure instance deployment allows you to configure networking using the **Networking** configuration.

- Choose the appropriate **Virtual network** and its **Subnet** that this VM should use.
- Select the right **NIC network security group** for this VM (if NSG has been created).

Management

The Azure instance deployment allows you to configure Management using the **Management** configuration.

- Set **Boot diagnostics** to `On`.
- Set **OS diagnostics** to On.
- Set **Diagnostics storage** account to your account.
- Leave all other fields set to `Off`.

Guest Config

You do not need to configure anything on the **Guest Config** dialog.

Tags

You can define tags in any way you want to help clarify details about objects, however, you are not required to configure anything on the **Tags** dialog.

Review and Create

Use the Review and Create tab to review your settings. Then click **Create** to complete creating the instance.

Create Networking for Additional Interfaces

The minimum Oracle Communications Interactive Session Recorder (ISR) deployment typically has four interfaces. You create networking for all other interfaces after deployment. Azure requires that you stop an ISR intsance before you create and attach additional network interfaces. If not, Azure displays an error during interface configuration. At a minimum, create the following additional interfaces:

- ISR Admin
- VoIP
- Data
- Local Interfaces

When you select an instance from the portal, Azure displays an instance-specific navigation pane on the left side of the dialog. Begin each interface configuration as follows:

- Click **Settings**, **Networking**.
- At the top of the interface configuration dialog, click **Attach Network Interface**.
- In the **Attach Network Interface** dialog click **Create Network interface**.

Create Network Interface

Configure the applicable Create Network interface fields, including the following:

- **Name**—Enter a distinguishable name.
- **Subnet**—Select the correct subnet from the drop-down field.
- **Private IP assignment**—Set this value to `Static`.
- **Private IP address**—Set to an address with a subnet.

Security Groups

The **Create Network interface** dialog includes the **Network security group** selection tool. By default, all network interfaces are set to deny all traffic. You assign security groups to each of the media interfaces to specify the traffic you want to allow. Assuming you have created these groups as a pre-requisite to instance deployment, you select the appropriate group from **Create Network interface** dialog. You can add rules to allow inter-component traffic for VoIP, data, and admin interfaces. See the ISR *Security Guide* for information about specific ports to use.

Complete Azure Deployment Process

Once you have finished configuring network interfaces, you can complete the Azure deployment process as follows:

- Attach the newly created network interfaces to your instance. Azure creates MAC addresses upon interface creation. Note these addresses so you can later verify they are attached to the correct Oracle Communications Interactive Session Recorder (ISR) by login to console.
- Restart the ISR after creating and attaching all interfaces. Use the instance's Serial Console to connect to the virtual COM1 serial port.
- Refer to the ISR Installation Guide and follow the instructions to install all ISR components.

Create and Deploy ISR on AWS

You can deploy the Oracle Communications Interactive Session Recorder (ISR) on Amazon's Elastic Computing (EC2) infrastructure. When deployed on this platform, you configure and operate the ISR as you would on any other platform. You deploy the ISR to use the environment's IP infrastructure, including the private and public addressing scheme, and its translation functions to protect the EC2 management environment from direct exposure to the ISR service delivery environment.

Prerequisites to AWS Deployment

Prerequisites to this deployment procedure include:

- Identify and deploy to the correct AWS **Region**. This is typically a default component of your EC2 Account.

- Identify and deploy to the correct AWS Availability Zone.
- An Amazon Virtual Private Cloud (VPC) is configured.
- A security policy is configured.
- You have determined the four interfaces (admin, VoIP, data, and local) for each instance.
- All subnets are configured. Each virtual network interface on Oracle Communications Interactive Session Recorder (ISR) should have its own unique subnet. Your EC2 workspace may present dialogs and fields that differ from this procedure. For full information on deploying EC2 instances, see the Amazon EC2 documentation here https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html.

AWS Deployment Procedure

Deploying the OCISR on EC2 includes the following high-level steps:

1. Launch your Instances on AWS—this is the main instance configuration procedure. It includes a multi-dialog wizard that presents configuration options in the preferred sequence. The result of this wizard is an installed, Oracle Linux 7.x image with no networking.
2. Open the EC2 console and select **Launch Instance**.
3. Navigate to the **My AMIs** link and choose the **Oracle Linux AMI** from the Community AMI.
4. Choose instance type you are using.
5. Click **Next**. The Configure Instance Details dialog appears.
6. Configure the following instance details; leave the rest of the fields set at their defaults:
   - Specify the number of instances.
   - Select the correct Network for wancom0.
   - Select the correct Subnet for wancom0.
   - Establish a public IP for wancom0, either by using the Auto assign Public IP control or by configuring an elastic IP after deployment.
   - Scroll down to the Network interfaces configuration fields.
   - Ensure you are configuring the Device named eth0.
   - Select `New network interface` from the **Network Interface** drop-down list for wancom0.
   - Select the correct **Subnet** from the dropdown list for wancom0.
   - Ensure the **Primary IP** field is set to `Auto-assign`.
   - Click **Add Device** to add wancom0 (eth0) to your instance.
7. Click **Next**.
8. Enter your desired ISR store size (in GB) in the **Add Storage** field. Click **Next**.
9. Enter a name in the **Add Tags** field to identify the instance. Ensure this name allows you to uniquely identify this instance during later deployment procedures and operations. Click **Next**.

10. Either create a new security group or select an existing security group in **Configure Security Group** to set the appropriate firewall rules. Refer to EC2 documentation for configuration instructions. You can add rules to allow inter-component traffic for VoIP, data, and admin interfaces. Refer to the ISR Security Guide for specific information about ports to use.
11. Click **Review and Launch**. EC2 creates your instances.
12. Return to the EC2 Dashboard and click **Running Instances**.
13. Select your new instances and name them. These names can be the same as your **Tag** names.

Create and Attach Network Interfaces to the ISR Instances

Every instance in a VPC has a default network interface, called the primary network interface (eth0). You cannot detach a primary network interface from an instance. You can create and attach additional network interfaces (admin, VoIP, data, local).

1. Access the EC2 Dashboard and click **Network Interfaces** under Network Security on the left panel.
2. Click Create Network Interfaces.
3. Specify the name of the interface and choose the **Subnet** and **Security group** to associate the Interface.
4. Return to the homepage of the EC2 Dashboard and click **Running Instances**.
5. Select your first instance and ensure it is highlighted.
6. Open the **Actions** drop-down and select **Networking**, **Attach Network Interface**.
7. From the Attach Network Interface pop-up, select your first network interface name.
8. Repeat these steps for all network interfaces and all of your instances you have created.

Configure Elastic IP Addressing

An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.

An Elastic IP address is a public IPv4 address, which is reachable from the internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the internet.

1. Click **Elastic IPs** under Network & Security in the left column.
2. Click **Allocate New Address**, then **Yes**, **Allocate**, and then click **Close**.
3. Select the newly allocated IP address and click **Actions**, and then **Associate Address**.
4. Click on the text box next to **Instance** and select your instance from the drop-down menu.
5. Click Associate.
   Once you have configured VM instances, see the ISR *Installation Guide* to install the ISR components.

C

Configuring an NFS Share For Archival

This chapter provides information about configuring a Network File System (NFS) share for archival.

To configure archival to an NFS share:

1. Once the NFS filesystem is properly being exported by the server, you may try mounting the share to the client host using the following command: object.

   ```
   mount -t nfs -o rw,nosuid <nfs_host_name>:<nfs_mount_path> /opt/isr/
   ArchivedRecordings" e.g. mount -t nfs -o rw,nosuid host01.mydoc.com:/usr/
   local/apps /opt/isr/ArchivedRecordings
   ```

   > **Note:**
   >
   > You may need to install the nfs-utils package for mounting an NFS file system. For more information, refer to https://docs.oracle.com/cd/E52668_01/E54669/html/ol7-cfgclnt-nfs.html.

2. For the mounted share to persist through reboots, you must edit the `/etc/fstab` file and add a line to the bottom with the following format:

   ```
   <server>:</remote/export> </local/directory> <nfs-type> <options> 0 0
   ```

   For example,

   ```
   1.2.3.4:/mnt/nfs_share /opt/isr/ArchivedRecordings nfs defaults 0 0
   ```

   > **Note:**
   >
   > Use the **mount -a** command to remount the filesystems and test your configuration.

3. From the RSS Linux shell, verify that users in the group "isr" have write permissions on the NFS share.
   - Verify the current user is in the "isr" group (in the following example the user's name is "isradm").

     ```
     #groups isradm
     isradm: isradm wheel isr wireshark
     ```

- Add a file on the share.

  ```
  touch /opt/isr/ArchivedRecordings/foo.txt
  ```

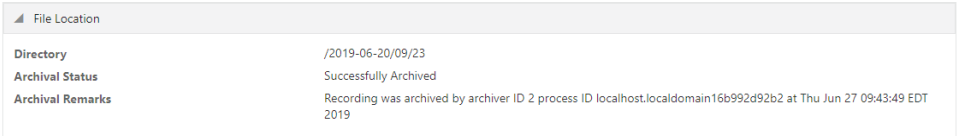
- Verify that the file exists

  ```
  ls -l/opt/isr/ArchivedRecordings/foo.txt
  ```

4. From the RSS Linux shell, using the **systemctl restart tomcatd** command, restart Tomcat. Since the Archived Location was not available as a resource to the application server responsible for serving recordings previously, this is necessary.
5. From the ISR Dashboard, add the new Archival Location.
   - Click **Admin**.
   - Click the **Sites** link.
   - Select the Site on which you are adding the new Archival Location and click **Manage Site**.
   - Click **Locations**.
   - Click **Create**.
   - **name**—Enter a specific name for the Location.
   - **Remote Access URL**—Set the URL serving recordings in the directory (this is likely to be http://<RSS IP>/ArchivedRecording).
   - Click **Local/Mount Configurations**.
   - **Local Recordings Directory**—Set the recordings directory path to **/opt/isr/ArchivedRecordings**.
   - Click **Conversion Configurations**.
   - **Converter IP Address**—Specify the RSS IP address for conversion to play recordings using certain codecs.
   - Click **Create**.
6. From the ISR Dashboard, configure Archival to the Location.
   - Click **Admin**.
   - Click the **Sites** link.
   - Select the Site on which you are configuring Archival to the Location and click **Manage Site**.
   - Click **Archivers**.
   - Click **Create**.
   - **IP Address**—Enter the RSS IP address.
   - **Source**—Set to **<RSS name> (<RSS IP>) Primary**.
   - **Destination**—Set to the name you gave the Location.
   - Click **Create**.

     For more information on advanced settings while configuring a new Archiver, see "Managing Archivers" in the *Administrator Guide*.
7. From the ISR Dashboard, verify that Archival is configured properly.

- Click on **Recordings**.
- Select a recording and click **Details**.
- Click the **File Location** tab and verify that the recording was archived in the **Archival Remarks** field.



> **Note:**
>
> By default, the Archival process runs every two minutes and you must wait for it to run at its scheduled time.

Troubleshooting

Issue:

If the **showmount** command fails:

```
$ showmount 10.138.217.89
clnt_create: RPC: Port mapper failure - Unable to receive: errno 113 (No
route to host)
```

Solution:

This is likely due to a firewalld configuration problem. Verify your configuration.

Issue:

You cannot write to share.

```
$ touch tmpshare/foo.txt
touch: cannot touch `tmpshare/foo.txt': Permission denied
```

Solution:

Update the permissions by changing the mode/ownership of the share on the NFS server using the **chmod** and/or **chown** commands.

D
Configuring Circular Replication

The Index software installation that you performed in Chapter 3, Installing the CIS Software installs and configures the database. For replication you need at least two index installations. You must setup circular replication manually for the Index. Use the following procedure to setup circular replication.

> **Note:**
>
> The below instructions are for configuring MySQL replication with two clean installations of the ISR Index. Any configuration or historical data causes this process to fail, while likely corrupting the data. Consult your Oracle account representative for instructions on configuring replication with an Index containing historical and configuration data.

Configuration Instructions

To configure circular replication:

1. Create a replication user on each MySQL instance.

   Using the MySQL command line client or a GUI tool such as MySQL Workbench, enter the following on the PRIMARY index:

   ```
   GRANT REPLICATION SLAVE ON *.* TO 'repl'@'<secondary index IP address>'
   IDENTIFIED BY '<your_password>';
   ```

   Using the MySQL client again, enter the following on the SECONDARY index:

   ```
   GRANT REPLICATION SLAVE ON *.* TO 'repl'@'<primary index IP address>'
   IDENTIFIED BY '<your_password>';
   ```

2. Enable binary logging on the PRIMARY host.

   a. Log into the Index Virtual Machine (VM) of the PRIMARY host and shut down the MySQL service by entering the following:

      ```
      systemctl stop mysqld
      ```

   b. Make a back-up instance of the file /etc/my.cnf (for example, /tmp/my.cnf), and then edit /etc/my.cnf by entering the following in the [mysqld] section:

      ```
      log-bin=Primary1-mysql-bin
      server-id=1
      #Replication increments to avoid primary key auto-increment
      #collisions for 2 hosts
      auto_increment_increment=2
      ```

```
auto_increment_offset=1
#Set the db/tables to replicate
replicate-do-db=ipcr_db
replicate-ignore-table=ipcr_db.log
replicate-ignore-table=ipcr_db.heartbeats
#Set the master for replication reporting (optional)
report-host= secondary host ip address
```

> **Note:**
>
> If copying and pasting directly from this document, ensure there are no erroneous carriage returns impacting the configuration "my.cnf" file formatting. This could prevent MySQL Server from starting properly.

c. Make sure the following lines are in the mysqld section:

```
binlog-format=mixed
slave-skip-errors=1032
sync_binlog=1
```

3. Enable binary logging on the SECONDARY host.

a. Using a secure shell client (SSH), log into the Index VM of the SECONDARY host. Then shut down the MySQL service by entering the following :

```
systemctl stop mysqld
```

b. Make a back-up instance of the file /etc/my.cnf (for example, /tmp/my.cnf), and then edit /etc/my.cnf by entering the following in the [mysqld] section:

```
log-bin=Secondary2-mysql-bin
server-id=2
#Replication increments to avoid primary key auto-increment
#collisions for 2 hosts
auto_increment_increment=2
auto_increment_offset=2
#Set the db/tables to replicate
replicate-do-db=ipcr_db
replicate-ignore-table=ipcr_db.log
replicate-ignore-table=ipcr_db.heartbeats
#Set the master for replication reporting (optional)
report-host=primary host address
```

> **Note:**
>
> If copying and pasting directly from this document, ensure there are no erroneous carriage returns impacting the configuration "my.cnf" file formatting. This could prevent MySQL Server from starting properly.

c. Make sure the following lines are in the mysqld section:

```
binlog-format=mixed slave-skip-errors=1032 sync_binlog=1
```

4. Start the MySQL instance on both the PRIMARY and SECONDARY hosts by entering the following:

```
systemctl restart mysqld
```

> **WARNING:**
>
> Ensure there are no connections to the ISR Record and Store Server (RSS), and that the Dashboard on both primary and secondary hosts is disabled. To disable the Dashboard via the CLI, issue the following command:
>
> ```
> systemctl stop puma
> ```
>
> To restart the Dashboard via the CLI, issue the following command:
>
> ```
> systemctl start puma
> ```

5. Using the MySQL client, check the Master status on the PRIMARY host by entering the following:

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SHOW MASTER STATUS;
```

The following is an example of the output from the above commands.

File	Position	Binlog_Do_DB	Binlog_Ignore_DB
Primary1-mysql-bin.000002	98	test	manual, mySQL

6. Make a note of the filename and position values from the output table.
7. Free the read lock by entering the following:

```
mysql> UNLOCK TABLES;
```

8. Using the MySQL client, on the SECONDARY host, edit the MySQL replication Slave configuration using the file and position values from the output in Step 5, and enter the following using the CHANGE MASTER command:

```
RESET SLAVE; CHANGE MASTER TO MASTER_HOST='<primary host IP address>',
MASTER_USER='repl', MASTER_PASSWORD='example123',
MASTER_LOG_FILE='Primary1-mysql-bin.000002', MASTER_LOG_POS=98;
```

9. Start the Slaves & ensure there are no errors in the "MySQL logs" by entering the following:

```
mysql> START SLAVE;
```

10. Check the Master status on the SECONDARY host by entering the following:

```
mysql> FLUSH TABLES WITH READ LOCK; mysql> SHOW MASTER STATUS;
```

The following is an example of the output from the above commands.

File	Position	Binlog_Do_DB	Binlog_Ignore_DB
Secondary2-mysql-bin.000002	98	test	manual, mySQL

11. Make a note of the filename and position values from the output table.
12. Free the read lock by entering the following:

```
mysql> UNLOCK TABLES;
```

13. Using the MySQL client, on the PRIMARY host, edit the MySQL replication Slave configuration using the filename and position values from the output in Step 10 (from the SECONDARY host), and enter the following using the CHANGE MASTER command:

```
RESET SLAVE; CHANGE MASTER TO MASTER_HOST='<secondary host IP
address>', MASTER_USER='repl', MASTER_PASSWORD='example123',
MASTER_LOG_FILE='Secondary2-mysql-bin.000002', MASTER_LOG_POS=98;
START SLAVE;
```

The following commands, run on each host, display the current replication status. To improve the formatting, append the command with **\G**.

```
mysql>SHOW MASTER STATUS \G mysql>SHOW SLAVE STATUS \G
```

Configuring Database Failover

To edit the configuration on the ISR API and Archival deployments to include database failover:

1. Using a secure shell (SSH) client, log into the RSS or FACE host/s using a user name and password.
2. To add the secondary database IP address to the API configuration, edit the following file.

```
/var/lib/tomcat/webapps/IsrApi/WEB-INF/web.xml
```

3. Using the arrow keys to navigate the file and edit the following line with the relevant IP addresses:

```
<context-param>
    <param-name>connectionString</param-name>
    <param-value>jdbc:mysql://169.254.1.50,<secondary_host_IP>/ipcr_db</
param-value>
    <description>MsSQLX connection URI</description>
  </context-param>
```

4. Save your changes to the file.
5. Restart the application server by performing the following:

```
systemctl restart tomcat
```

6. If required, verify successful failover between the PRIMARY and SECONDARY servers.

E
ISR RMC

The ISR records sessions in several RTP codecs and handles the conversion and playback of most codecs using the RMC. This RMC is automatically installed as part of the RSS installation and runs on its own license. Contact your Oracle sales representative for more information about obtaining the RMC license.

The ISR RMC is a media converter that converts recordings from RTP packet data (“.rpdd” formatted files) to Pulse Code Modulation (PCM) wave files (.wav formatted files), for playback by the ISR Dashboard. It allows the ISR to record calls from multiple codecs, including G.729, g.711 mulaw, g.711, alaw, and g.722. Consult the ISR Release Notes for a complete list of RTP codecs currently supported on the ISR.

In previous releases, the location configurations through the ISR Dashboard were associated only with archiving - the moving of recorded files and updating of the recording information in the database. Now each location also has an RMC configuration to define which RMC has access to the files at that location. When a user plays a recording that is in raw RTP format (.rpdd formatted file), the dashboard makes a request to the RMC converter set for that file's location. Once the RMC converter is finished transcoding (to .wav format), the browser's media player plays the file.

Testing the RMC Converter

Test that the RMC is converting properly by playing a G.729 recording through the ISR Dashboard.

To test the RMC converter:

1. Open your Internet Web browser.
2. Enter the IP address of the ISR Dashboard. For example:

   ```
   http://172.54.66.7
   ```

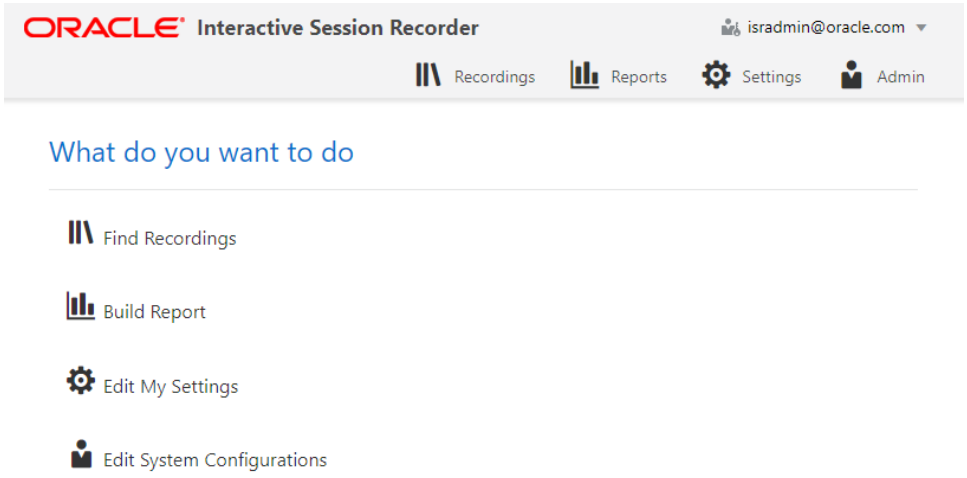
   The Login page displays.
3. Enter your credentials in the **Email** and **Password** fields.

   The default user name and password are:

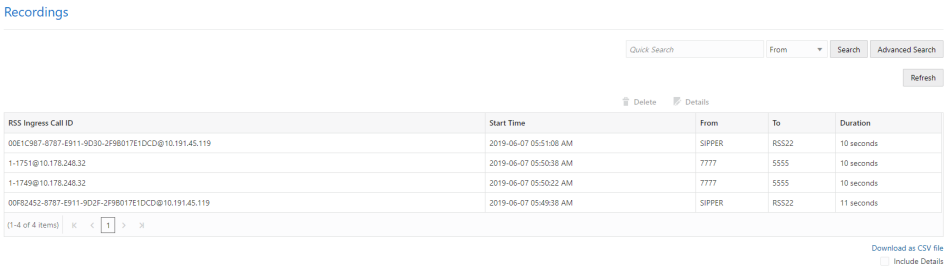
   User name: isradmin@acmepacket.com

   Password: admin123

   The following page displays.



4. From the Main Menu, click **Recordings**. The following page displays.



5. Select a recording that has a file name in the format .rpdd and then click the Play icon.

   If the RMC conversion process was successful (recording is converted from a ".rpdd" file to a .wav file), the recording opens and an audible playback of the recording is heard.

   If the RMC conversion process was unsuccessful, an error message displays.

   Converter logs can be found on the RSS host in /opt/isr/logs/converter/ for troubleshooting.

ISR RMC License

This RMC is automatically installed when performing the RSS installations.

Assigning RMC Conversion to Specific Locations

The ISR recordings are stored at locations you specified during the installation process of the CIS and RSS. If you enable the RMC license on your ISR, each location containing files that could require conversion must have an RMC set to handle conversion of the files for playback.

By default, a converter is configured on every location that is created. Some locations, like SANs, do not have a converter installed and should be configured to use an existing converter.

To specify RMC conversion to a specific location:

1. Open your Internet Web browser.
2. Enter the IP address of the ISR Dashboard. For example:

   ```
   http://172.54.66.7
   ```

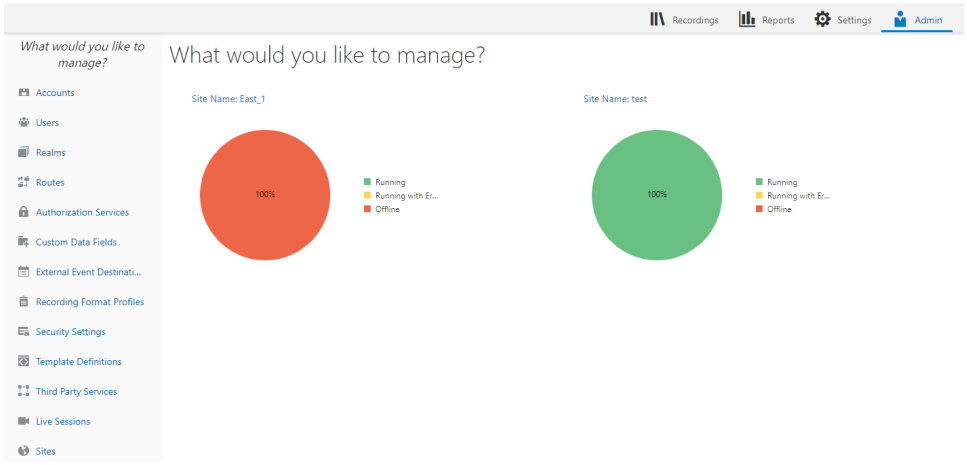
   The Login page displays.
3. Enter your credentials in the **Email** and **Password** fields.

   The default user name and password are:

   User name: isradmin@acmepacket.com

   Password: admin123

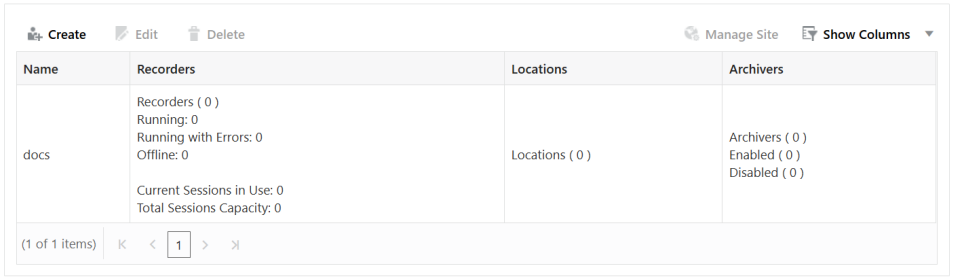
   The home page displays.
4. From the Main Menu, click **Admin**. The following page displays.



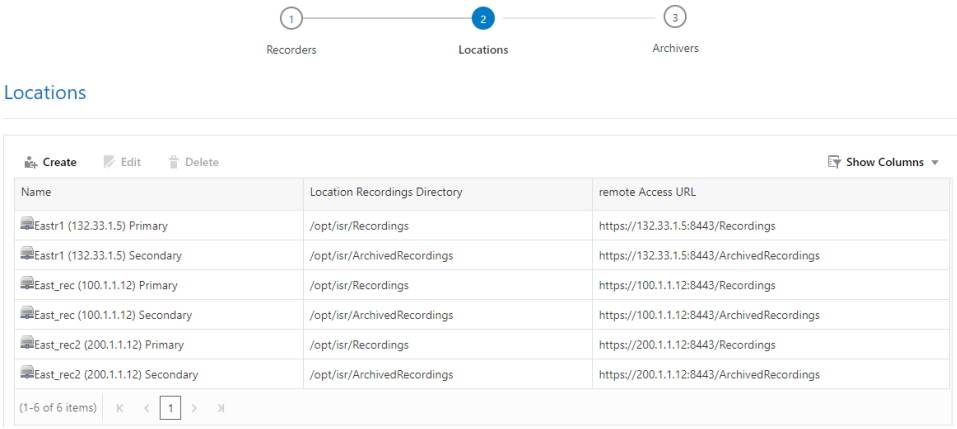
5. Click **Sites**.

   The Sites page displays.

Sites



6. Select the Site you want to edit and click **Manage Site**.
7. Click **Locations**. The following page displays.



8. Select the Location you want to edit and click **Edit**. The Edit Location page displays.
9. Click **Conversion Configurations**.
10. Specify the RMC IP address in the **Converter IP Address** field.
11. Click **Update** to update the location with the RMC information.

F

ISR Troubleshooting and Customizations

This Appendix provides FAQs and additional information regarding the ISR components for your reference.

Log Collection Scripts

Each ISR component contains a log collection script. To collect logs for a service request, run the 'collectLogs.sh' script and attach the resulting TGZ file to the request.

> **Note:**
>
> By default, the TGZ file can be found in the directory from where the script was executed.

vSphere Hypervisor

Q. How do I manage the virtual machine (VM) host?

A. You use the VMware vSphere client to monitor and configure the VM host. To install the vSphere client, see Chapter 3, Installing the CIS Software.

Q. What operating system do the virtual machines use?

A. All VMs use the Oracle Linux Server release 7.2.

Q. How do I monitor and manage the virtual machines?

A. You use the VMware vSphere client to monitor and configure the VMs. To install the vSphere client, see Chapter 3, Installing the CIS Software.

A. How do I download files from a virtual host?

A. SSH file transfers with an SFTP client such as Filezilla using the root user and password gains access to any file on the system.

Index Virtual Machine

Q. What version of MySQL Server is installed with the CIS?

A. The MySQL Server version is MySQL Enterprise Commercial (Advanced) Edition Version 5.7.36.

Q. How do I view the logs in MySQL Server?

A. MySQL Server's log file can be found in the directory /var/lib/mysql.log. The main log file is named <host_name>.err. The error log can be found in the directory /var/lib/mysql/index.err.

If configured to do so, slow query logs can be found in the directory /var/lib/mysql/index-slow.log.

> **Note:**
>
> All ISR-related errors are found in the respective component logs.

Q. How do I log slow queries in MySQL Server?

A. To start logging slow queries without restarting mysql server, execute the following:

1. At MySQL command prompt, enter **set global slow_query_log=1**.
2. Enter **set global long_query_time=1** (or whatever you want for query seconds).
3. To verify the settings for these commands, use the following show variables: **%slow% %length%** By default, the slow query logs are stored in the directory /var/lib/mysql/index-slow.log.

Q. How do I find the data files in MySQL Server?

A. Data files for the '**ipcr_db**' database are found in the directory /var/lib/mysql/ipcr_db/.

Dashboard Virtual Machine

Q. How do I log in to the ISR Dashboard?

A. Perform the following:

1. Open your Internet Web browser.
2. Enter the IP address of the ISR. For example:

   ```
   http://172.54.66.7
   ```

   The Login page displays.
3. Enter your email and password, respectively, in the Email and Password fields.

> **Note:**
>
> When logging into the ISR Dashboard for the first time, you are required to enter new email and password credentials, and then again every 90 days.

Q. How do I find the version of the ISR Dashboard?

A. The ISR Dashboard version number is shown on the bottom border of all pages in the graphical user interface (GUI).

Q. How do I troubleshoot problems with the web interface on the Dashboard VM?

A. A common error during Dashboard deployment leaves the Dashboard unable to connect to the Index VM database. If browsing to the Dashboard IP results in the

display of a "500 Internal Server Error" message (for example, in Chrome HTTP Error 500 (Internal Server Error): An unexpected condition was encountered while the server was attempting to fulfill the request.), the error should be described in the Dashboard application log.

To access the application log:

4. Access the Dashboard VM shell.
5. Enter **less /var/www/dashboard/current/log/production.log**.
6. Enter **G** to scroll to the bottom of the log.
7. Scroll up the file looking for the following lines:

```
Status: 500 Internal Server Error
Can't connect to MySQL server on '169.254.1.50' (113)
```

8. Enter **q** to exit.
9. Enter **ping 169.254.1.50**.
10. If the following appears:

```
PING 169.254.1.50 (169.254.1.50) 56(84) bytes of data
From 169.254.1.50 icmp_seq=2 Destination Host Unreachable.
```

<Ctrl> C to discontinue the ping and check the network service status and connections on the Index host's eth1 interface.

Multiple Partition Support

The ISR can be configured with more than one partition. If needed, you can store recording files and logs on one partition and other application files on another. This section provides information on configuring multiple partitions.

Before running the `configIsr.sh` script, ensure the following prerequisites are complete:

- The partitions are already created on the RSS host. For example, `/home` and `/opt`.

> **Note:**
>
> During the installation, the default configuration of partitions allocates almost the entire disk to the `/home` directory. ISR software is installed by default on the path `/opt/isr`, requiring more space on the root ("/") directory, or more specifically the `/opt` directory.

- Ensure that the directory path to store Recordings and ArchivedRecordings has been created on the correct partition.
- Ensure that the partition directory path has valid ownership and permissions. For example:

```
# ls -ltr /home/
drwxrwxrwx. 4 isr    isr     4096 May 31 06:15 isr
```

```
#ls -ltr /home/isr
drwxrwxr--. 2 tomcat isr 53370880 Jun 12 21:14 ArchivedRecordings
drwxrwxr--. 2 isr    isr  7577600 Jun 12 22:20 Recordings
```

- If needed, update the permissions, using the **chmod** and **chown** commands, to change the mode and ownership of the partition directory paths.

```
chown isr:isr isr/
chown isr:isr Recordings/
chown tomcat:isr ArchivedRecordings/

chmod 777 isr
chmod 774 Recordings
chmod 774 ArchivedRecordings
```

For instructions on configuring the ISR for storing other files (for example, application logs) on different partitions, consult your Oracle representative.

To configure multiple partitions in the ISR file system:

1. Execute the `/opt/isr/configIsr.sh` script.
   You are prompted to specify the path for the Recording and ArchivedRecordings files.
   - Enter the Recordings path to be served by Tomcat:

     > **Note:**
     >
     > This value must match the Primary location entry configured for this RSS.

     ```
     [/opt/isr/Recordings]
     ```

     This is where you can specify a different path for Recordings than `/directory`. For example,

     ```
     [/home/isr/Recordings]
     ```

   - Enter the Archived Recordings path to be served by Tomcat.

     > **Note:**
     >
     > This value must match the Secondary location entry configured for this RSS.

     ```
     [/opt/isr/ArchivedRecordings/]
     ```

This is where you can specify a different path for ArchivedRecordings than `/directory`. For example,

```
[/home/isr/ArchivedRecordings]
```

2. Verify that different Recordings and ArchivedRecordings paths are updated appropriately in the `/usr/share/tomcat/conf/server.xml` file.

```
<Context docBase="/home/isr/Recordings" path="/Recordings"/>
<Context docBase="/home/isr/ArchivedRecordings" path="/
ArchivedRecordings"/>
```

3. When you are creating an RSS in the Dashboard, from the **Sites, Locations**, **Local/ Mount Configurations**, **Local Recordings Directory** parameter, specify the paths you configured for Recording and ArchivedRecordings.

G

Selective Call Recording SIPREC

The SIPREC protocol is used to interact between a Session Recording Client (SRC) (the role performed by the ISR) and a Session Recording Server (SRS) (a third-party call recorder or Oracle Communications Interactive Session Recorder's Record and Store Server (RSS)). Selective Call Recording controls the recording of media transmitted in the context of a communications session (CS) between multiple user agents.

SIPREC provides a selective-based call recording solution that increases media and signaling performance on a recording server, more robust switchovers, and the ability to selectively record. SIPREC also isolates the RSS from the communication session.

The SRC starts a recording session for every call within a configured realm. All call filtering, if needed, must be accomplished by the recording server. The recording server performs the filtering and the selection of which sessions it should record.

SIPREC supports sending transcoded and SRTP calls.

SIPREC for Active Recording

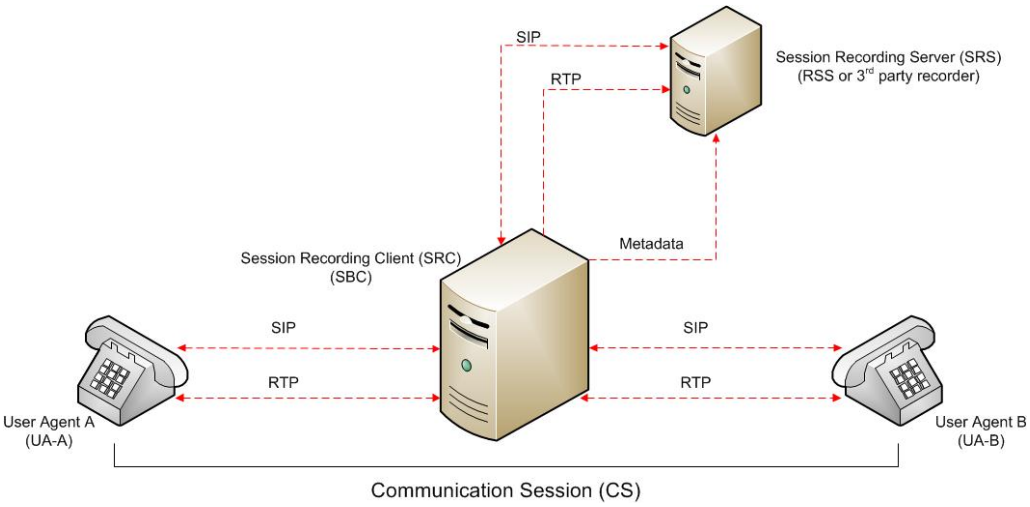
SIPREC supports active recording, where the ISR (ISR) acting as the Session Recording Client (SRC), purposefully streams media to the Oracle Communications Interactive Session Recorder's RSS (or 3rd party call recorder) acting as the SRS. The SRC and SRS act as SIP User Agents (UA). The SRC provides additional information to the SRS to describe the communication sessions, participants and media streams for the recording session to facilitate archival and retrieval of the recorded information.

The ISR acting as the SRC, is the source for the recorded media. The ISR consumes configuration information describing the ecosystem within which it operates. The interface, realm and session agent configuration objects specify the SIPREC configuration. A SIP UA can elect to allow or disallow any network element from recording its media.

During the establishment of a SIP Session, the ISR determines if SIPREC is configured for recording the call. If so, it then duplicates the media prior to initiating the session with the SRS. (Media replication is set up prior to the recording session). The SRS may choose to record, not record, or cancel the recording session, and then communicates by way of SIP signaling to the ISR. If the call is not to be recorded, the SRS signals termination of the recording session.

The ISR maintains SIPREC metadata information associated with recording sessions. The recording session metadata describes the current state of the recording session and its communication session(s). It is updated when a change of state in the communication session(s) is observed by the ISR. The SRS is responsible for maintaining call history, etc. The ISR creates and logs call detail records (CDRs) in the current manner, the 3rd party SRS vendor may collate this information if desired.

The following illustration shows two endpoints, User Agent A (UA-A) and User Agent B (UA-B). Their session is being recorded by an SRC (the ISR) and an SRS.



Preserve SIPREC with SIP REFER Header

When the ISR (ISR) generates a new INVITE as part of terminating a SIP REFER, the ISR evaluates the SIPREC configuration of the realms and session agents involved in the new call leg and responds accordingly. The REFER and Transfer mechanism automatically preserves the UCID, XUCID, GUID, GUCID, and UUI in the metadata, and can forward this information to the Session Recording Server. The ISR can Start, Stop, Pause, and Resume SIPREC sessions in response to any re-INVITE, UPDATE, new INVITE, REFER, or specified SIP Response Message.

The ISR can establish a new session or update the existing session with the SIPREC server in the following ways.

- When the A-B call leg SA-realm-sipinterface is configured for SIPREC, and the B-C call leg SA-realm-sipinterface is not configured for SIPREC, the ISR sends metadata to the Session Recording Server to stop the recording on the sessionID associated with the original call.
- When both the A-B call leg and the B-C call leg have the same SIPREC configuration on their SA-realm-sipinterface, the ISR sends metadata to the Session Recording Server to stop Party A participation and start Party C participation within the same sessionID.
- When the A-B and B-C call legs have a different SIPREC configurations on their SA-realm-sipinterface, the ISR sends metadata to the A-B call leg Session Recording Server to stop the current recording session and sends metadata to the B-C call leg Session Recording Server to start a new recording session with a new sessionID.

Configuring SIPREC

For more information on configuring SIPREC on an SBC, see the *Oracle Communications Session Border Controller Call Monitoring Guide*.

H

Creating a Virtual Machine

This section describes the process of creating a VM.

Configuring a VMware Enterprise vSphere Hypervisor (ESXi)

What is vSphere Hypervisor?

The vSphere Hypervisor (formerly known as ESXi), is the free edition of vSphere offering the bare-metal architecture for best possible performance. It installs during boot-time of the Hypervisor host.

The following components traditionally run on the Hypervisor platform:

- **Index** - MySQL Server stores the recording and management data
- **Dashboard** - Single ISR Dashboard for both the Administrator and User
- **FACE API**

Virtual Machine Default Resource Configurations

Any Hypervisor that Supports Oracle Linux Releases 7.2 - 7.7 are permitted. For more information, see the "Hardware" section of this guide.

Note:

A table on the VMWare Knowledge Base recommends certain VM virtual hardware versions (“VM Version” above) with Hypervisor (ESXi) platform versions. Although no misbehavior associated with the ISR hosts has been confirmed as related to hardware version incompatibilities, the latest virtual hardware version, vmx-10, has been successfully tested with the recommended Hypervisor version, VMware ESXi 5.5 Update 2. The following instructions from VMWare’s Knowledge Base explain upgrading the virtual hardware version of a VM:

1. Power on the VM to be upgraded.
2. Install VMware Tools using vSphere client by right-clicking on the VM, selecting the **Guest** menu, and the **Install/Upgrade VMWare Tools** option.
3. In vSphere client, right-click the entry for the VM and select **Upgrade Virtual Hardware**.
4. In vSphere Client’s General Summary of the VM confirm the **VM Version** value is **vmx-10**.
5. Power on the VM.

Installing vSphere Hypervisor

Use the following procedure to install vSphere Hypervisor. Before beginning this installation, be sure you have performed the tasks in the section Before You Begin.

To install vSphere Hypervisor:

1. Open a web browser and enter the following URL to navigate to the VMware download page:

   https://my.vmware.com/web/vmware/evalcenter?p=free-esxi5&lp=default

2. Download the ESXi 5.5 update 1 file to your server.

> **Note:**
>
> You may need to login into the VMware download page with a user name and password before downloading the file. If not already registered, please register and then login to download the applicable file.

3. Burn the ESXi 5.5 update 1 <filename>.ISO image to a CD.
4. Boot the server from the ESXi 5.5 update 1 CD you just created.
5. At the prompt, press Enter to proceed with the installation.
6. Press <**F11**> to accept the ESXi 5.5 license.
7. At the Select a Disk menu, press Enter to confirm the remote storage device and continue.
8. Press <**F11**> to install the ESXi 5.5 update 1.
9. When the installation is complete, remove the CD and press Enter to reboot the server.
10. Configure the vSphere Hypervisor using the procedures in Configuring vSphere Hypervisor.

Configuring vSphere Hypervisor

After installing the vSphere Hypervisor, you must perform two basic configuration step before you can use it. Use the following procedure to configure vSphere Hypervisor.

1. After installing vSphere Hypervisor and rebooting the server, press <**F2**> **Customize System**.
2. At the login prompt, enter the following:

```
User name: root
Password: <leave blank>
```

3. Select **Configure Password** and follow the instructions to assign a password to assign for logging into vSphere Hypervisor.

   The password rules as stated on the VMWare knowledge base are as follows:

   A valid password requires a mix of upper and lower case letters, digits, and other characters. You can use a 7-character long password with characters from at least

3 of these 4 classes, or a 6-character long password containing characters from all the classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used. It is recommended that the password does not contain the username.

> **WARNING:**
>
> This password is required to login to your Hypervisor instance (this console) as well as for accessing through the vSphere client.

Keep this password secure.

4. Press Enter when complete to enter the System Customization Menu.
5. Select **Configure Management Network** and press Enter.
6. Select **Network Adapters** and confirm at least one network interface card (NIC) has status showing "Connected". Press Enter.

> **Note:**
>
> Make a note of this NIC; you will need this information later.

7. Select **IP Configuration** and press Enter.
8. Press <space bar> to select **Set Static IP Address and Network Configuration**.
9. Enter the IP address of your ESXi Host and press Enter.

   For example, IP Address: 172.40.34.56
10. Enter the subnet mask and press Enter.

    For example, Subnet Mask: 255.255.255.0
11. Enter the default gateway and press Enter.

    For example, Default Gateway: 172.40.34.1
12. Press <**Esc**> to exit the IP Configuration Menu.
13. Select **DNS Configuration**.
14. In the DNS Server field, specify the domain name system (DNS) server addresses if required.

> **Note:**
>
> Internet access is required to download the vSphere Client in the next section.

15. In the Hostname field, specify the Hostname for the server to use.
16. Press <**Esc**> to exit the DNS Configuration Menu.
17. Press <**Esc**> to exit the Management Network Menu.
18. At the Save Changes prompt, press **Y** to apply the changes and restart the management network.

19. Select **Test Management Network**.
20. Attempt to ping your server in the network.

> **Note:**
>
> The ping you send out may include any DNS server configured in your network.

If the first attempt fails, try pinging again. The test should show a response from your server indicating that your server was setup correctly for network management in your network.

> **Note:**
>
> If your hostname cannot be resolved by your DNS servers, or you didn't configure any DNS servers, the resolving hostname test will fail. This does not adversely affect the CIS performance.

21. Press <**Esc**> to exit the Test Management Network Menu.
22. Press <**Esc**> to log out.

    Once the ESXi host is on the network, perform all configuration management through the vSphare client.

VMware vSphere Client

What is vSphere Client?

The vSphere Client is an application that enables management of a vSphere installation. The vSphere Client provides an administrator with access to the key functions of vSphere without the need to access a vSphere server directly.

Installing vSphere Client

After installing the vSphere Hypervisor onto your server, you can then install the vSphere Client onto your Microsoft Windows® machine. Installing the vSphere Client, includes:

- Downloading the vSphere Client from VMware
- Assigning a License to VMware vSphere Hypervisor
- Assigning the network time servers
- Adding additional virtual network

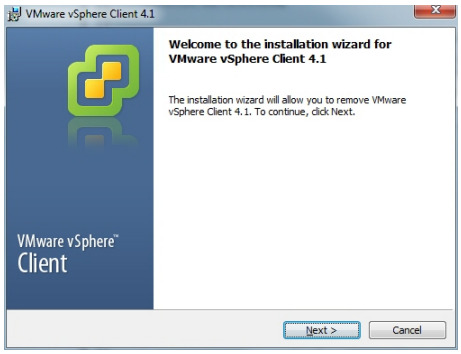
To install the vSphere Client:

1. Open your web browser. Enter the IP address of the ESXi host which you configured in the procedure, Configuring vSphere Hypervisor. (http://<ESXi host ip address>) and press Enter. This accesses the web page to download the vSphere Client to your Windows machine. For example,

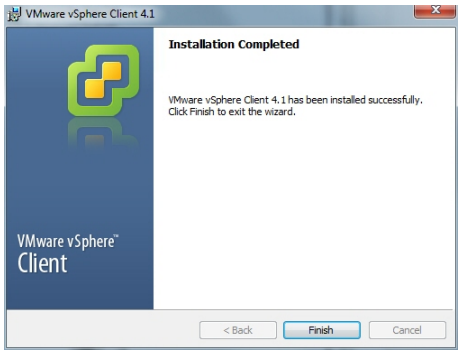
http://172.30.58.164

A warning displays followed by a prompt allowing you to accept or reject the certificate.

2. Press Enter to accept the certificate.
3. Click **Download vSphere Client.**
4. Navigate to the location on your PC where you downloaded the vSphere Client.
5. Double-click the file to begin the installation. The file proceeds to extract the application files and continues the installation process. The following screen displays.



6. Click **Next**. Select I agree to the terms in the license agreement and click **Next**. Continue the installation by following all remaining instructions for installing the vSphere Client. When the installation is complete, the following screen displays.



7. Click **Finish** to complete the installation. The VMware vSphere Client icon appears on your PC desktop.

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

9. 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**

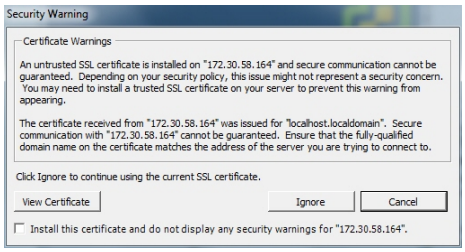
10. In the **User name** text box, enter the user name assigned to you by the system administrator of the ESXi host. For example:

    User name: **root**

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

    Password: **jre453i**

12. Click **Login**. The following Security Warning displays:



13. 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.

14. Press **Ignore**. The VMware Evaluation Notice alert displays.

15. Click "Assign license to the ESXi host."

> **Note:**
>
> vSphere 4 Hypervisor is licensed for 2 physical CPUs (free, never expires).

Getting the vSphere Hypervisor License

To get the VMware vSphere Hypervisor License:

1. Enter the following URL:

   https://www.vmware.com/account/login.do

2. Register for a VMware account by clicking Register. Or if already registered, enter your email address or VMware customer number, and password, and click Sign In.

   VMware sends the following message to the email address you specified during registration:

   Thank you for creating a VMware account. To complete the registration process, please click the button below.

3. Open your email message from VMware and click the Activate Now button.

   The VMware ‘s Enter Your Password screen displays.

4. In the Password text box, enter the password you specified when registering with VMware and click Continue.

   The "Account Activated" screen displays with the following message:

   Success! Your account has been activated.

5. Copy and paste the following link into your browser:

   https://my.vmware.com/web/vmware/evalcenter?p=free-esxi5&lp=default&lp=1&ie=UTF-8&q=vmware%20vsphere%20hypervisor%20esxi%204.1%20license

6. In the box, **On how many physical servers do you plan to install VMware vSphere Hypervisor?**, enter the number of servers on which you are installing the VMware vSphere Hypervisor.

   Valid values are 1 - 999.

7. Place a check mark in the box, **I agree to the terms and conditions outlined in the VMware vSphere Hypervisor End User License Agreement**. and click **Register**.

   VMware sends you an email message for accessing your VMware ESXi License.

8. Open your email message from VMware and click **Access Now**.

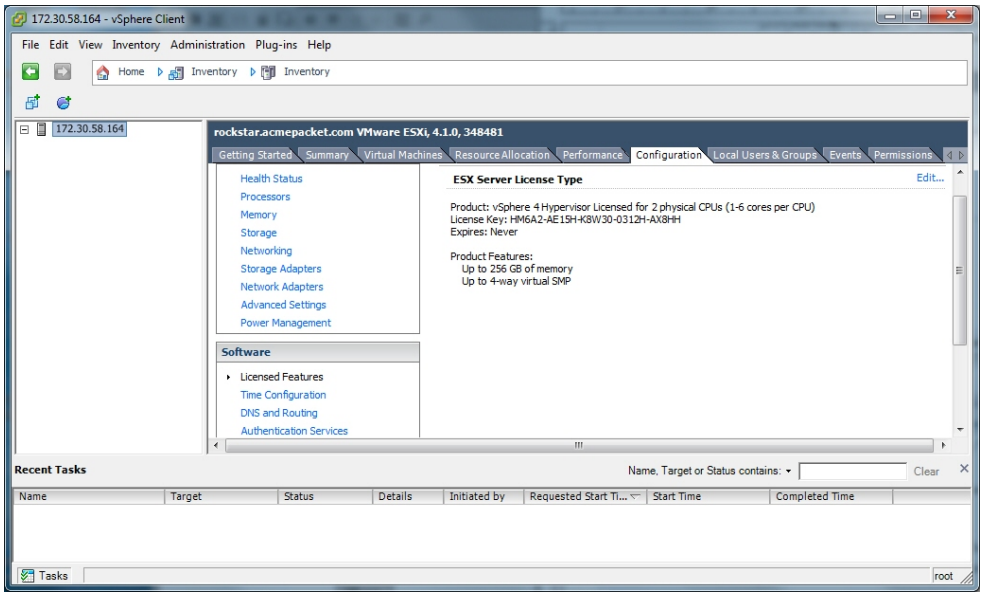
   A VMware vSphere Hypervisor license string displays.

9. Copy the VMware vSphere Hypervisor license key string.

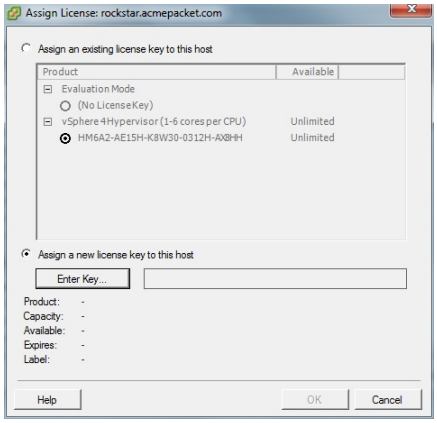
Applying the VMware vSphere Hypervisor License

To apply the VMware vSphere Hypervisor license:

1. Click **OK** to close the VMware Evaluation Notice window that displayed in Step 14. The following window displays. The ESXi Host IP displays in the left column.



2. Click the **Configuration** tab.
3. In the left column, under the Software category, click **Licensed Features**.
4. In the upper right corner of the window, click **Edit**. The following window displays.



5. Click the radio button **Assign a new license to this host**. and click **Enter Key**. A pop-up displays allowing you to enter the license key string.
6. In the **New License Key** text box, paste the license key string you copied from Step 24. Or enter the license key string manually.

Configuring your vSphere ESXi Host

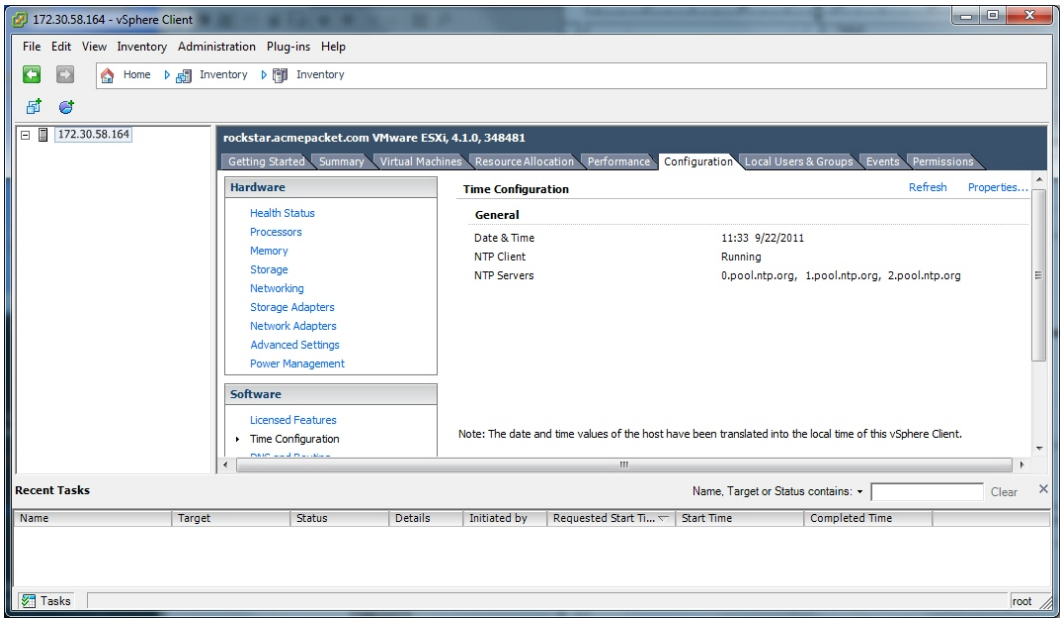
After installing your vSphere Client, you must configure the vSphere ESXi host's network time server. Use the procedures in this section to configure the network time server of your ESXi host.

Assigning Network Time Server

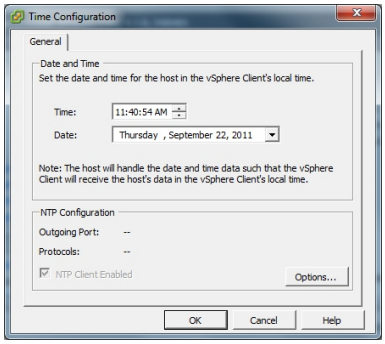
To assign a network time server:

1. Open the vSphere Client and enter your username and password to login.

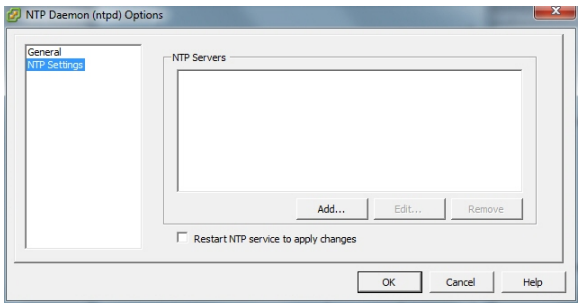
2. In the vSphere Client window, click the **Configuration** tab.



3. In the left column, under the Software category, click on **Time Configuration**.
4. In the upper right corner of the window, click on **Properties**. The following window displays.

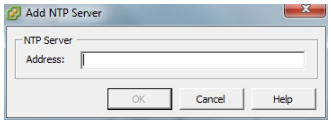


5. Click on **Options**. The following window displays.



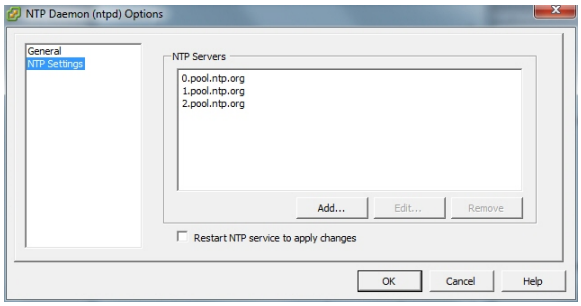
6. In the left column, click on **NTP Settnigs**.

7. Click **Add**. The following window displays.

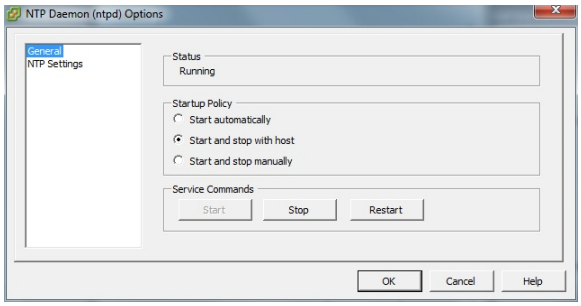


8. Add each of the following in the **Address** text box, clicking **OK** after each entry:
   - 0.pool.ntp.org
   - 1.pool.ntp.org
   - 2.pool.ntp.org

   The entries display in the NTP Servers box.



9. In the left column, click on **General**. The following window displays.



10. Click **Restart**.

> **Note:**
>
> It is important that your ISR component hosts are assigned the same timezone, except the Index host, which must be set to UTC.

You must now configure your local network using the procedures in Configuring the Local Network.

Configuring Additional Networks

This section describes how to configure a local network, a VoIP network, and a Data Network.

Configuring the Local Network

The ISR applications have network default configurations to simplify initial deployment, particularly for VM environments. These configurations expect a private, internal network known as "Local" that offers the IP address range of 169.254.1.x.

The default application Local IPs are set to the following:

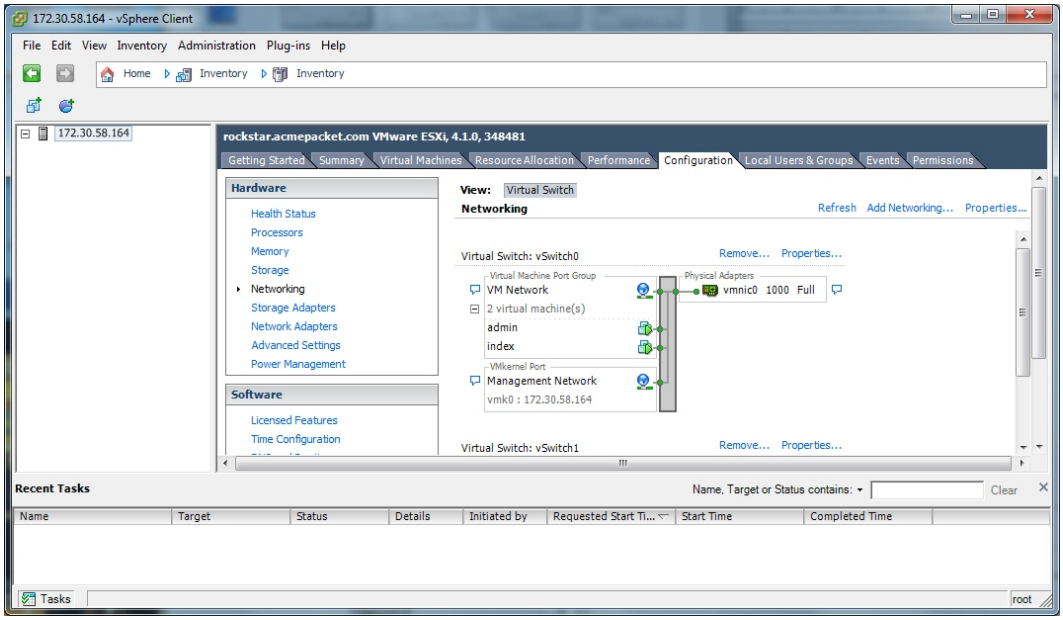
Component	Default Local IP
Dashboard	169.254.1.20
Index	169.254.1.50
RSS	169.254.1.xyz (where xyz=RSS's Administration network host address
FACE API	169.254.1.40

This section describes adding the Local network.

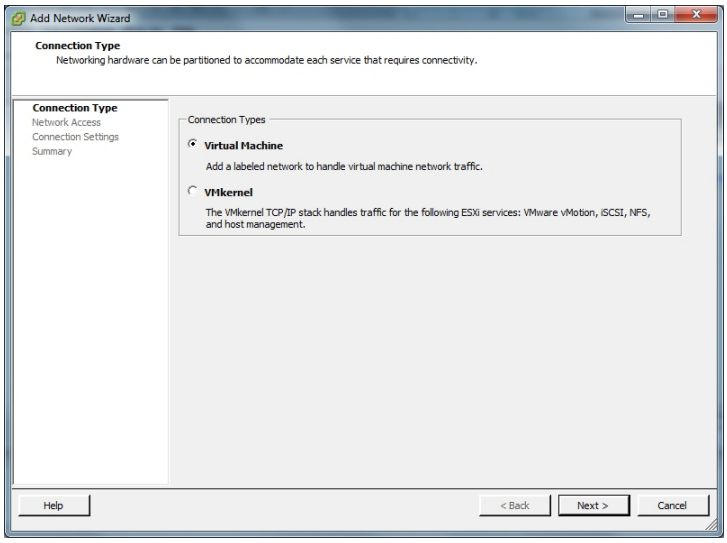
To create and configure your local network:

1. Open your vSphere Client and enter your username and password to login.

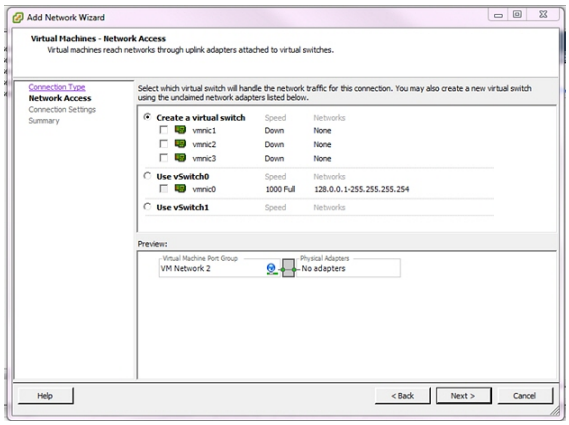
   The following window displays.



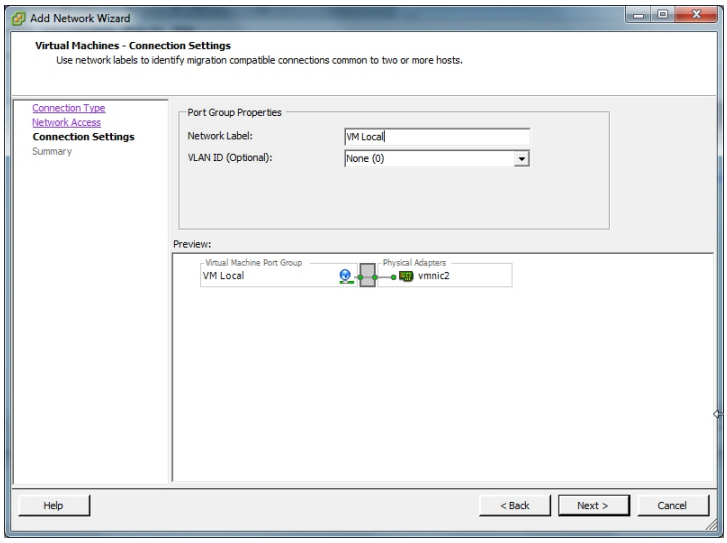
2. Click on the **Configuration** tab.
3. In the left column, under the Hardware category, click on **Networking**.
4. In the upper right corner of the window, click on **Add Networking**. The following window displays.



5. Click on the radio button for **Virtual Machine** and click **Next**. The following window displays.



6. The **Create a virtual switch** radio button is enabled by default. Make sure you leave this enabled. In the case of a pure-VM solution, the virtual network you are creating is not affiliated with any of the physical network interfaces on your ESXi host. However, a bare-metal RSS installation requires a physical interface between the CIS server and RSS server(s). For more information, see "Configuring a Bare-Metal RSS Installation".
7. Uncheck (disable) the vmnic1 adapter.
8. Click **Next**. The following window displays.



9. In the Port Group Properties section, enter a network label for this virtual switch in the **Network Label** text box. For example, VM Local.
10. The VLAN ID value is set as None(0). Do not change the default value in this field.
11. Click **Next**. Click **Finish**.

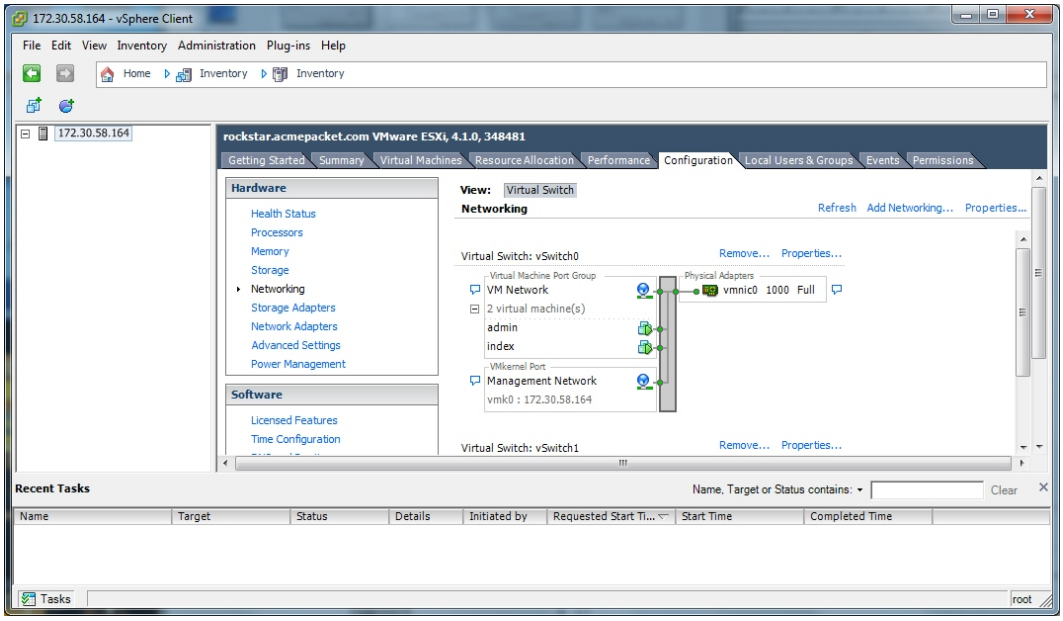
    The local virtual switch is now created.

Configuring the VoIP Network

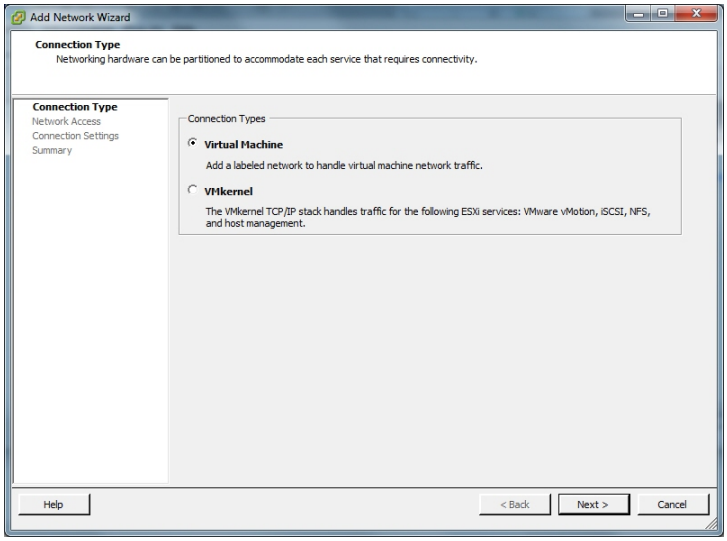
This section describes adding the VoIP network.
To create and configure your VoIP network:

1. Open your vSphere Client and enter your username and password to login.

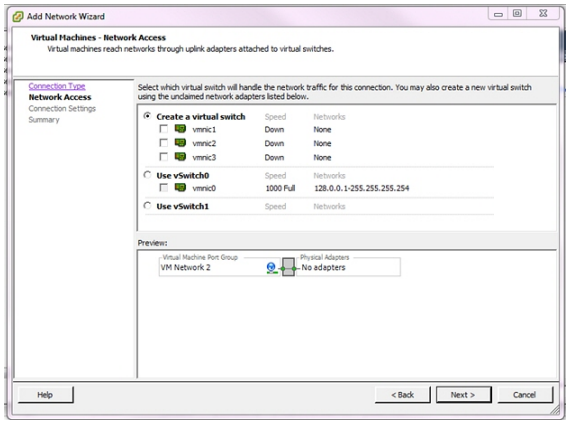
   The following window displays.



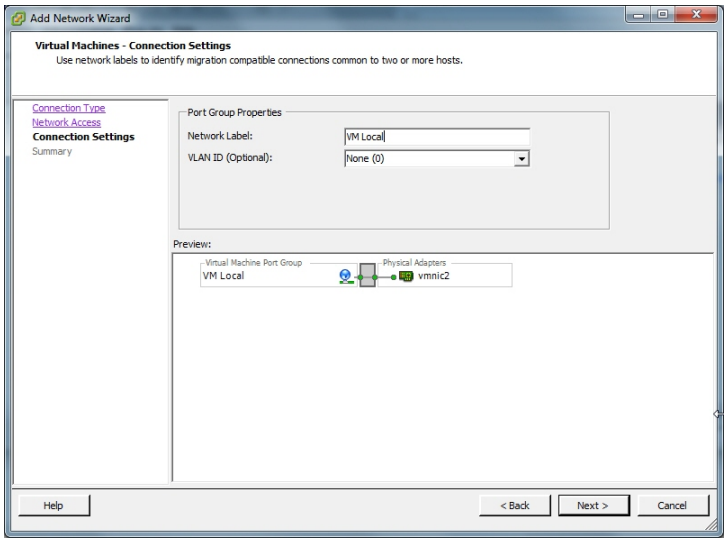
2. Click on the **Configuration** tab.
3. In the left column, under the Hardware category, click on **Networking**.
4. In the upper right corner of the window, click on **Add Networking**. The following window displays.



5. Click on the radio button for **Virtual Machine** and click **Next**. The following window displays.



6. The **Create a virtual switch** radio button is enabled by default. Make sure you leave this enabled. In the case of a pure-VM solution, the virtual network you are creating is not affiliated with any of the physical network interfaces on your ESXi host. However, a bare-metal RSS installation requires a physical interface between the CIS server and RSS server(s). For more information, see "Configuring a Bare-Metal RSS Installation".
7. Uncheck (disable) the vmnic1 adapter.
8. Click **Next**. The following window displays.



9. In the Port Group Properties section, enter a network label for this virtual switch in the **Network Label** text box. For example, VM Local.
10. The VLAN ID value is set as None(0). Do not change the default value in this field.
11. Click **Next**. Click **Finish**.

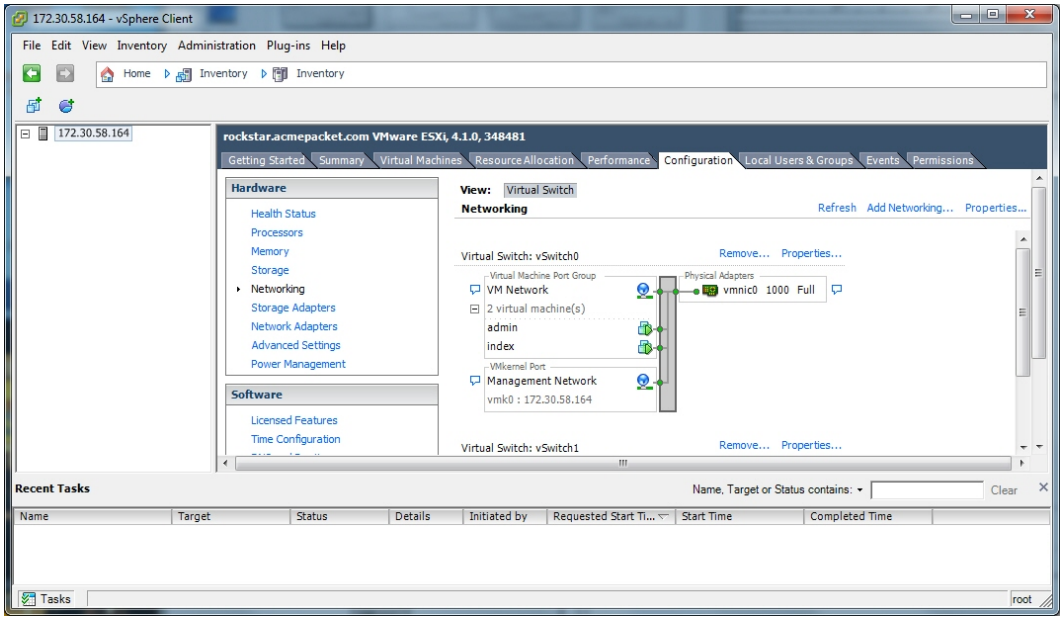
    The VoIP network is now created.

Configuring the Data Network

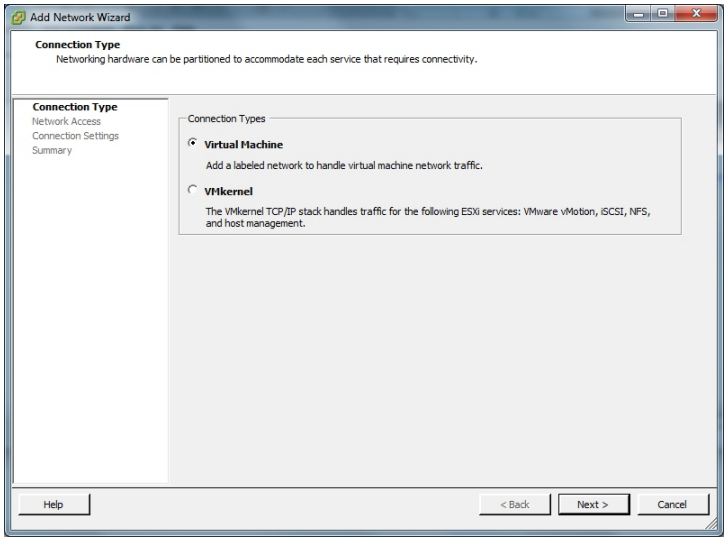
This section describes adding the Data network.
To create and configure your Data network:

1. Open your vSphere Client and enter your username and password to login.

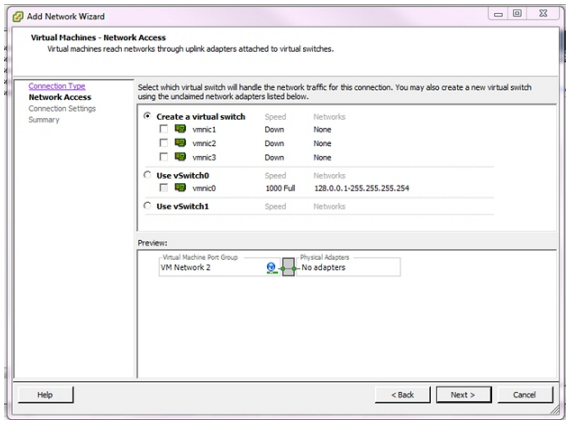
   The following window displays.



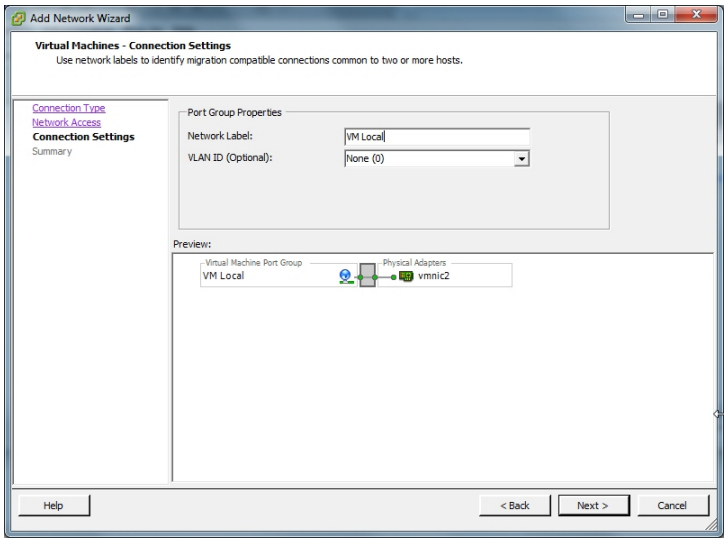
2. Click on the **Configuration** tab.
3. In the left column, under the Hardware category, click on **Networking**.
4. In the upper right corner of the window, click on **Add Networking**. The following window displays.



5. Click on the radio button for **Virtual Machine** and click **Next**. The following window displays.



6. The **Create a virtual switch** radio button is enabled by default. Make sure you leave this enabled. In the case of a pure-VM solution, the virtual network you are creating is not affiliated with any of the physical network interfaces on your ESXi host. However, a bare-metal RSS installation requires a physical interface between the CIS server and RSS server(s). For more information, see "Configuring a Bare-Metal RSS Installation".
7. Uncheck (disable) the vmnic1 adapter.
8. Click **Next**. The following window displays.



9. In the Port Group Properties section, enter a network label for this virtual switch in the **Network Label** text box. For example, VM Local.
10. The VLAN ID value is set as None(0). Do not change the default value in this field.
11. Click **Next**. Click **Finish**.

    The Data network is now created.

Creating an Oracle Linux Virtual Machine

This section describes creating an Oracle Linux Virtual Machine (VM).
To create an Oracle Linux VM:

1. Download the "Oracle Linux 7.x for x86 64 bit ISO image" from http://edelivery.oracle.com/linux.
   a. Sign in.
   b. Enter **Oracle Linux** in the search field.
   c. From **Select Platform** choose **x86 64 bit** and click **Select**.
   d. Click **Continue**.
   e. Click **Continue** again if the correct version is displayed.
   f. Follow the instructions to complete the download.
2. Open the vSphere Client and create a new VM.
   a. Set **Configuration** to **Typical**.
   b. Enter the **Name and Location**.
   c. Set **Storage** to the appropriate datastore.
   d. Set **Guest Operating System** to **Linux** with **Version Oracle Linux 4/5/6/7 (64-bit)**.
   e. Set **Networks**, with the number of NICs set to **4**. Also set the following networks (all with **Adapter** set to **VMXNET3** and **Connect at Power On** selected):
      - 1: "VM Network"
      - 2: "VM Local"
      - 3. "VM Voip"
      - 4. "VM Data"
   f. Set **Create a Disk** as **Thin Provisioned** at either the Virtual Disk Size or a different size.
   g. On the "Ready to Complete" screen, select **Edit the virtual machine setting before completion** to adjust resources such as Memory and CPUs.
   h. If necessary, select the "Options" tab's **Boot Options** menu item to force entry into the BIOS setup screen.
3. Select **File**, **New**, **'Virtual Machine...'**
   a. Follow the Typical instructions.
   b. Choose **Oracle Linux 4/5/6/7 (64-bit)** for **Guest Operating System**.
   c. Connect the 4 NICs.
   d. Select **Thin Provision** for the datastore.
   e. Click **Finish**.
4. Right-click the new VM and select **Edit Settings...**.

a. Select the **Options** tab.

b. Select **Boot Options** from the left panel.

c. Check the box under **Force BIOS Setup** in the right panel.

d. Click **OK**.

5. Start the VM.
6. 'Open Console' to the VM, and you see the BIOS screen.

a. Select the **Boot** table using the arrow keys.

b. Move the curser over the **CD-ROM Drive** and hit the '**+**' key to move it above the **Hard Drive**.

c. Do not exit BIOS yet.

7. Within the vSphere Client, ensure the VM is selected and click the CD icon in the toolbar.

a. Select **CD/DVD drive 1**.

b. Select **Connect to ISO image on local disk...**.

c. Select the Oracle 7 ISO image downloaded in step 1.

8. In the console, **Save & Exit** from BIOS.

   Installation begins. Follow the instructions provided.

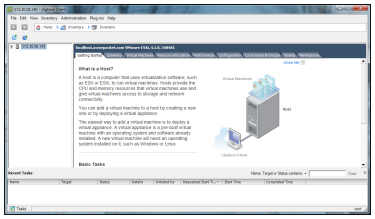
> **Note:**
>
> During the installation, the default configuration of partitions allocates almost the entire disk to the "/home" directory. ISR software is installed by default on the path /opt/isr, requiring more space on the root ("/") directory, or more specifically the "/opt" directory. If the Oracle Linux 7 installer defaults are accepted, the ISR components can very easily run out of disk space and not function properly.

Deploying the Oracle Linux Virtual Machine

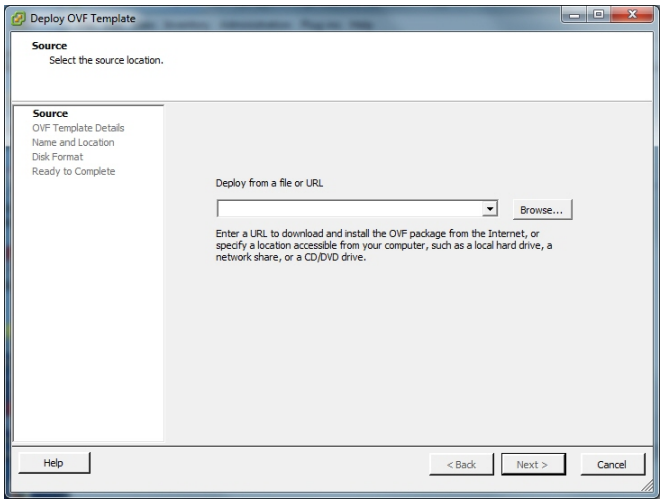
Once you configure your ESXi host and local network, you use the vSphere Client to deploy your Oracle Linux VMs into that network.

To deploy the Oracle Linux VM:

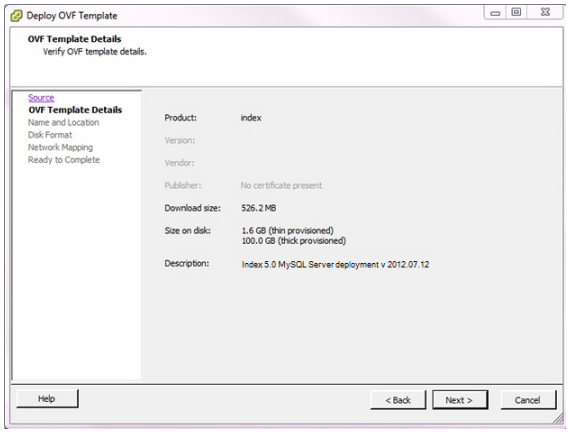
1. Open the vSphere Client application to the Home page.



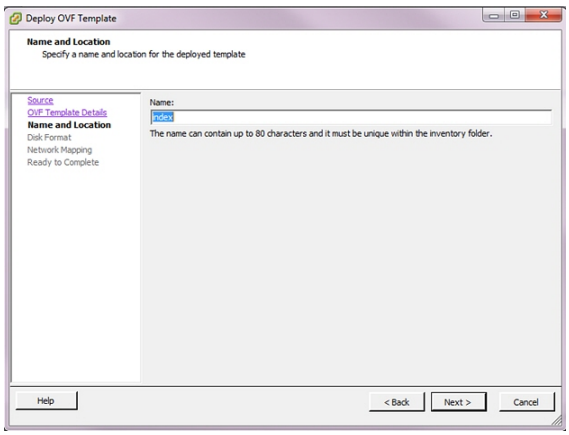
2. From the Main Menu, select **File**, **Deploy OVF Template...**. The following window displays.



3. Click **Browse** and navigate to the directory where you have unzipped the VM.
4. Select the file for the component you are deploying and click **Open**. The following window displays.

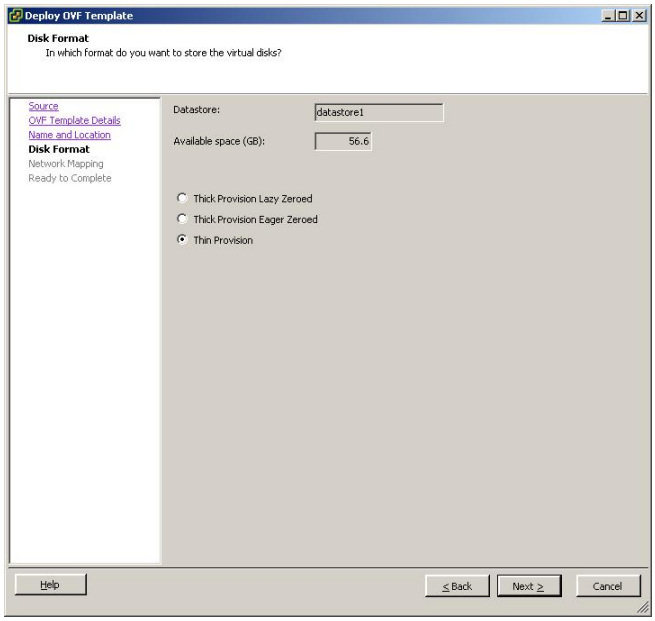


5. Click **Next** in the Deploy OVF Template window. The Name and Location window displays. This field is automatically populated with the name and location of the VM you selected in Step 4.



> **Note:**
>
> You are able to change this name if desired.

6. Click **Next**. The Disk Format window displays.



> **Note:**
>
> If using CIS certified hardware, ensure the datastore name is the datastore you created in the section, "Adding the Datastore to the ESXi Storage Pool". This datastore is larger to accommodate database growth.

7. Select **Thin provision** and click **Next**. The Network Mapping window displays.
8. Map the Source Network column to the Destination Network column if only one physical interface is configured on your ESXi host.
9. Map VM Local to the network you created in "Configuring the Local Network".
10. Click **Next**.
11. Review all selections in the Ready to Complete window and click **Finish**.
12. Click **OK** to close the Deploy OVF Template window.
13. In the left column, click on the VM you are deploying.
14. Press the **Start/Play** icon to power on the VM.
15. To complete the VM installation, configure the network address of the VM using the procedure in "Configuring the VM Network Addresses".

J

Mounting the NFS Server to the RSS

This section describes mounting the NFS server to the RSS.

Set Up the Server

The following is an example of a server setup. Depending on your needs, your configuration may differ slightly. For more information, contact your Oracle representative. For information on configuring Oracle Linux, see Oracle Linux Administrator's Guide.

```
yum install nfs-utils
yum install lsof
Note: Ensure a writeable folder exists to share.
 vi /etc/exports
<local>/<folder> 10.138.217.0/24(rw,no_root_squash)
- no_root_squash allows root user to write without it getting converted to
nfsnobody user/group
systemctl start nfs-server
systemctl enable nfs-server
vi /etc/idmapd.conf
Domain = <domain>
firewall-cmd --zone=public --add-service=nfs
firewall-cmd --permanent --zone=public --add-service=nfs
vi /etc/sysconfig/nfs
# Port rpc.statd should listen on.
STATD_PORT=662
# Port rpc.mountd should listen on.
MOUNTD_PORT=892
vi /etc/sysctl.conf
fs.nfs.nlm_tcpport = 32803
fs.nfs.nlm_udpport = 32769

check no return for:
lsof -i tcp:32803
lsof -i udp:32769
lsof -i :892
lsof -i :662
systemctl reboot
systemctl restart firewalld
firewall-cmd --zone=public --add-port=2049/tcp --add-port=2049/udp --add-
port=111/tcp --add-port=111/udp --add-port=32803/tcp --add-port=32769/udp --
add-port=892/tcp --add-port=892/udp --add-port=662/tcp --add-port=662/udp
firewall-cmd --permanent --zone=public --add-port=2049/tcp --add-
port=2049/udp --add-port=111/tcp --add-port=111/udp --add-port=32803/tcp --
add-port=32769/udp --add-port=892/tcp --add-port=892/udp --add-port=662/tcp
--add-port=662/udp
16 .Verify the share is available (can be done from localhost, better to do
from a non-RSS remote host):
$ showmount -e <nas_ip>
Export list for <client_ip>:
```

```
/home/nfs_share <client_ip>/<prefix>,<e.g.10.10.248.102/24>
```

Set Up the RSS as the Client

This section describes configuring the RSS as the client. For information on configuring Oracle Linux, see Oracle Linux Administrator's Guide.

1. Execute the **yum install nfs-utils** command.
2. Ensure the local folder, `/opt/isr/ArchivedRecordings`, exists and mount the directory using the following command:

   ```
   mount -t nfs -o rw,nosuid <NFS Server IP>:/home/shareDir /opt/isr/
   ArchivedRecordings
   ```

3. Execute the **ls -ltr** command to ensure the directory is mounted properly. The following is a successful example output.

   ```
   drwxrwxrwx. 4 isr isr 83 Dec 2 00:51 ArchivedRecordings
   ```

4. Ensure the directory is a part of an ISR group.

   ```
   chown isr:isr /opt/isr/ArchivedRecordings
   ```

   The ISR is now able to read and write files.

Troubleshooting the RSS on Oracle Linux

- Unable to "showmount" when you execute the following command:

  ```
  $ showmount 11.145.333.05
  clnt_create: RPC: Port mapper failure - Unable to receive: errno
  113 (No route to host)
  ```

  This indicates a problem with the firewalld configuration.

- Unable to write to share.

  ```
  $ touch tmpshare/foo.txt
  touch: cannot touch `tmpshare/foo.txt': Permission denied
  ```

  This indicates an issue with the permissions. Change the mode and ownership of the share on the NFS server with the commands **chmod** and **chown**.

K

Installing Oracle Linux 7 On a Bare-Metal Server

Prior to installing the ISR components, you must have Oracle Linux installed on your hardware. You can either install Oracle Linux via a USB stick or a DVD. This guide documents installing Oracle Linux via a USB.

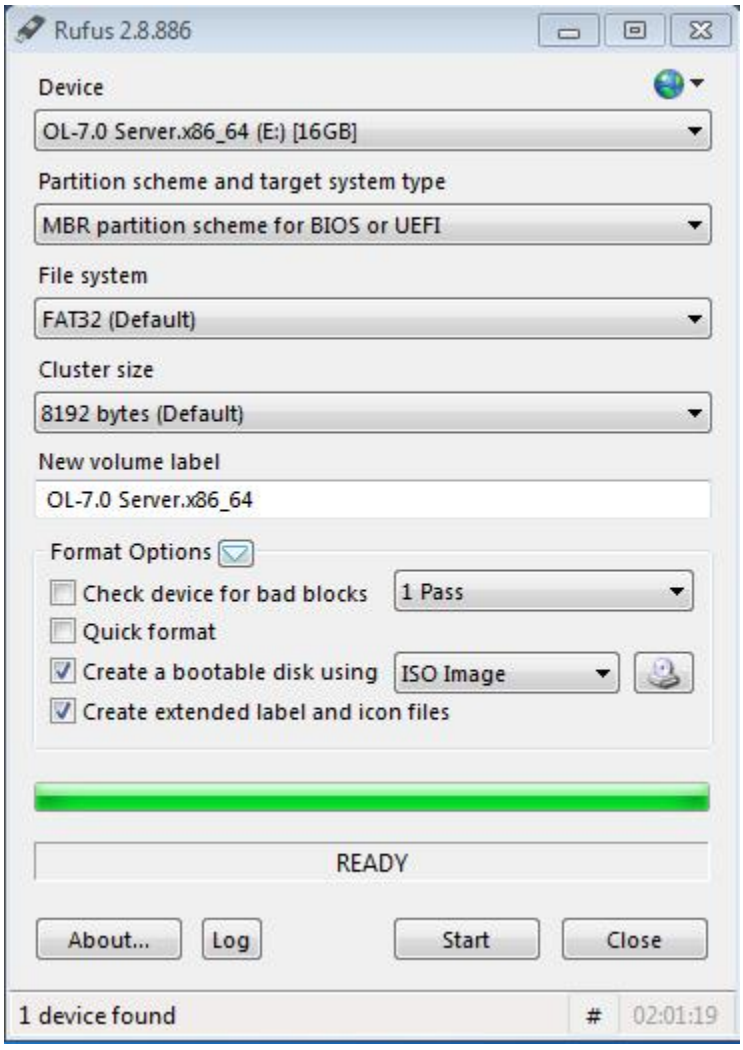
> **Note:**
>
> When you install Oracle Linux via a USB stick, you must have a 16 GB or bigger USB drive.

For a much more comprehensive and thorough description of installing Oracle Linux 7, see https://docs.oracle.com/cd/E52668_01/E54695/E54695.pdf.

> **Note:**
>
> Traditionally CIS hosts are installed as Virtual Machines (VMs) on VMware. For more information on installing VMware, see APPENDIX.

To install Oracle Linux via a USB stick:

1. Download “Oracle Linux 7.X for x86 64 bit ISO image” from http://edelivery.oracle.com/linux.
   a. Sign in.
   b. Enter **Oracle Linux** in the search field.
   c. Select **x86 64 bit** from **Select Platform** and click **Select**.
   d. Click **Continue**.
   e. Click **Continue** if the correct version is displayed.
   f. Follow the instructions provided to complete the download.
2. Create a bootable USB stick that contains the full Oracle Linux 7 ISO image. The following example uses Rufus 2.8 software to create the bootable USB stick.

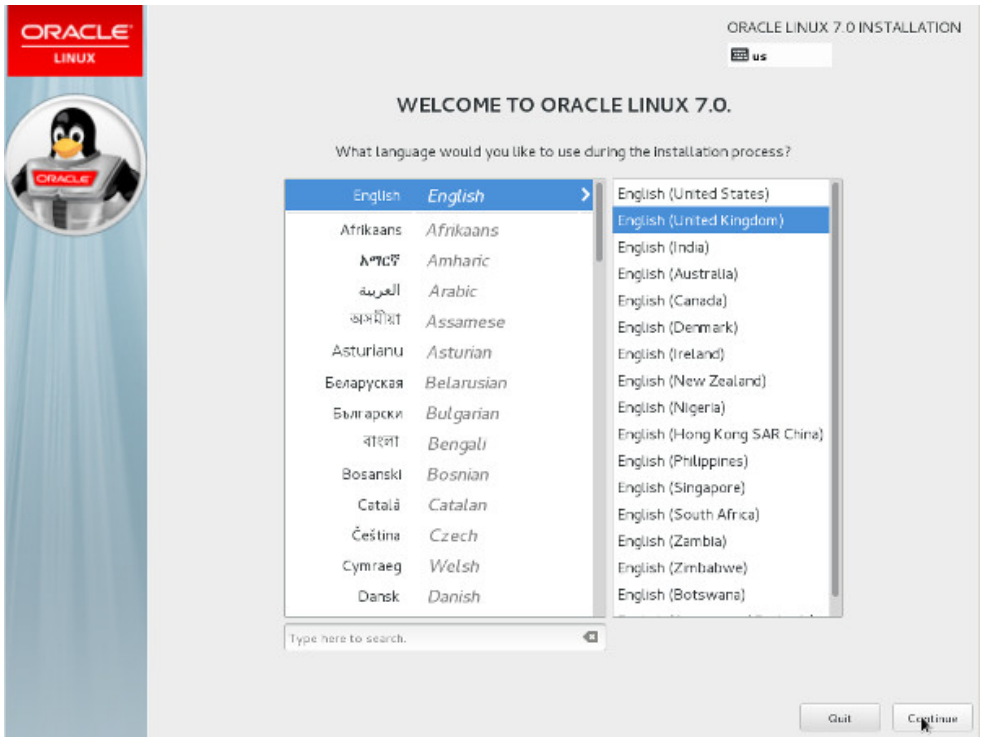


> **Note:**
>
> You can also install Oracle Linux via a DVD by downloading “Oracle Linux 7.1 for x86 64 bit ISO image” from http://edelivery.oracle.com/linux and burning the *.iso image onto a DVD.

3. Insert your bootable Oracle Linux 7 USB drive onto your hardware.
4. Boot the system from the boot image by selecting **Boot from usb** from the boot menu options.

The system locates the boot image file and the boot menu appears.

5. Select **Install Oracle Linux 7.2**, hit **<Enter>**, and follow the Oracle Linux Installer instructions.
6. Select the appropriate language and select **Set keyboard to default layout for selected language**. Click **Continue**.



The Installation Summary screen appears.

> **Note:**
>
> During the installation, the default configuration of partitions allocates almost the entire disk to the "/home" directory. ISR software is installed by default on the path /opt/isr, requiring more space on the root ("/") directory or, more specifically, the "/opt" directory. If the Oracle Linux 7 installer defaults are accepted, the ISR components can very easily run out of disk space and not function properly.

L

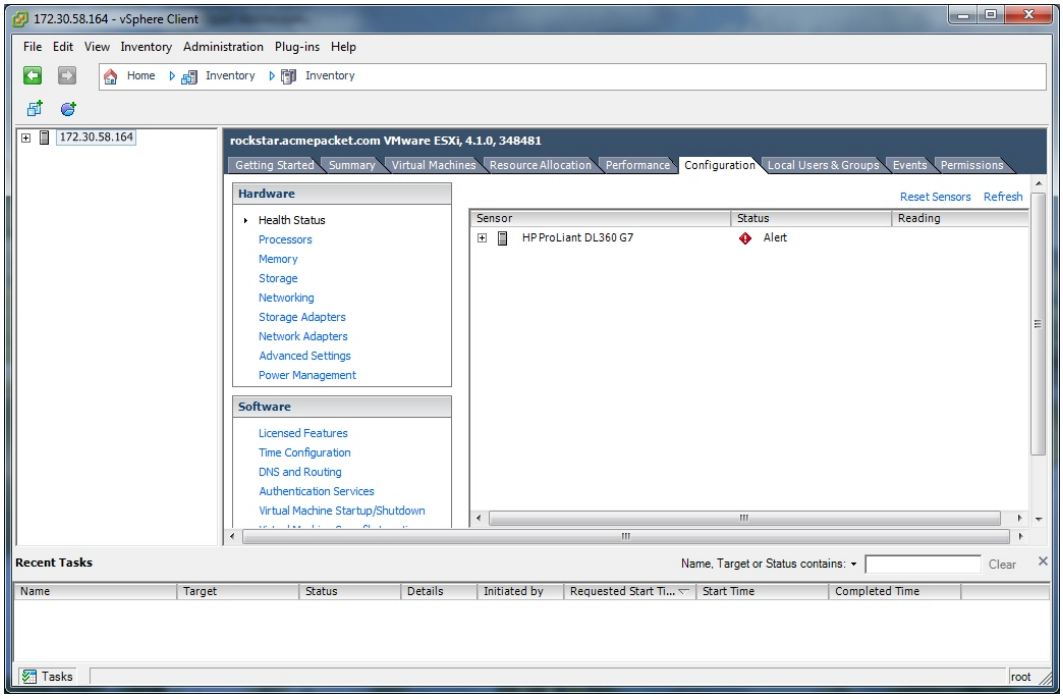
Configuring Automatic Start of the VMs

When all virtual components are installed, Oracle recommends you configure the VMs to start automatically.

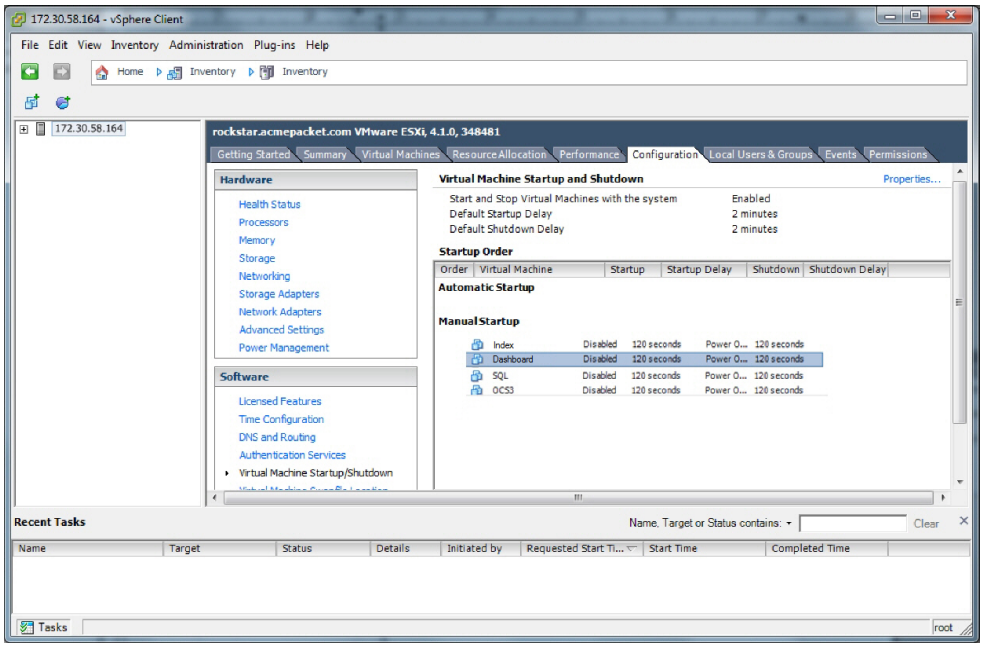
Use the following procedure to configure the virtual machines to start automatically.

To configure the VMs to start automatically:

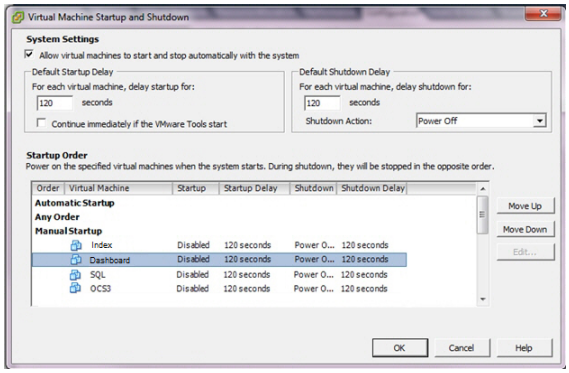
1. Open the vSphere Client application to the Home page.
2. Click on the **Configuration** tab.



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



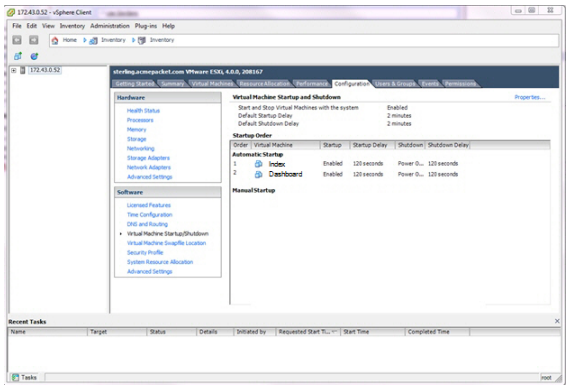
4. In the upper right corner of the window, click **Properties**. The following window displays:



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.



You must continue the ISR installation process by installing the Record and Store Server (RSS). For RSS installation procedures, see Installing the RSS Software.