AVAYA

Migrating from Intuity™ Audix® LX R2.0 to Avaya Aura™ Communication Manager Messaging Federal R6.3

Contents

Contents

Chapter 1: Introduction

Purpose

This document describes the migration process from Intuity Audix server to Communication Manager Messaging.

Intended audience

The information in this book is intended for use by Avaya technicians, provisioning specialists, business partners, and customers.

Document changes since last issue

The following changes have been made to this document since the last issue:

Communication Manager Messaging Release 6.3 Service Pack 3 and above does not support migration from Intuity Audix R1.1 and Intuity Audix R2.0

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Implementation			

Document number	Title	Description	Audience
18-603644	Implementing Avaya Aura® Communication Manager Messaging	Describes the implementation instructions for Communication Manager Messaging.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Migration			
18-603649	Migrating from Intuity™ Audix® LX R1.1 to Avaya Aura® Communication Manager Messaging R6.3	Describes the migration scenario for Communication Manager Messaging.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
18-603650	Migrating from Intuity™ Audix® LX R2.0 to Avaya Aura® Communication Manager Messaging R6.3	Describes the migration scenario forCommunication Manager Messaging.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title	Duration	Delivery Mode
4U00030E	Avaya Aura® Communication Manager and Communication Manager Messaging Embedded Implementation This is a 54-hour course and consists of the following components: • 4U00030E_TH – 18 hours – self-directed theory • 4U00030E_INTRO – 4 hours – instructor-facilitated overview of content • 4U00030E_LAB – 32 hours – instructor-facilitated hands-on lab exercises using remote equipment	54 hours	Self-directed and Instructor-facilitated
5U00060E	Avaya Aura® Communication Manager and Communication Manager Messaging Support This is a 37-hour course and consists of the following components: • 5U00060E_TH – 17 hours – self-directed theory	37 hours	Self-directed and Instructor-facilitated

Course code	Course title	Duration	Delivery Mode
	• 5U00060E_INTRO – 4 hours – instructor-facilitated overview of content • 5U00060E_LAB – 16 hours – instructor-facilitated hands-on lab exercises using remote equipment		

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support web site, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

• To find videos on the Avaya Support web site, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.

• To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

  • Enter a key word or key words in the Search Channel to search for a specific product or topic.

  • Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

  ⊛ **Note:**

    Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Migration overview

Introduction

The migration process from Intuity Audix server to Communication Manager Messaging R6.3 involves the backup and migration of the following types of data:

- Subscribers
- Recorded names
- Personal greetings
- Messages
- Mailing lists
- Class of service records
- Networked computers

> ❗ **Important:**
>
> Communication Manager Messaging Release 6.3 Service Pack 3 and above does not support migration from Intuity Audix R1.1 and Intuity Audix R2.0.

Prerequisites

Installing the latest patch on the Intuity Audix LX R2.0 system

About this task

You need to install the latest `L7043rf+f RFU` patch for the network backup feature to be available on the Intuity Audix LX R2.0 system.

> ❗ **Important:**
>
> You need Avaya Technical Support for this migration to provide this patch. Raise a ticket to Backbone Engineering team (BBE) to request the patch.

Procedure

1. Click Start > Run.

2. Type `telnet` *Intuity Audix LX R2.0 IP address*.

3. Copy file latest `L7043rf+f RFU` patch to `/var/msg/home/tsc/` path.

4. Open a compatible Web browser.

5. In the Address field type the IP address of the Intuity Audix LX R2.0 system.

6. Select **Utilities** > **Software Management** > **Advance Software Installation** > **Choose LAN**.

7. Enter the `/var/msg/home/tsc/` path that contains the patch you need to install.

8. Press **Enter**.

9. Click **Continue this operation without current system backup**.

10. Choose the patch and proceed to install it.

Next steps

Verify the installed patch.

- Select **Utilities** > **Backup Restore** > **Remote storage configuration menus**.

Verifying the number of subscribers on the Intuity Audix LX system

About this task

The Intuity Audix LX system must not exceed 15,000 subscribers.

Procedure

1. Log in to the Intuity Audix LX system using PuTTy.

2. On the command line, type `Fc`.

3. In the Fc window, type `list measurements feature day`.

4. On the **Subscribers** field, ensure that the number in the **Local** field does not exceed 15,000.

FTP server requirement

Ensure that you have an FTP server connected to the network. The system requires the server to transfer backup data.

Determining the announcements installed on the Intuity Audix LX system

Procedure

1. Log in to the Intuity Audix LX server using PuTTy.

2. Open an SSH session.

3. On the command line, type `Fc`.

4. On the Fc window, type `list annc-sets`.

   The system displays the announcements installed on the sever.

5. Note down the announcement sets that are installed on the server.

6. Type `display system-parameters features`.

7. Go to page 3. The **Announcements Sets: System** field displays the custom announcement sets installed on the server.

   ⊛ **Note:**

   Customized announcements are not migrated to the Communication Manager Messaging server.

   🛈 **Important:**

   During migration, install the language files on the Communication Manager Messaging Federal R6.3 server.

Installing RFU

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the Avaya Support site.

Procedure

1. On the System Management Interface Web page, select **Administration**.

2. Click **Messaging**.

   The system displays the Messaging Administration screen.

3. Click **Software Install** from the **Software Management** section.

4. Click **Continue without current system backup**.

   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.

5. Click **Installed selected packages**.

   🛈 **Important:**

   The Communication Manager Messaging processes stop during RFU installation.

   If the RFU modified the Messaging Administration Web page, you must close and reopen this page.

Do not start the messaging software at this time.

Determining the languages installed on the Intuity Audix LX system

Procedure

1. Open a PuTTy window.

2. Log in to the Intuity Audix LX server using an SSH session.

3. On the command line, type `list annc-sets`.

4. Note the language files installed on the server.

   ✴ **Note:**

   During migration, install the language files on the Communication Manager Messaging Federal R6.3 server.

Verifying system-level settings on the Intuity Audix LX server

About this task

Ensure that settings for each of the options on the Intuity Audix LX server and the Communication Manager Messaging R6.3 server match.

Procedure

1. Log in to the Intuity Audix LX server.

2. Note down the settings for each of the following system-level settings on the Intuity Audix LX server and match it to the settings on the Communication Manager Messaging R6.3 server.

System-Parameters (Intuity Audix system)	Messaging Administration (System Management Interface > Administration> Messaging) (CM Messaging system)
activity-log	Under Messaging Administration -> Activity Log Configuration
analog-network	Under Server Administration -> Networked Servers
dial-sequences	Under Messaging Administration -> Dial Sequences
features	Under Messaging Administration -> Features
imapi-options	Under Messaging Administration -> MCAPI Options
limits	Under Messaging Administration -> Limits
outcalling	Under Messaging Administration -> Outcalling Options

System-Parameters (Intuity Audix system)	Messaging Administration (System Management Interface > Administration> Messaging) (CM Messaging system)
sending-restrictions	Under Messaging Administration -> Sending Restrictions
thresholds	Under Messaging Administration -> Thresholds

Chapter 3: Backing up data on the INTUITY AUDIX LX R 2.0 server

Log in to the Intuity Audix LX R2.0 system

Procedure

1. Open a PuTTY window.

2. Select **SSH**.

3. In the **Host Name (or IP address)** field, type the IP address of the INTUITY AUDIX LX R2.0server.

4. Log in as `craft`.

5. For `[ialx2]:craft>`, type **sroot**.

6. For `TERM =[vt100]?`, press **Enter**.

7. For `[ialx2]`, type **Fc**.

   The system displays the Intuity Main Menu screen.

Creating a Test Mailbox on the Intuity Audix LX server

Procedure

1. Before you create the backup, create a test mailbox on the Intuity Audix LX server.

2. In the command line window, to add a subscriber, type **add subscriber**.

   ⊛ **Note:**

   To go to the next page, use the key combination **Control+N**.

3. On page 1, provide basic details for the new subscriber. Confirm the extension range before assigning one to the subscriber.

4. Go to page 2. In the **Permissions** > **Type** field, type `call-answer`. This sets the type of call answer for the subscriber.

5. In **Permissions** > **Announcement Control** field, enter `y` to record names.

6. Save the settings. The test mailbox is added to the list of existing mailboxes.

   To confirm the test mailbox has been added, on the Audix Administration page, type `list subscribers` and press **Enter**. The system displays the list of subscribers.

7. Use the Telephone User Interface (TUI) to record names and greetings. Use another mailbox to send messages to the test mailbox.

Backing up data from the Intuity Audix LX system

Procedure

1. Open a compatible Web browser and type the IP address of the Intuity Audix LX system.
2. Log in as `craft`.
3. On the Legend, select **Backup / Restore** > **Backup**.
4. Enter **Yes** for all data types except Announcements.
5. Click **Start Backup**.

Transferring migration data to the services laptop

Before you begin

Change your laptop network settings to use an IP address on the customers network.

Plug a straight cable into a hub or router port, and then connect to the server using FTP connection to get the tar files.

Procedure

1. On the services laptop, click **Start** > **Run**, and type `cmd`.
2. On the prompt, type `ftp` *IPaddressoftheftpserver*.
3. Type `Binary`.
4. Type `Hash`.
5. Type `ls`. All files in the directory are displayed.
6. Identify the file that you backed up and type `cd` *directoryname* to change the directory.
7. Type `ls` to view files under the main backup file.
8. If you backed up files in a subdirectory, type `cd` *subdirectoryname*.
9. Type `ls` to view the files under the subfolder.
10. Type `get` *tarfilename*. The file is copied to the services laptop.

11. Type **bye** to log out of Unix.

Next steps

Once the files are on the services laptop, change the network settings back to DHCP.

Use a crossover cable and connect to the services port on the Communication Manager Messaging server.

Clearing the ARP cache on the laptop

About this task

Depending on the operating system of your Services laptop computer, you might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. If you enter an IP address and your computer cannot connect, perform the following procedure to clear the cache.

Procedure

1. On your computer laptop, click **Start** > **Run**.

2. Type **command** and press **Enter** to open an MS-DOS command line window.

3. Type **arp -d 192.11.13.6** and press **Enter** to clear the ARP cache in the laptop.

   If the ARP cache does not contain the specified IP address, the message The specified entry was not found appears. You can ignore this message.

4. Type **exit** and press **Enter** to close the command line window.

Chapter 4: Installing Communication Manager Messaging Federal R6.0

System Platform Installation for Communication Manager Messaging Federal R6.3

To install System Platform for Communication Manager Messaging Federal R6.3, see the *Implementing Avaya Aura™ Communication Manager Messaging Federal R6.3*.

To upgrade System Platform for Communication Manager Messaging Federal Release 6.3, see the *Upgrading Avaya Aura® System Platform*.

❗ Important:

Do not install the Communication Manager Messaging Federal solution template R6.3 after installing the System Platform. You must install the solution template only after installing the licenses.

Next steps

Install the licenses for Communication Manager and Communication Manager Messaging Federal using the CDOM Web interface.

Installing the license file

Assigning IP address to the WebLM Server

Procedure

1. Log in to the System Management Interface Web page.

2. On the **Administration** menu, click **Licensing**.

   The system displays the WebLM Configuration Web page.

3. If the customer has a standalone WebLM Server and wishes to point to that server, enter the IP address of the standalone WebLM Server.

> ✴ **Note:**
>
> By default, the system takes the IP address of cdom (console domain of the virtual machine) for the WebLM Server. This is because the WebLM Server is installed on cdom during the installation of System Platform.

Launching WebLM

Before you begin

You are using one of the following Internet browsers:

- Microsoft Internet Explorer, versions 7.*x* and 8.*x*
- Mozilla Firefox, versions 3.5 and 3.6

About this task

System Platform uses Web License Manager (WebLM) to manage its licenses. Use this procedure to launch WebLM from System Platform.

Procedure

1. Click **Server Management** > **License Management**.

2. On the License Management page, click **Launch WebLM License Manager** .

3. When WebLM displays its Logon page, enter the user name and password for WebLM. For initial login to WebLM, the user name is `admin`, and the password is `weblmadmin`. However, you must change the password the first time that you log in to WebLM.

4. Manage the licenses as appropriate.

   For more information on managing licenses in Avaya WebLM, see *Installing and Configuring Avaya WebLM Server* at http://support.avaya.com.

Installing the License file

Before you begin

Procure the license file for the messaging system from https://plds.avaya.com.

Procedure

1. Log in to the System Platform Web console from a Web browser.

2. Click **Server Management** > **License Management**.

   The system displays the License Management screen.

3. Click **Launch WebLM License Manager**.

4. Log in as admin.

5. Change the password.

   The system logs out and you need to re-login using the new password.

6. On the Install License screen, locate the license path.

   ✱ **Note:**

   You can store the license file on an HTTP server or locally on the services laptop computer.

7. Click **Install**.

Next steps

After you install the license file, the WebLM License Manager screen displays the installed license on the License Products screen.

Install license field descriptions

Use this page to install the license file of a product on the WebLM server.

Field/Button	Description
Enter license path	Specify the complete path where you saved the license file.
Browse	Opens the dialog box using which you can select the license file.
Install	Installs the product license file.

Communication Manager Messaging Federal solution template installation

Prerequisite

Install the license for Communication Manager and Communication Manager Messaging Federal.

Refer to the *Implementing Avaya Aura™ Communication Manager Messaging Federal* book to install the Communication Manager Messaging Federal solution template.

Accessing the System Management Interface

About this task

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.

2. In your browser, choose one of the following options depending on server configuration:

   • LAN access by IP address

   To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.

   • LAN access by host name

   If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.

   • Portable computer access by IP address

   To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   ⊛ **Note:**

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   ⊛ **Note:**

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

After successful authentication, the system displays the home page of the Communication Manager SMI.

Obtain the Authentication file

Installing the authentication file

Procedure

1. In the navigation pane, click **Security > Authentication File**.

2. If you have a downloaded copy of the authentication file, select **Install the Authentication file I previously downloaded**.

3. If you have an authentication file either on a local computer or the WebLM server, do one of the following tasks as applicable:

   • Click **Browse** and locate the authentication file.

   • In the **URL** field, type the URL of the authentication file and in the **Proxy Server** field, type the hostname of the WebLM server.

4. Click **Install**.

Downloading the Communication Manager patch

Procedure

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.

2. In the **Miscellaneous** field, click **Download Files**.

3. Select one of the following methods to download the patch:

   • File(s) to download from the machine I'm using to connect to the server.

   • File(s) to download from the LAN using URL.

4. Depending on the download method you select, perform either of the following:

   • Click **Browse** to download the patch.

   • Enter the URL to download the patch and enter the host name and domain name of the proxy server.

5. Click **Download**.

Activating the Communication Manager patch

Procedure

1. In the **Server Upgrade** field, click **Manage Updates**.

2. Select the patch.

3. Click **Unpack**.

4. Click **Activate**.

Logging in to the messaging virtual system

Procedure

1. Open a compatible Web browser.

   Currently only Microsoft Internet Explorer versions 7.0 and 8.0 are supported.

2. In the **Address (or Location)** field, type the IP address or name of the Communication Manager Messaging Federal virtual system and press **Enter**. For example, http://*CMMIPaddress.domain*.com.

   The system displays the Logon screen.

3. Log in as craft.

   The system displays the System Management Interface Web page.

4. Click **Administration** > **Messaging**.

   The system displays the Messaging Administration page. You can administer Communication Manager Messaging Federal application from this page.

Administering the Switch Link

Procedure

1. On the navigation pane, under **Switch Link Administration**, click **Switch Link Admin**..

2. In the **Switch Number** field, type 1.

3. In the **Extension Length** field, select the appropriate length or select **Variable** for variable extensions.

   ✱ **Note:**

   The extension length must match the length assigned to the station on Communication Manager

4. In the **Switch Integration Type** field, enter H.323 as the type of integration between the Communication Manager virtual system and the Communication Manager Messaging virtual system.

5. In the **IP Address Version** field, select **IPv4** or **IPv6**.

6. In the **Link Addresses** > **Switch** field, type the IP address of the Communication Manager virtual system.

7. In the **Messaging Ports** field, enter the number of voice ports the messaging virtual system uses for mailbox connections to the Communication Manager virtual system.

8. In the **Switch Trunks** > **Total** field, enter the value of the total switch trunks for Communication Manager.

   ✱ **Note:**

   You might want to determine the capacity for Messaging at this point. For the procedure, see *Implementing Avaya Aura®Communication Manager Messaging*.

9. In the **Signal Group 1** field, enter the value of the Messaging TCP port as 11720 and the Switch TCP port as 1720. The port numbers have to be different because Communication Manager and Communication Manager Messaging share the same IP address.

10. Click **Show Advanced Options**

   The system displays advanced options that you need to administer.

11. In the **Quality of Service** field, type a value for Call Control Per Hop Behavior (PHB) and Audio PHB or accept the default values. The value you enter for both the fields sets the quality of service level for call control messages and audio streams respectively on networks that support this feature. The value for both the fields must be in the range 0 to 63. The value must match the corresponding number configured for the network region used by the messaging signaling group on the switch.

12. In the **UDP Port Range** field, enter a starting UDP port number for RTP. The end port number is calculated automatically.

13. If you have configured SRTP for messaging, in the **Media Encryption** field, enter the type of Secure Real-time Transport Protocol (SRTP) encryption for messaging.

   ❗ **Important:**

   You need to enable the SRTP feature in the change customer-options form and set the media encryption type in the change ip-codec-set form on Communication Manager.

14. Type the **Passphrase**. This must match the Passphrase administered on the Communication Manager. This field is optional and is to be used only if SRTP encryption has been set on Communication Manager.

15. Click **Save**.

   The system calculates the number transfer ports and displays them in the **Transfer Ports** field.

> ⊛ **Note:**
>
> The number of the H.323 trunks set on the Communication Manager virtual machine server must accommodate the sum of voice ports and transfer ports you administer on the Switch Link screen. This number of H.323 trunks for messaging is in addition to the H.323 trunks that the Communication Manager virtual machine requires for other functions, such as IP telephone connections, faxes, and other data connections throughout the network. The number of H.323 trunks on the Communication Manager virtual machine is listed in the **Maximum Number of H.323 Trunks** field, which is available on the System Parameters Customer Options SAT screen.

Installing RFU

About this task

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure if there are no remote field update (RFU) files on the [Avaya Support site](#).

Procedure

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.

   The system displays the Messaging Administration screen.
3. Click **Software Install** from the **Software Management** section.
4. Click **Continue without current system backup**.

   The system displays the Following packages will be installed... screen with a list of the messaging RFUs.
5. Click **Installed selected packages**.

   > ❗ **Important:**
   >
   > The Communication Manager Messaging processes stop during RFU installation.
   >
   > If the RFU modified the Messaging Administration Web page, you must close and reopen this page.
   >
   > Do not start the messaging software at this time.

Installing the language files for messaging

Procedure

1. On the System Management Web interface, click **Administration** > **Messaging**.

2. Select **Software Management**.

3. Click **Advanced Software Installation**.

4. Click **Install selected package**.

5. Select the announcement sets that need to be installed.

6. Click **Proceed with installation**.

Chapter 5: Migrating backup data to the Communication Manager Messaging Federal server

Copying files to the server

About this task

Use the Web interface of the System Management Interface to copy the latest RFUs, if any, and optional languages, if any, from the Services laptop to the virtual system. The backup tar files need to be copied from the laptop to the Messaging server.

Procedure

1. Select **Administration**.

2. Click **Server (Maintenance)**.

3. In the navigation pane, select **Miscellaneous**, click **Download Files**.

4. Select one of the following:

   - **File(s) to download from the machine I'm using to connect to the server**

   - **File(s) to download from the LAN using URLs**

      a. Enter the name of the proxy server.

5. Click **Browse** to locate the file(s).

6. Click **Download** to copy the files to the media server.

Stopping Communication Manager Messaging

Procedure

1. Select **Administration**, click **Messaging**.

   The system displays the Messaging Administration screen.

2. On the left navigation pane, select **Utilities**, select **Stop Messaging**.

   The system displays the Stop Messaging Software screen.

3. Click **Stop**.

The Stop Messaging Software screen displays the status as messaging begins to stop. When Messaging stops, the screen displays the message, `Stop of voice system completed` at the top of the screen.

Migrating Intuity Audix LX data to Communication Manager Messaging R6.3

Procedure

1. Open a PuTTy window.

2. Ensure that in the **Category** column, **Session** (first on the column) is selected by default.

3. In the **Host Name (or IP address)** field, enter the name of the server name or IP address you want to connect to.

4. In the **Connection** type field, select **ssh**. ssh uses port 22.

5. Click **Open**.

6. Log in using `craft`.

7. Type `statapp -c` to check if the messaging process is up.

8. If the messaging process is up, stop messaging by typing `stop -s Audix`.

9. In the ssh session, enter `/vs/bin/mv_backup_files`, to move the backup tar files from `~ftp/pub` into a temporary folder.

10. Log in to the Communication Manager System Management Interface Web interface.

11. Select **Miscellaneous** > **Messaging Administration**.

12. Select **Start Messaging**. The database conversion begins automatically.

13. In the ssh session window, type `cd /migrate/ialx/log`.

14. Execute `tail -f migration_log`.

Watch the database migration proceed. When this log stops growing and you see a line containing `Executing.ia_restore -f /var/ backup/lx_messaging-1.tar` (multiple tar files are displayed in the log when the backup contains multiple files), the next phase of the migration is underway.

15. Type `control-c` to abort the tail command.

16. Type `tail -f restore_log` to monitor the progress of the database restore and upgrade.

This log also shows the status of transcoding names and messages from Code excited linear prediction (CELP) to G.711. After transcoding is complete, the database is upgraded to the

current release. When this log stops growing and you see a line with the phrase `Executing /mtce/scripts/restore/S10checkfs.postpost`, the restore is finished and the migration continues.

17. Type **control-c** to abort the tail command.

18. Type **tail –f migration_log** and you can monitor the final phase of the migration.

    When this log stops growing and you see a line containing `The migration has completed`, it means migration is finished and messaging starts automatically.

19. Type **control-c** to abort the tail command.

    ❗ Important:

    You might need to wait a few minutes before Messaging starts automatically.

Testing if Migration is successful

Procedure

1. Log in to the Communication Manager System Management Web Interface.

2. Select **Administration** > **Messaging**.

3. Select **Messaging Administration** > **Subscriber Management**.

4. Click **Manage** on the Local Subscribers row to find the migrated test mailbox listed as Local Subscribers.

5. Confirm what data has been successfully migrated. For example, call the test mailbox extension to listen to the greeting that you created. Furthermore, you can listen to messages on the mailbox that you created while creating the test mailbox.

    ❗ Important:

    During migration, most of the system administration data is not migrated. Avaya recommends that you revalidate the system administration after the migration is complete. For example, you must revalidate System-Parameters Features, System Out calling.

Restarting the system

Procedure

1. Open a compatible Internet browser on your computer.

    Currently System Management Interface only supports Microsoft Internet Explorer 7.0, 8.0 and Mozilla Firefox 3.6 and above.

2. Enter the IP address of the Communication Manager virtual machine.

3. On the System Management Interface Web page, select **Administration**.

4. Click **Server (Maintenance)**.

5. In the navigation pane, click **Server** > **Shutdown Server**.

   The system displays the Shutdown This Server Web page.

6. Select **Immediate Shutdown**.

7. Select the **Restart server after shutdown** check box.

8. Click **Shutdown**.

   The Communication Manager virtual machine restarts. The server takes approximately 10 to 15 minutes to restart.

Index