Novell Conferencing

1.0

www.novell.com

SERVER INSTALLATION GUIDE

October 20, 2007

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

ICEcore*

Contents

About This Guide 5

1 System Overview 7

1.1 System Components . . . 7
1.2 Cluster Architecture . . . 8

2 Installation Procedures 9

2.1 Installation Prerequisites . . . 9
2.1.1 Conferencing Server Requirements . . . 9
2.1.2 Network Requirements . . . 10
2.1.3 Firewall Requirements . . . 10
2.1.4 DNS and Hostname Requirements . . . 10
2.1.5 VoIP Requirements . . . 11
2.1.6 Load Balancer Requirements . . . 11
2.2 Security . . . 12
2.3 Installation Overview . . . 13
2.3.1 Conferencing Cluster Components . . . 13
2.3.2 Conferencing Client Components . . . 13
2.4 Preparing for Installation . . . 14
2.5 Installing the Conferencing Server . . . 15
2.6 Review the Conferencing Cluster Components Installation Process . . . 20
2.6.1 Initial Installation . . . 20
2.6.2 System Administration E-mail Configuration (Optional) . . . 20
2.6.3 Configuring LDAP Synchronization (Optional) . . . 21
2.6.4 Mailer Configuration (Optional) . . . 22
2.6.5 Database Backup Configuration (Optional) . . . 22
2.6.6 Meeting Archive and Document Sharing Repository Configurations (Optional) . . . 23
2.6.7 Chat Audit Log Configuration (Optional) . . . 24
2.6.8 Event Logging Configuration (Optional) . . . 25
2.6.9 Port Forwarding (Optional) . . . 25
2.6.10 XML Router Security . . . 26
2.6.11 Template Configuration (Optional) . . . 26
2.6.12 Summary of Configuration . . . 26
2.7 Starting and Stopping the Cluster . . . 26
2.8 Conferencing Administration Console . . . 27
2.9 Conferencing Client Installation . . . 27
2.9.1 Building the Conferencing Client RPM . . . 27
2.9.2 Installing the Conferencing Client . . . 28
2.9.3 Installing the Pidgin Instant Chat Client . . . 28

3 Reconfiguring and Upgrading 29

3.1 Backing Up and Restoring the Database . . . 29
3.2 Reconfiguring Conferencing Hosts . . . 30
3.3 Upgrading the Conferencing Client . . . 30
3.4 Upgrading the Conferencing Servers . . . 30
3.5 Starting and Stopping Conferencing Services . . . 31

4 Modifying Template Files **33**

4.1 Modifying the Meeting Invitation Template . . . 33
4.2 Using IF Statements . . . 35
4.3 Modifying the Meeting Summary E-mail Template . . . 35
4.4 Modifying the New User Greeting E-mail Template . . . 36

A Configuring ssh(1) private/public Key Authentication **37**

A.1 Generating a Private/Public Key Pair . . . 37
A.2 Configuring the ssh Key Agent . . . 38
A.3 Adding the Public Key to the Root User's Set of Authorized Keys . . . 38

B Editing the global-config File **39**

B.1 Assigning Services to Nodes . . . 39
B.2 Configuring Web Services . . . 41
B.3 Configuring the Mailer . . . 41
B.4 Using Port Forwarding . . . 41

C Editing the dialing.xml File **43**

D Updating Meeting Invitation Web Pages **45**

E LDAP User Authentication **47**

About This Guide

This guide covers the installation and initial configuration of the Conferencing software component of Novell Teaming + Conferencing. The term “Conferencing” in this guide applies to all versions of Conferencing unless otherwise noted.

Audience

This guide is intended for administrators or IT personnel in charge of installation.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the Conferencing User Guide, visit the Novell Web site (http://www.novell.com/documentation/team_plus_conf/).

Additional Documentation

You may find more information in additional Conferencing documentation:

- Conferencing Help system
- Conferencing Quick Start Guide
- Conferencing User Guide
- Conferencing Operations Guide

Contents of this Manual

This manual provides information about the following:

- System Overview
- Installation Procedures
- Reconfiguring and Upgrading
- Modifying Template Files
- Various Appendices

Document Conventions

This manual uses the following conventions:

A greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX, should use forward slashes as required by your software.

What you see	What it means
Click the *Add toolbar* item. Click the *Getting Started* link. Click the *Add Document* menu item. Click *Close*.	References to toolbar items, links, menu items, and buttons are presented in *italic* font.
Type `status`, then press Enter. Open the `ManagerGuide.pdf` file.	Text that you must type and file names are presented in `Courier` font.

System Overview

1

This chapter provides an overview of the Conferencing architecture and a description of the system components.

This chapter includes the following sections:

- Section 1.1, “System Components,” on page 7
- Section 1.2, “Cluster Architecture,” on page 8

1.1 System Components

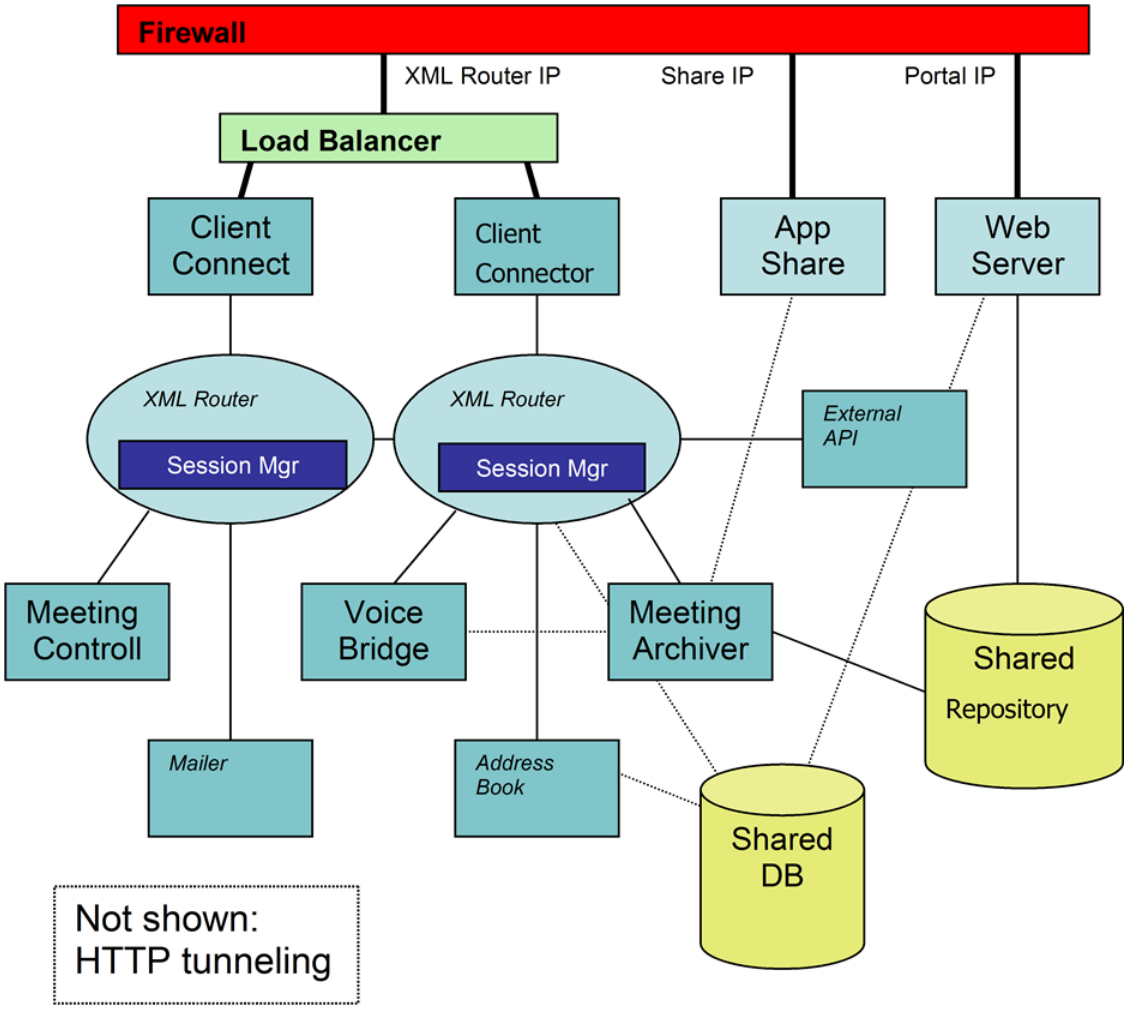
The Conferencing Server is a highly modular suite of components that you can configure to run on one or more servers. Each component provides a core service to the system through a well-defined XML API. Since all communication occurs over an XML transport, the allocation of components to physical hardware is very flexible.

The system components are as follows:

- XML Router - Routes XML data and APIs calls between other components.
- Client Connector - Handles incoming connections from desktop clients and establishes user sessions with the Session Manager component.
- Session Manager - Tracks connected users and related presence information, and allows users to exchange instant messages.
- Meeting Controller - Manages in-progress meetings and dispatches meeting events to meeting participants.
- Notification Server - Sends notification e-mails and IM messages on behalf of the Meeting Controller and Schedule Server components.
- Address Book - Stores and retrieves community/personal address books and system profile information.
- Schedule Server - Stores and retrieves meeting schedule, options, and participant information.
- Voice Bridge - Controls telephony resources, connects calls to conferences, makes outbound calls, and provides telephone access to meeting features.
- Meeting Archiver Server - Collects audio, application/desktop shared images, and chat sessions to create Macromedia Flash-based meeting archives, which are stored in a web accessible repository.
- App Share Server - Forwards application shared data from meeting presenter to meeting participants and manages remote control access to the presenter’s desktop.
- Invitation Web Service - Joins participants to meetings when they use the invitation URL.
- External Web Service - Provides a web service API for external parties as needed for integration with existing service provider systems.

1.2 Cluster Architecture

A cluster is a set of components providing services to a community of users. The following diagram illustrates the architecture of an example cluster (this is not a database fail-over cluster). This example displays a multiple server configuration.



Installation Procedures

2

The following chapter describes the installation requirements and procedures:

- Section 2.1, “Installation Prerequisites,” on page 9
- Section 2.2, “Security,” on page 12
- Section 2.3, “Installation Overview,” on page 13
- Section 2.4, “Preparing for Installation,” on page 14
- Section 2.5, “Installing the Conferencing Server,” on page 15
- Section 2.6, “Review the Conferencing Cluster Components Installation Process,” on page 20
- Section 2.7, “Starting and Stopping the Cluster,” on page 26
- Section 2.8, “Conferencing Administration Console,” on page 27
- Section 2.9, “Conferencing Client Installation,” on page 27

2.1 Installation Prerequisites

The following are requirements for the Conferencing installation unless noted as optional.

2.1.1 Conferencing Server Requirements

NOTE: You need to install the `libneon` and `libpq` libraries before running the installer. On SLES 10, these libraries are not installed on the system by default.

- **SUSE Enterprise Server 10 or Red Hat Enterprise Server 4** - Each Conferencing server host must be running SUSE Enterprise Server 10 or Linux.
- **PostgreSQL** - The PostgreSQL database server must be installed on one of the Conferencing hosts. A default Linux installation does not install the PostgreSQL database server. You must choose to install it explicitly. When installing the PostgreSQL software, select the `postgresql` server software. Once you have installed the PostgreSQL software, the Conferencing installation initializes the database.

  NOTE: Ensure that you do not have any existing PostgreSQL databases on any of the servers in the Conferencing cluster.

- **Time synchronization** - All Conferencing hosts must be time synchronized and the system time zones must all be consistent. To maintain accurate system time, you can configure reliable time servers in `/etc/ntp.conf` and `/etc/ntp/step-tickers` (see the `ntpd(1)` man page).
- **Emacs** - During the installation, you have the opportunity to edit both the new user and invitation templates. You can do this by editing the templates and then importing them, or by using emacs on an install host. If you are going to use emacs on an install host, ensure that emacs has been installed, as it may not be part of the default Linux installation and must be explicitly installed.
- **License key** - The installation script asks you to provide a license key for the Conferencing Server.

2.1.2 Network Requirements

IP addresses - You must define at least three IP addresses that are used by Conferencing clients to connect to Conferencing services. The services that Conferencing clients connect to are the XML router, web portal and desktop/app share server. The XML router and web portal each require a single IP address, and the desktop/app share services need an IP address for each instance. If any of the Conferencing clients are outside your firewall, the IP addresses must be externally accessible.

See DNS and Hostname Requirements below.

2.1.3 Firewall Requirements

- **XML router IPs** - IP addresses have ports 1270, 443, and 80 open.
- **Desktop/Application Sharing IPs** - IP addresses have ports 1270, 443, and 80 open.
- **Web portal IPs** - You must have port 80 open.

  NOTE: Port 443 must be open if you have enabled SSL/TLS. Then, you may choose to block port 80 to disable unencrypted access.

- **DMZ Configuration (optional)** - If you choose to run Conferencing services in the DMZ and you are concerned about database security, you can run the database inside the firewall. XML routers, Address Book and web portal HTTP servers connect to the database using port 5432.

2.1.4 DNS and Hostname Requirements

IMPORTANT: All hostnames currently need to be lowercase.

- **Three hostnames** - The XML router, desktop/application sharing, and web portal IP addresses each require a hostname resolvable by Conferencing clients.

  A Conferencing server requires 3 IP addresses and host names for proper operation of all services:

  a. Typically one address is given a friendly name and used for the XML router service--this is the service to which the Conferencing client initially connects.

  b. The second address has "`-share`" appended to the base name and is used for the desktop sharing components.

  c. The third address has "`-portal`" appended to the name and is used for web services and client download.

- **Fully qualified domain name** - The web portal host requires a fully qualified domain name. For example, www.mycompany.com or webportal.conferenceinstall.com
- **Unique hostnames (multiple machines)** - Multiple-machine Conferencing installations require each machine to have a distinct host name. These host names do not need to be resolvable outside the local network.

To Add IP Addresses to a SUSE Enterprise Server:

1. Open *YaST Administrator Settings,* select *Network Devices*, and then select *Network Card*.
2. Click *Next*, select the desired network interface and click *Edit*.
3. Click *Advanced*, and select *Additional Addresses* from the drop-down list.
4. Click *Add* and enter the IP addresses and netmasks appropriate for your network.

2.1.5 VoIP Requirements

The client connects to a gateway server using the IAX protocol and first attempts to UDP over port 4569. If that fails, it tries a TCP connection on port 443. The VoIP client does not attempt to do HTTP tunneling. The gateway then uses SIP to communicate with the voice bridge itself. The SIP traffic is sent to the voice bridge server itself, while all voice data is streamed via RTP to the NMS board.

To configure VoIP, you need to specify two additional IP addresses during server installation. One is for the gateway process and must be exposed to the external network; the second is assigned to the NMS board.

WARNING: VoIP is not encrypted.

2.1.6 Load Balancer Requirements

Multi-host installations only:

- A load balancer is only required when either multiple web portal hosts or multiple XML router hosts are used.
- Conferencing clients need to maintain an open connection while a user is signed on.
- Connections to the web portal should be sticky. For example, if a host is assigned to a web portal IP address, that host should continue to access the assigned web portal IP address.

2.2 Security

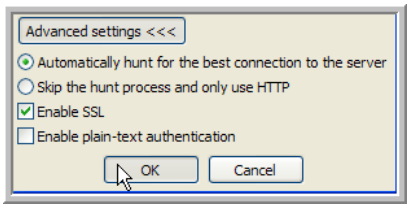
We recommend that you configure the length of any Conferencing PINs (Invitee PINs and Meeting IDs) to six characters or more for increased security, see the Conferencing Online Help, User Guide or Operations Guide for how to set the length of the Conferencing PINs in your Administration Policies.

WARNING: VoIP is not encrypted.

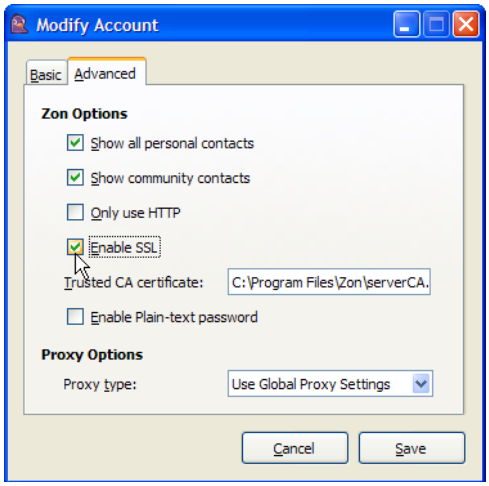
Enabling SSL

NOTE: The communication channel between the recording server and the Conferencing server is not encrypted.

To ensure the security of your Conferencing services, you need to enable SSL, which is not enabled by default. You can enable this in the client *Sign On* window under *Advanced Settings*.



For Pidgin, select the *Enable SSL* option under the *Advanced* tab in the *Modify Account* window.



2.3 Installation Overview

To install Conferencing, you need to install the following:

- Section 2.3.1, “Conferencing Cluster Components,” on page 13
- Section 2.3.2, “Conferencing Client Components,” on page 13

2.3.1 Conferencing Cluster Components

To install or upgrade the Conferencing Cluster Components:

1. Verify the Installation Prerequisites are in place.
2. Unzip/untar the file.
3. Unpack the files.
4. Backup the sitescape-conferencing directory (if applicable).
5. Install the software using the installation script, which is comprised of:
   - Initialization of the database server
   - Installation and configuration of the XML router services
   - Installation and configuration of the web portal services
   - Installation and configuration of the application/desktop sharing
   - Installation and configuration of e-mail configuration
   - Installation and configuration of Backup, Meeting Archive, Logging and Port Forwarding
   - Modification of the template files

2.3.2 Conferencing Client Components

To install and administer communities and new users:

1. Launch the Administration Console.
2. Create a New Community with the Administration Console (see the “Conferencing Operations Guide” for more information).
3. Install a Conferencing Client.
4. Use the Conferencing Client to create users and perform other administrative tasks.

2.4 Preparing for Installation

IMPORTANT: The following are important pre-installation steps.

Install “neon”, “postgresql” and “postgresql-server” packages

These packages should be available from the original installation media or from the online update. Install dependencies as required.

Using ssh(1)

For multi-machine installations, we strongly recommend that you configure `ssh(1)` public/private key authentication between the system administrator on the staging host and the root user on the Conferencing hosts. Otherwise, you need to enter the root password for the Conferencing hosts numerous times during the installation. See Appendix A, “Configuring ssh(1) private/public Key Authentication,” on page 37.

Unpacking the Files

You should have the Conferencing distribution file in a compressed `.tar` archive named `sitescape-conferencing-<version>.tar.gz` (where <version> is the version of the system you received). You can extract the contents of the tar file on an installation-staging host (you can use one of the Conferencing hosts) using:

```
tar -zxvf sitescape-conferencing-<version>.tar.gz
```

Unpack the distribution compressed tar archive (`sitescape-conferencing-<version>.tar.gz`) on a Linux staging machine (you can use one of the cluster nodes). After unpacking, you should see the following files and directories in the `sitescape-conferencing` directory:

```
sitescape-conferencing/utils.sh
sitescape-conferencing/control-cluster.sh
sitescape-conferencing/install-cluster.sh
sitescape-conferencing/config-cluster.sh
sitescape-conferencing/cluster-prototype/install.sh
sitescape-conferencing/cluster-prototype/check-config.sh
sitescape-conferencing/zon-svr-<svrversion>.tar.gz
sitescape-conferencing/cluster-prototype/installers_<version>.tar.gz
sitescape-conferencing/cluster-prototype/global-config
sitescape-conferencing/cluster-prototype/invitation-template.default
sitescape-conferencing/cluster-prototype/meeting-summary-
template.default
sitescape-conferencing/cluster-prototype/new-mtgarchive-
template.default
sitescape-conferencing/cluster-prototype/new-user-template.default
sitescape-conferencing/cluster-prototype/voiceconfig.xml
sitescape-conferencing/cluster-prototype/dialing.xml
sitescape-conferencing/cluster-prototype/ldap.xml.in
```

Backup the Directory

After configuring the cluster (see following sections), backup the `sitescape-conferencing` directory, as it is the location where future upgrades and re-configurations are performed.

You are now ready to install and configure the Conferencing software.

2.5 Installing the Conferencing Server

Perform this procedure after you extract the Conferencing server distribution file (`sitescape-conferencing-<version>.tar.gz`) on an installation-staging host (you can use one of the Conferencing hosts):

1. Open the `sitescape-conferencing` directory
2. Run: `./install.sh`

   NOTE: You need to install the `libneon` and `libpq` libraries before running the installer. On SLES 10, these libraries are not installed on the system by default.

3. The installation script prompts you for the configuration information, license key and then installs the software.

   NOTE: If you do not have the correct ports open, disable the firewall during installation (see Section 2.1.3, "Firewall Requirements," on page 10).

During the installation process, you are asked whether you want to modify the associated templates. See Chapter 4, "Modifying Template Files," on page 33.

Running the Installer on SLES:

1 Unpack the distribution compressed tar archive (`sitescape-conferencing-<version>.tar.gz`):

```
#/ tar -zxf filename.tar.gz
```

2 Copy the license key to the `sitescape-conferencing` directory that contains `install.sh` (the directory files exist after you unpack the compressed tar archive):

```
# cp license_key.xml
```

3 Change directories to the `sitescape-conferencing` directory that contains `install.sh`:

```
# cd sitescape-conferencing
```

4 If you plan on running Active Directory LDAP Synchronization, you need to edit the `ldap.xml.in` file in the `cluster-prototype` directory (see Appendix E, "LDAP User Authentication," on page 47):

4a Open the `ldap.xml.in` file.

4b Comment out the `eDirectory` attributes section and uncomment out the `ActiveDirectory` attributes section.

4c Save the file.

5 Run the installer:

```
# ./install.sh
```

6 The installer prompts you to accept the license (the default is `N`), enter `Y`:

```
Accept License (Y/N): Y
```

7 The installer prompts you to proceed, enter `Y`:

```
Ready to proceed (Y/N): Y
```

8 The installer prompts you to select whether this is a new install or an upgrade (the default is `N`), enter `Y` to run a new installation:

```
New Install or upgrade (Y/N): Y
```

9 The installer prompts you to enter a name for the install (the default is `ourzon`), enter the name you want to use for the install:

```
Choose a name for Install: <enter_install_name>
```

NOTE: The name of the installation cannot contain spaces, but can contain any combination of ASCII and alphanumeric characters.

10 The installer prompts you to initialize the database for a new install (the default is `Y`), you must enter `Y` here for a new installation or the database service does not start:

```
Initialize Database for new install (Y/N): Y
```

NOTE: Ensure that you have created the `PostgreSQL` database prior to installation. Refer to the Installation Prerequisite section for additional information.

IMPORTANT: If your upgrading and have an existing database, you can enter `N`. For new installations, always enter `Y`.

11 The installer prompts you to enter a password for the administrator user (this should be set for security reasons since the Administrator account needs to be a controlled environment):

```
Password for Administrator User: <enter_password>
```

12 The installer prompts you whether to enable SSL/TLS security (the default is `Y`):

```
Should System enable SSL/TLS security (Y/N): <enter_value>
```

NOTE: SSL= Secure Socket Layer and TLS= Transport Layer Security. If you enable SSL/TLS security, the user and password information is encrypted on the network and shows up as hashes in the database table. If you select `N`, password information is still hashed but everything else is readable.

13 The installer prompts you to enter the path and name of the certificate for the XML router (the default is `/upt/lic/conf/server.pem`), enter the default certificate:

```
Insert path and name of certificate for XML router:
/upt/lic/conf/server.pem
```

IMPORTANT: You must use the default XML router certificate at this time for the Conferencing server to function correctly.

14 The installer prompts you to enter the path and name of the certificate for the Web Server.

```
/upt/iic/conf/webserv.pem
```

IMPORTANT: You must use the default Web Server certificate at this time for the Conferencing server to function correctly.

15 The installer prompts you to identify whether you are installing on a Single-Host or a Multiple-Host installation (the default is `Y`), if you have multiple servers then select `N` and the installer will prompt you to enter the additional information for a Multiple-Host installation:

```
Are you installing on single host (Y/N): <enter_value>
```

16 The installer prompts you to enter the IP address for thew XML router:

```
What is IP address for XML router?: <enter_ip_address>
```

NOTE: The installer attempts to ping hosts and IP addresses to ensure that they are running and reachable. If an intervening firewall is filtering out ICMP messages or the host is intentionally down, it may not appear to be reachable even though the entered value is valid.

17 The installer prompts you to enter the hostname of the conferencing server:

```
What is hostname that conferencing clients will use to connect to
XML?: <enter_value>
```

18 The installer prompts you to enter the IP address for the Web Portal:

```
What is IP address for Web Portal?: <enter_ip_address>
```

19 The installer prompts you to enter the portal name:

```
What is Web Portal name URL's?: <enter_portal_name>
```

NOTE: For example, `Renaldo.homedns.org-portal`.

---

20 The installer prompts you to enter the IP address for the App-Share:

```
What is IP address for App-Share?: <enter_ip_address>
```

21 The installer prompts you to enter the Hostname for the desktop App-Share:

```
What is Hostname for desktop app-share: <enter_hostname>
```

NOTE: For example, `renaldo.homedns.org-share`.

---

22 The installer prompts you to select whether you are running Conferencing Bridge (the default is `N`), if you enter `Y`, the installer will prompt you to enter the bridge information:

```
Are you running Conferencing Bridge? (Y/N): <enter_value>
```

23 The installer prompts you to select whether you want to change the system administration e-mail configuration (the default is `N`), if you enter Y, the installer will prompt you to enter the new e-mail address configuration information instead of using default configuration:

```
Do you want to change system admin email configuration? (Y/N):
<enter_value>
```

NOTE: See Section 2.6.2, “System Administration E-mail Configuration (Optional),” on page 20.

---

24 The installer prompts you to verify what you have entered up to this point (enter `Y` if the information is correct or enter `N` if you need to make any changes):

```
Is this correct (Y/N): <enter_value>
```

NOTE: The questions from Step 25 through Step 38 all have default values of `N`.
If you select `Y`, the installer will prompt you to enter additional values and information to customize your server configuration. You can customize your configuration for information like how long a file is archived, with a different header look, the way summaries are viewed, security settings, etc. If you use the defaults and decide to customize your server configuration later, you have to re-run the installer to change these values.

---

25 The installer prompts you to select whether you want to change the mailer configuration:

```
Do you want to change mailer config? (Y/N): <enter_value>
```

NOTE: See Section 2.6.4, “Mailer Configuration (Optional),” on page 22.

---

26 The installer prompts you to select whether you want to change the database backup configuration:

```
Do you want to change DB backup config (Y/N):
```

NOTE: See Section 2.6.5, “Database Backup Configuration (Optional),” on page 22.

---

27 The installer prompts you to select whether you want to change the meeting archive maintenance configuration:

```
Do you want to change meeting archive maint? (Y/N): <enter_value>
```

NOTE: See Section 2.6.6, "Meeting Archive and Document Sharing Repository Configurations (Optional)," on page 23.

28 The installer prompts you to select whether you want to change the document share repository maintenance configuration:

```
Do you want to change doc share repository maint config? (Y/N):
<enter_value>
```

NOTE: See Section 2.6.6, "Meeting Archive and Document Sharing Repository Configurations (Optional)," on page 23.

29 The installer prompts you to select whether you want to change the audit logs:

```
Do you want to change Audit logs? (Y/N): <enter_value>
```

NOTE: See Section 2.6.7, "Chat Audit Log Configuration (Optional)," on page 24.

30 The installer prompts you to select whether you want to change the logging configuration:

```
Do you want to change logging config? (Y/N): <enter_value>
```

NOTE: See Section 2.6.7, "Chat Audit Log Configuration (Optional)," on page 24.

31 The installer prompts you to select whether you want to change the real-time call user-reservations logs:

```
Do you want to change real-time call user-reservations logs? (Y/N):
<enter_value>
```

NOTE: See Section 2.6.8, "Event Logging Configuration (Optional)," on page 25.

32 The installer prompts you to select whether you want to change the security configuration:

```
Do you want to change security configuration? (Y/N): <enter_value>
```

NOTE: See Section 2.6.10, "XML Router Security," on page 26.

33 The installer prompts you to select whether you want to change the LDAP configuration:

```
Do you want to change LDAP (Y/N): <enter_value>
```

NOTE: See Section 2.6.3, "Configuring LDAP Synchronization (Optional)," on page 21. For Active Directory LDAP Synchronization, you need to complete Step 4 on page 15 first.

34 The installer prompts you to select whether you want to change the system e-mail header configuration:

```
Do you want to change system email header config? (Y/N):
<enter_value>
```

35 The installer prompts you to select whether you want to change the e-mail template:

```
Do you want to change Email template? (Y/N): <enter_value>
```

36 The installer prompts you to select whether you want to change the meeting invitation template:

```
Do you want to change Meeting invite template? (Y/N): <enter_value>
```

37 The installer prompts you to select whether you want to change the summary e-mail template:

```
Do you want to change Summary email template? Y/N): <enter_value>
```

38 The installer prompts you to select whether you want to change the meeting archive e-mail template:

```
Do you want to change Meeting archive email template? (Y/N):
<enter_value>
```

39 The installer lists all the services running on the local host, hit the `ENTER/RETURN` key to continue:

```
All services running on local host
```

40 The installer lists all the configuration information, hit the `ENTER/RETURN` key to continue:

```
View Config
```

41 The installer prompts you to select whether you are satisfied with the configuration (the default is `Y`), enter `N` to change the configuration:

```
Satisfied with config (Y/N): <enter_value>
```

42 The installation begins and uses whatever values you entered during the installation setup.

43 The installation completes and displays information stating the services that should be running.

Initial Address Book Configuration (Synchronization)

If you are using LDAP synchronization, execute `/opt/iic/bin/ldap-sync.sh <portal-server-hname>` to perform the initial synchronization.

NOTE: After starting the server, wait 20 seconds or so before executing this command; if you do not get an XML message back, you probably did not wait long enough.

This script displays an XML message if it fails (the fault message is clearly visible); if it succeeds, the XML data contains a single number that is the number of users actually synchronized. You can run this script manually as needed, or configured to run periodically using `cron` (the default setting is for it to run daily).

2.6 Review the Conferencing Cluster Components Installation Process

The installation script takes you through the following to install and configure a new Conferencing Server instance:

- Section 2.6.1, “Initial Installation,” on page 20
- Section 2.6.2, “System Administration E-mail Configuration (Optional),” on page 20
- Section 2.6.3, “Configuring LDAP Synchronization (Optional),” on page 21
- Section 2.6.4, “Mailer Configuration (Optional),” on page 22
- Section 2.6.5, “Database Backup Configuration (Optional),” on page 22
- Section 2.6.6, “Meeting Archive and Document Sharing Repository Configurations (Optional),” on page 23
- Section 2.6.7, “Chat Audit Log Configuration (Optional),” on page 24
- Section 2.6.8, “Event Logging Configuration (Optional),” on page 25
- Section 2.6.9, “Port Forwarding (Optional),” on page 25
- Section 2.6.10, “XML Router Security,” on page 26
- Section 2.6.11, “Template Configuration (Optional),” on page 26
- Section 2.6.12, “Summary of Configuration,” on page 26

2.6.1 Initial Installation

1. Create and name a new Conferencing installation.

   The name of the installation cannot contain spaces, but can contain any combination of ASCII and alphanumeric characters.

2. Initialize the `PostgreSQL` database.

   Ensure that you have created the `PostgreSQL` database prior to installation. Refer to the Installation Prerequisite section for additional information.

3. Identify a Single-Host or a Multiple-Host installation.

4. Provide the IPs and the hostnames for the XML Router, Web Portal and Desktop/App Server.

   The installer attempts to ping hosts and IP addresses to ensure that they are running and reachable. If an intervening firewall is filtering out ICMP messages or the host is intentionally down, it may not appear to be reachable even though the entered value is valid.

5. Install a Conferencing Voice Bridge (optional).

2.6.2 System Administration E-mail Configuration (Optional)

You can define a list of system administrator e-mail addresses that are used when an error or event occurs:

1. Type in the systems administrator e-mail address.
2. To configure multiple e-mail addresses, type in the first e-mail address (for example `admin@company.com`) and press *Enter*. At the next `EMAIL>>>>` prompt, type-in the second e-mail address and press *Enter*, etc.

2.6.3 Configuring LDAP Synchronization (Optional)

Synchronization between eDirectory or ActiveDirectory users and Conferencing users is established when you install Conferencing.

NOTE: If you plan on running Active Directory LDAP Synchronization, you need to edit the `ldap.xml.in` file in the `cluster-prototype directory` (see Appendix E, "LDAP User Authentication," on page 47) before running the installer.

During the installation, you are prompted:

```
Do you want to change the LDAP configuration? (y/n)
```

1. Type `y`, then press Enter.

   Next, you are prompted:

   ```
   Should the system enable LDAP synchronization? (y/n)
   ```

2. Type `y`, then press Enter.

   Next, you are prompted with options:

   ```
   LDAP servers
     1: URL=ldap://ldapserver, bindDN=cn=admin, o=yourcompany,
   bindPW=password, baseDN=ou=employees, dc=sleepy, dc=com,
   import filter=(objectClass=User), auth filter=(uid=%s),
   community=2
      A - Add
      E - Edit
      D - Delete
      Q - Quit
   ```

   The line of settings indicates the information that the Conferencing installation program gathers for each LDAP server.

3. Type `e` for *Edit* to define your first LDAP server, then press Enter.
4. Type `1` for the server number, then press Enter.

   Next, you are prompted:

   ```
   Input the URL of the LDAP server:
   ```

5. Specify the URL in the following format, then press Enter.

   `ldap://`*`hostname`*

   Next, you are prompted:

   ```
   Input the dn with which to bind to the LDAP server:
   ```

6. Specify the Admin-equivalent username with full context, then press Enter.

   Next, you are prompted:

   ```
   Input the password for the bind dn:
   ```

7. Type the password for the Admin-equivalent user, then press Enter.

   Next, you are prompted:

   ```
   Input the base dn under which to search for users:
   ```

8 Specify the eDirectory/ActiveDirectory container that defines the search scope, then press Enter.

Next, you are prompted:

```
Input the filter used to select users for import:
```

9 Press Enter to accept the default value.

Next, you are prompted:

```
Input the filter used to select users for import:
```

10 Press Enter to accept the default value.

Next, you are prompted:

```
Input the community into which to place users imported from LDAP:
```

11 Press Enter to accept the default value.

You return to the original options prompt, which displays the information you have provided for the first LDAP server.

12 To add more LDAP servers to the list, type a for Add, press Enter, then repeat Step 4 through Step 11, adjusting the information as needed for each LDAP server.

13 If you make a mistake and need to remove an LDAP server from the list, type d for Delete, press Enter, type the number of the server to delete, then press Enter, type y to confirm, then press Enter again.

14 When you are finished listing LDAP servers, type q for Quit, then press Enter.

15 Continue as usual with the Conferencing installation.

NOTE: See "Address Book Configuration (Synchronization)" on page 48 for testing the LDAP synchronization.

2.6.4 Mailer Configuration (Optional)

The mailer is used to notify Conferencing users of events. By default, the mailer uses the SMTP service provided on its host, but you can change the SMTP Server and provide user and password authentication for that server, if required:

1. Identify the SMTP Server.
2. Configure the SMTP Server's User and Password Authentication.

2.6.5 Database Backup Configuration (Optional)

Daily database backups are stored in the `/var/iic/db-backups` directory.

1. Identify the directory where you want to store the database backups.

NOTE: We recommend that you do not store the database backups on the database server. Mount an external file system using NFS to maintain the daily database backup archives.

---

2. Configure the number of days backups are kept.
3. Define when backups are performed.

2.6.6 Meeting Archive and Document Sharing Repository Configurations (Optional)

The Meeting and Document Sharing (DocShare) Archive Repositories are both monitored daily at 4:00 a.m. to ensure that they have not reached a size of 2500MB. When a repository exceeds 2500MB, archives that have not been accessed within the last 30 days are deleted until the archive repository reaches 2000MB. If the system cannot delete archives to reach the 2500MB repository size, a warning e-mail is sent to the system administrator indicating the need for appropriate manual action. To avoid the automatic deletion of archives, the maintenance procedure can be configured to send daily notification when a meeting or document sharing archive repository reaches the specified maximum.

To modify the default maintenance procedure for a repository:

1. Determine the repository maximum size. Set the repository size in MBs.
2. Identify the action to take if the archive repository maximum is exceeded. The two available options are to automatically clean up archives that have not been accessed within the last 30 days, or to send e-mail notification to the systems administrator with no automatic archive deletion.
3. Determine what time of day the archive maintenance occurs.
4. If automatic maintenance was specified in Step 2, do the following:
    a. Determine the minimum target repository size after automatic clean up.
    b. Identify the minimum days-since-accessed that an archive can be deleted during the automated clean up procedure. For example, if the minimum days-since-accessed was set to 60 days, the automated clean up procedure does not delete archives that have been accessed within the past 60 days.
    c. Determine if the archives should be permanently deleted, or moved into another designated folder, which must be monitored manually by the system administrator.

2.6.7 Chat Audit Log Configuration (Optional)

You can configure chat audit logging at system installation or reconfiguration time using the `install.sh` script.

1. The chat audit logs are placed in `/var/iic/chatlog` on the hosts assigned to run the XML router and meeting controller(s). Conferencing IM and Conferencing chat room messages are written to the file `/var/iic/chatlog/chat.log`. Meeting chat messages are written to `/var/iic/chatlog/mtgchat.log`.
2. The chat messages contained in `chat.log` are XML stanzas:

   ```
   <message type='<"chat"|"groupchat">' from='<from_jid>'
   to='<to_jid>' time='<timestamp>' >
   <body> ... </body><x xmlns='jabber:x:event' />
   </message>
   ```

   The `from_jid` and `to_jid` tags have the forms:

   ```
   <screenname>@<xmlrouter_hostname>/<resource>
   ```

   Resource is a session identifier in the case where the message type is "chat" and it identifies the sender screen name in the case of "groupchat" type messages.

   The timestamp has the form `<YYYY><MM><DD>"T"<hh><mm><ss>` and uses GMT time.
3. Each chat message is logged to a line in `mtgchat.log`. The each line contains comma-separated fields. Each field is quoted with double quotes at the beginning and end of the field (for example, "field value").

The fields are as follows:

Field	Type	Description
timestamp	String (YYYMMDDTHH:MM:SS)	The time of the chat message in GMT.
from_id	String	The participant ID of the sender. A participant ID is assigned to each meeting participant and is sent in meeting invitations.
from_name	String	The display name of the meeting participant who sent the chat message.
delivery	String (one of: ToAll, ToOne, ToHost, ToModerators, ToNonModerators)	This field shows to whom the message was delivered.
to_id	String	This participant ID received the message. This field is empty unless the `delivery` field value is `ToOne`.
to_name	String	The display name of the meeting participant who received the chat message. This field is empty unless the `delivery` field value is `ToOne`.
message	String	The contents of the chat message.

2.6.8 Event Logging Configuration (Optional)

Log files are written to `/var/log/iic`, except for the web portal and external API server logs, which are written to files in `/usr/local/apache2/logs`. Additional information may be found in `/var/log/messages`.

There are three levels for logging. You can modify these logging levels at any time from the Administration Console (see the "Conferencing Operations Guide"):

- Error - Logs only error conditions.
- Info - Logs error conditions as well as summary information about all server tasks.
- Debug - This level logs error conditions, summary information and detailed debugging information.

NOTE: We recommend that the Error logging level be the default logging level due to the increased CPU and I/O loads associated with more verbose logging.

To set the logging:

1. Set default logging levels for system components.
2. Determine at what size the logs should be rotated.
3. Configure the number of rotated logs that should be kept.
4. Configure real time, call, user and reservation logging.

   You can configure the Conferencing servers to produce real-time event logs for call, user and meeting reservation events. The real-time interface provides the event data records as they occur so that third-party systems (billing systems, cost accounting systems, management reporting systems, directory databases, etc.) can use them. The records are provided to event record consumers via a TCP connection to Conferencing server hosts. Real time event logs are stored in the `/var/iic/cdr` directory.

   NOTE: You cannot modify real-time event logging from the Administration Console. If you do not install real-time event logging during installation, you need to re-run the installation script when you want to install real-time event logging.

2.6.9 Port Forwarding (Optional)

The Conferencing client attempts to connect to ports 1270, 443 and 21 when the primary port (either 5222 for the XML router or 2182 for desktop/app-share server) is blocked by a firewall. Connections to these ports should be forwarded to the primary port. If you are not running a load balancer that performs this task, you must forward these ports locally on the XML router host(s) or the desktop/app-share server host(s).

2.6.10 XML Router Security

In order for a Conferencing service (meeting controller, voice bridge, etc.) to connect to the XML router it must use the correct authentication key. If your XML router allows connections from the Internet, change the Service Connection Key so that unauthorized services cannot access and connect to your router. Additionally, the meeting controller needs to provide a User Session Creation Key. You should change this key so that unauthorized meeting controllers cannot create sessions on behalf of your users.

- The default value for the Service Connection Key is: `secret`
- The default value for the User Session Creation Key is: `QAZXSW88`

2.6.11 Template Configuration (Optional)

You can modify the e-mail templates that Conferencing uses to communicate with users (see Chapter 4, "Modifying Template Files," on page 33).

1. Configure system e-mail headers.
   - Configure the New User e-mail *From* display name.
   - Configure the New User e-mail *Subject*.
   - Configure the Meeting Invitation e-mail *Subject*.
   - Configure the New Meeting Archive e-mail *From* display name.
   - Configure the New Meeting Archive e-mail *From* e-mail address.
2. Configure the New User e-mail template.
3. Configure the Meeting Invitation template.
4. Configure the Meeting Summary e-mail template.
5. Configure the New Meeting Archive e-mail template.

2.6.12 Summary of Configuration

Once you have completed the installation script, you are presented with a summary of the choices you selected. If you are not satisfied with the configuration setup, you can either modify the configuration or you can exit the installer and run the script again. If you exit the installer, the current configuration is saved, and when you rerun the install script, it is used for the default values during the reconfiguration.

2.7 Starting and Stopping the Cluster

You can start and stop the Conferencing services for the entire cluster using the `control-cluster.sh` script.

To Stop Conferencing Services, type:

```
./control-cluster.sh --cluster <your-cluster> [--single-host <your-host>] stop
```

To Start Conferencing Services, type:

```
./control-cluster.sh --cluster <your-cluster> [--single-host <your-host>] start
```

Use the `--single-host` argument with the script if there is only one host in your cluster.

2.8 Conferencing Administration Console

Once you have successfully installed the Conferencing System Components, you can access the web-based Conferencing Administration Console. Use the Administration Console to monitor the state of the Conferencing components and services, as well as to create Conferencing communities.

The Conferencing Administration Console is available via the URL:
`http://<webportalhostname>/imidio/console/`

NOTE: If you have SSL enabled, you should specify https in the URL instead of http.

Logging on to the Administration Console

The initial installation creates the screen name *admin* with password *admin*. You can use these values to log on, and change them later (see the "Conferencing Operations Guide" for further information on using the Conferencing Administration Console).

Creating Conferencing Communities

See the "Conferencing Operations Guide" for information on adding Conferencing Communities.

2.9 Conferencing Client Installation

The following procedures cover the creation of the Conferencing Client RPM file to use for web download, how to install the Conferencing Client using this file and how to install the Pidgin Instant Chat Client:

- Section 2.9.1, "Building the Conferencing Client RPM," on page 27
- Section 2.9.2, "Installing the Conferencing Client," on page 28
- Section 2.9.3, "Installing the Pidgin Instant Chat Client," on page 28

NOTE: The Windows executable file is automatically generated during the server install process and already in the web download directory.

2.9.1 Building the Conferencing Client RPM

NOTE: Installers are included for all client components in the server installation package, but the client package kits are still available so that you can customize the default values for site-specific options such as host name and security settings to make deployment easier.

---

1. Untar the Conferencing client package from root directory:
   `tar -zxf zon-package-kit-<version>.tar.gz`
2. Build the Conferencing Client Install RPM (specify `yes` or `no` for the "use-ssl" parameter below):
   ```
   cd zon-package-kit
   ./build-rpm.sh <conferencing-xml-router-external-hostname> <conferencing-portal-hostname> <use-ssl>
   ```
3. If generated on the Conferencing server, the RPM is automatically copied to the web download directory. Otherwise, copy the generated RPM manually to the Conferencing server:
   ```
   cd /usr/src/packages/RPMS/i586
   scp zon-binary-<version>-1.i586.rpm root@<conferencing-portal-hostname>/usr/local/apache2/htdocs/imidio/downloads/.rpm
   ```

2.9.2 Installing the Conferencing Client

1 After installing the Conferencing server, you can download the Conferencing client from the following URLs:

- Windows: http://<conferencing-portal-hostname>/imidio/downloads/conferencing.exe
- Linux: http://<conferencing-portal-hostname>/imidio/downloads/conferencing.rpm

You can send these Conferencing client installation URLs to your Conferencing users via e-mail for them to install the Conferencing client on their desktops.

NOTE: If you have SSL enabled, you should specify https in the URL instead of http.

---

2 Select *Open* or *Run* to invoke the installer after the download completes.

NOTE: It may take a while for the installation to begin on a Linux desktop.

After you install the client, use the *admin* screen name (password = *admin*) or the screen name of the first user of the first community to sign on.

Once you sign on, you can add Conferencing users to the community (see the "Conferencing Operations Guide").

2.9.3 Installing the Pidgin Instant Chat Client

After installing the Conferencing server, you can download the Pidgin client with Conferencing protocol support from the following URLs.

- Windows: http://<conferencing-portal-hostname>/imidio/downloads/pidgin.exe
- Linux: http://<conferencing-portal-hostname>/imidio/downloads/pidgin.rpm

1 Download the `pidgin.exe` (Windows) or `pidgin.rpm` (Linux) executable file to your desktop.

The URLs for downloading these files should be in your invitation e-mail.

2 In Linux and Windows, double-click the *pidgin* (.rpm or .exe) installer (placed on the desktop during download), or select *Open* or *Run* to invoke the installer.

NOTE: It may take a while for the installation to begin on the Linux desktop.

---

3 In the *Installer Language* dialog that appears, select your language from the drop-down list.

NOTE: The installer wizard walks you through the installation process. The defaults should be fine for your install, though you may want to select the *Shortcut* > *Desktop* option.

---

4 Click *Finish* to complete the installation process.

The integrated Pidgin instant chat client is now installed and ready for use.

NOTE: See the Conferencing Online Help or the Conferencing User Guide for information on using the integrated Pidgin client with Conferencing.

Reconfiguring and Upgrading

3

The following sections discuss both reconfiguration and upgrading the Conferencing servers and clients:

- Section 3.1, “Backing Up and Restoring the Database,” on page 29
- Section 3.2, “Reconfiguring Conferencing Hosts,” on page 30
- Section 3.3, “Upgrading the Conferencing Client,” on page 30
- Section 3.4, “Upgrading the Conferencing Servers,” on page 30
- Section 3.5, “Starting and Stopping Conferencing Services,” on page 31

3.1 Backing Up and Restoring the Database

Before doing any reconfiguration or upgrade of the Conferencing software, we recommend that you perform a backup of your existing database.

Backing Up the Database

The system automatically backs up the database on a daily basis. The backups can be found in `/var/iic/db-backups` on the db-host (as defined in `/opt/iic/conf/global-config`). Each backup is a tar(1) archive compressed using the bzip2(1) utility. The current daily backup is called `db.tar.bz2`.

You can also back up the database at any arbitrary time using the `pg_dump(1)` utility. The state of the database in the backup is that of all committed transactions at the time `pg_dump(1)` is run. Any updates done after the backup is started are ignored.

The following command line shows how to dump the contents of the database to a tar(1) archive named `db.tar`:

```
pg_dump -b -F t -f db.tar <db_name>
bzip2 db.tar
```

You can either execute `pg_dump` on the `db_host` machine or set up the PostgreSQL environment variables according to the database configuration in `/opt/iic/conf/global-config`.

Restoring the Database

Restoring an archived database is done using the `pg_restore` command. To restore a backup in a `bzip2` compressed tar file, the following command line can be used:

```
bunzip2 db.tar.bz2
pg_restore -d <db_name> db.tar
```

You can either execute `pg_restore(1)` on the `db_host` machine or set up the PostgreSQL environment variables according to the database configuration in `/opt/iic/conf/global-config`.

3.2 Reconfiguring Conferencing Hosts

Follow these steps to reconfigure the installation:

1. Make a backup copy of the sitescape-conferencing directory:
   `cp -r sitescape-conferencing sitescape-conferencing.bk`
2. Open the `sitescape-conferencing` directory.
3. Run: `./install.sh`
4. The installation script prompts you for the configuration information. The prior configuration is used as the default values for the new configuration.

You are also asked whether you want to initialize the system database. You must initialize a database once before it can be used by the system. However, initializing a database that is already in use by the system results in all of the data being lost. Only initialize a database once on a database host.

3.3 Upgrading the Conferencing Client

Follow these steps to upgrade the Conferencing client:

1. Make a backup copy of the `sitescape-conferencing` directory:
   `cp -r sitescape-conferencing sitescape-conferencing.bk`
2. Open the `sitescape-conferencing` directory.
3. Copy the new `installers.tar.gz` archive into your installation directory
4. Run: `./install.sh`

Conferencing users are automatically upgraded the next time they log on.

3.4 Upgrading the Conferencing Servers

Follow these steps to upgrade the Conferencing servers:

1. Make a backup copy of the `sitescape-conferencing` directory:
   `cp -r sitescape-conferencing sitescape-conferencing.bk`
2. Extract the new distribution file using:
   `tar zxvf sitescape-conferencing-<version>.tar.gz.`
3. Open the `sitescape-conferencing` directory.
4. Copy the prior configuration directory to the current location:
   `cp -r ../sitescape-conferencing.bk/myzon`
5. Run: `./install.sh`
6. The installation script prompts you for the configuration information. The prior configuration is used as the default values for the upgrade.

WARNING: When asked whether you want to initialize the system database, answer `no` unless you want to delete all of your data.

3.5 Starting and Stopping Conferencing Services

Starting and Stopping the Cluster

You can start or stop Conferencing services for the entire cluster using the `control-cluster.sh` script.

To Stop Conferencing Services, type:

```
./control-cluster.sh --cluster <your-cluster> [--single-host <your-host>] stop
```

To Start Conferencing Services, type:

```
./control-cluster.sh --cluster <your-cluster> [--single-host <your-host>] start
```

Use the `--single-host` argument with the script if there is only one host in your cluster.

Starting and Stopping Individual Machines

To start or stop services on only one of the machines on the cluster, use the script: `/opt/iic/conf/control-services.sh`.

To Stop Conferencing Services with `control-services.sh`, type:

```
/opt/iic/conf/control-services.sh stop
```

To Start Conferencing Services with `control-services.sh`, type:

```
/opt/iic/conf/control-services.sh start
```

Modifying Template Files

4

The installation script `install.sh` prompts you whether you want to modify various e-mail body templates. The following sections describe the available e-mail body templates:

- Section 4.1, “Modifying the Meeting Invitation Template,” on page 33
- Section 4.2, “Using IF Statements,” on page 35
- Section 4.3, “Modifying the Meeting Summary E-mail Template,” on page 35
- Section 4.4, “Modifying the New User Greeting E-mail Template,” on page 36

During the installation, you have the opportunity to edit both the new user and invitation templates. You can do this by editing the templates and then importing them, or by using emacs on an install host.

4.1 Modifying the Meeting Invitation Template

The meeting invitation template has two roles. The first role is to fill the body of the meeting invitation e-mail sent to meeting participants. The second role is to create the content of an IM invitation sent to meeting participants. In order to fulfill these two roles, the template is divided into sections. The purpose of each section is to specify whether the text produced in a section should be included in an e-mail body, IM content or both. The syntax for a section is as follows:

```
#SECTION <selector>
.
.
.
#SECTION END
```

The `<selector>` variable represents one of the following values:

Value	Description
EMAIL_IM	The text produced in this section is present in both e-mail and IM meeting invitations.
EMAIL_ONLY	The text produced in this section is present only in e-mail meeting invitations.
IM_ONLY	The text produced in this section is present only in IM meeting invitations.

The basic operation in the section is to echo (i.e. output) text. For example:

```
echo Click here to enter the meeting <MEETINGURL><NEWLINE>
echo Pin:
echo <INVITEE-PIN><NEWLINE>
```

There are several things to notice about these lines. One is that the output from an echo is appended to the result of the prior echoes. If you want a line break at a particular point, you must explicitly provide the line break using the `<NEWLINE>` tag. Also, an echo line may contain tags that are replaced with values particular to the meeting to which the participant is invited. You can use the following tags:

Tag	Description
<TITLE>	This tag is replaced with the title of the meeting.
<HOST>	This tag is replaced with the host of the meeting.
<TIME>	This tag is replaced with the scheduled start time of the meeting.
<DESCRIPTION>	This tag is replaced with the description of the meeting.
<MESSAGE>	This tag is replaced with the invite message (if any) that the host provided when creating the meeting.
<INVITEE-NAME>	This tag is replaced with the name of the participant.
<INVITEE-PHONE>	This tag is replaced with the phone number of the participant.
<INVITEE-PIN>	This tag is replaced with the pin of the participant.
<MEETING-URL>	This tag is replaced with URL to click for the participant to join the meeting.
<ANONYMOUS-URL>	This tag is replaced with URL to click for an anonymous meeting participant to join the meeting.
<MEETING-PHONE>	This tag is replaced with the title of the meeting.
<ANONYMOUS-PIN>	This tag is replaced with the pin for an anonymous invited participant.
<PASSWORD>	This tag is replaced with the meeting password for the meeting.

4.2 Using IF Statements

In addition to the echo command, conditional text may be generated. The way to specify conditional text is using an `%IF` statement. The `%IF` statement is as follows:

```
%IF <variable-expression>
.
.
%IF END
```

The `<variable-expression>` variable is either a Boolean variable or if prefixed with an exclamation point, the negation of the variable. If the `<variable-expression>` is true, the contents of the `%IF` are executed. If false, they are not. Note that there is no `ELSE` clause.

The following variables are available for use:

Variable	Description
CALL_IN	True when the meeting has a voice conference associated with it and the participant has no phone number.
CALL_OUT	True when the meeting has a voice conference associated with it and the participant has a phone number.
DESCRIPTION	True when a non-empty description exists for the meeting.
MESSAGE	True when a non-empty invite message exists for the meeting.
PASSWORD	True when a non-empty password exists for the meeting.
PRIVATE	True when the meeting is a private meeting.

4.3 Modifying the Meeting Summary E-mail Template

The meeting summary e-mail body template contains text with embedded tags that are replaced with values particular to the meeting that ended. The non-tag text is left as is in the e-mail body.

The following table lists the available tags:

Tag	Description
<MeetingID>	This tag is replaced with the meeting ID of the meeting that ended.
<StartDateTime>	This tag is replaced with the start time and date of the meeting that ended.
<Duration>	This tag is replaced with duration of the meeting that ended.
<VoiceRecording>	This tag is replaced with YES or NO depending on if there is a voice recording associated with the meeting that ended.
<DataRecording>	This tag is replaced with YES or NO depending if there is a recording of the app/desktop sharing session(s) associated with the meeting that ended.
<MeetingParticipants>	This tag is replaced with a list of the participants and some of their contact information for the meeting that ended.

4.4 Modifying the New User Greeting E-mail Template

When a new user is added to the system, they receive an e-mail notification informing them that they are now a user of the system and providing them with information on using Conferencing. You can tailor the body of this e-mail by modifying the file: `sitescape-conferencing/<cluster>/new-user-template.default`.

When the system creates the body of new user e-mail, it replaces a number of tags with information particular to the new user. Any remaining text that is not a tag is left as is.

The following table lists the available tags:

Tag	Description
<IICNAME>	This tag is replaced with the user's full name.
<IICUSERNAME>	This tag is replaced with the user's screen name.
<IICPASSWORD>	This tag is replaced with the user's initial password.
<IICDIALIN>	This tag is replaced with the voice bridge phone number.
<IICPERSONALPIN>	This tag is replaced with the user's instant Meeting PIN.
<IICMEETINGID>	This tag is replaced with the user's instant Meeting ID.

Configuring ssh(1) private/public Key Authentication

A

The installation script uses `ssh(1)` and `scp(1)` to copy files to and execute scripts on the Conferencing hosts. In order to avoid typing the root password for the Conferencing hosts numerous times during the install, you can configure private/public key authentication for `ssh(1)`. If private/public key authentication is in place, rather than prompting for the root password, `ssh(1)/scp(1)` gets an authentication token generated using the private key. It authenticates the token on the Conferencing host using the root user's list of authorized public keys.

Follow these steps to configure private/public key authentication:

1. Section A.1, "Generating a Private/Public Key Pair," on page 37
2. Section A.2, "Configuring the ssh Key Agent," on page 38
3. Section A.3, "Adding the Public Key to the Root User's Set of Authorized Keys," on page 38

A.1 Generating a Private/Public Key Pair

To generate a key pair, use the `ssh-keygen(1)` command.

Here is a sample interaction with `ssh-keygen`:

```
-bash-2.05b$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase): ******
Enter same passphrase again: ******
Your identification has been saved in /home/admin/.ssh/id_rsa.
Your public key has been saved in /home/admin/.ssh/id_rsa.pub.
The key fingerprint is:
8c:ff:d4:50:65:46:9f:6b:59:34:43:3a:5f:e7:5a:54 admin@staging.my.com
```

At this point there are two new files in the home directory: `~/.ssh/id_rsa` and `~/.ssh/id_rsa.pub`. The first file is the private key (in binary form) and the second is the public key (in text form).

A.2 Configuring the ssh Key Agent

In order to use the newly generated private key, you must start the ssh key agent, `ssh-agent`, and add the key to the set of keys held by the agent. In order to have the keys available whenever you log on, edit the file `~/.bash_profile`. The following shell script snippet should be inserted at the end of the file:

```
if [ -z "$SSH_AUTH_SOCK" ]; then
  eval $(ssh-agent)
  ssh-add
fi
```

After saving `~/.bash_profile`, log off and back into the staging host. You are prompted for the private key pass phrase entered when the key pair was generated. After successfully entering the pass phrase, the private key is available for generating authentication tokens.

A.3 Adding the Public Key to the Root User's Set of Authorized Keys

The final step is to add the public key (`~/.ssh/id_rsa.pub` on the staging host) to the set of authorized keys for the root user on the Conferencing host.

Follow these steps to add the key:

```
$ scp ~/.ssh/id_rsa.pub root@zonhost:/tmp
$ ssh root@zonhost
The authenticity of host 'zonhost (W.X.Y.Z)' can't be established.
RSA key fingerprint is
df:c7:21:77:ec:53:89:77:4f:32:4d:a8:7a:a2:c2:7c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'jabber,10.0.1.3' (RSA) to the list of
known hosts.
root@zonhost's password: ******
# cat /tmp/id_rsa.pub >> .ssh/authorized_keys
# chmod 700 .ssh
# chmod 600 .ssh/authorized_keys
```

You need to repeat the above steps for all the Conferencing hosts.

Editing the global-config File

B

The installation script `./install.sh` takes care of updating the `global-config` file. If you want to edit the file directly, see the following information.

The overall cluster configuration is in the file `global-config`. The following steps are required to configure a Conferencing server cluster. A later section describes optional configuration steps that you should review and may wish to consider implementing:

- Section B.1, "Assigning Services to Nodes," on page 39
- Section B.2, "Configuring Web Services," on page 41
- Section B.3, "Configuring the Mailer," on page 41
- Section B.4, "Using Port Forwarding," on page 41

IMPORTANT: All hostnames currently need to be lowercase.

B.1 Assigning Services to Nodes

The following steps are necessary to configure what services run on which cluster nodes.

1 Configure the database server

   1a Change the `db_host` variable assignment to specify the database host.

   1b For new installations, it is not necessary to change `db_name`, `db_user` and `db_pswd`.

   1c Define the host access to the database. The servers that run the address book, XML routers and web portals must have access to the database. You can specify access to the database host using a set of IP addresses and netmasks. An IP address/netmask pair specifies a range of IP addresses that are allowed to connect to the database. For instance, 10.1.1.1/255.255.255.0 allows IP addresses 10.1.1.* to connect to the database. The IP addresses are specified in `db_ip_addr` and the netmasks in `db_netmask`. Both are arrays so the above example would be:

```
db_ip_addr=( 10.1.1.1 )
db_netmask=( 255.255.255.0 )
```

2 Configure XML router services:

   2a Set `external_hname` to the hostname used by Conferencing clients to connect to XML router services.

   2b Set the `lcl_xmlrouter` and `lcl_xmlrouter_ip` arrays to specify the cluster hosts and IP addresses for the XML router services. More than 2 XML routers are not currently supported.

3 Configure services connected to the XML router:

   3a Configure the meeting controller service and the backup meeting controller service (if necessary). Specify the cluster host(s) to run each and the XML router listen ports. The host(s) is specified in the `controller_host` array and the listen ports in the `controller_port` array.

3b Configure the `addressbk` service. Specify the cluster host and XML router listen ports by setting the `addressbk_host` array and the `addressbk_port` array. Currently, only one `addressbk` is supported.

3c Configure the `mailer` service. Specify the cluster host and XML router listen ports by setting the `mailer_host` array and the `mailer_port` array. Currently, only one `mailer` is supported.

3d Configure the voice bridge(s). Multiple voice bridges may be configured for scaling purposes (see Appendix C, "Editing the dialing.xml File," on page 43):

3d1 Specify the cluster host(s) and XML router listen ports by setting the `voice_host` array and the `voice_port` array.

3d2 Specify the voice provider for the voice bridges using the `voice_provider` variable. If no voice support has been purchased, use the value `stub`. If an NMS voice bridge has been purchased, use the value `nms`.

3d3 Also, specify the phone numbers allocated to each bridge using the `voice_phones` array. You can assign multiple phone numbers to a single voice bridge by separating the phone numbers with commas. Note that if spaces appear in phone numbers, the phone numbers must be quoted. Also, if the stub voice provider is in use, a dummy voice bridge number must be specified (e.g. "999-555-1234").

3e Configure the meeting archiver service(s). You can configure multiple meeting archivers for scaling purposes:

3e1 Specify the assigned cluster host(s) and XML router listen ports by setting the `mtgarchiver_host` array and the `mtgarchiver_port` array.

3e2 If the meeting archiver hosts are separated from a voice bridge host by a NAT router, use the `mtgarchiver_voice_host` array to specify the voice bridge host(s) from the meeting archivers' perspective. If no NAT router is involved, the meeting archivers attempt to connect to the voice bridge(s) using the hostnames found in `voice_host`.

3f Configure the external API service:

Specify the cluster host and XML router listen ports by setting the `extapi_host` and `extapi_port` arrays. You can use multiple external API hosts.

4 Configure the app/desktop sharing servers:

4a Configure the `share_host` array to specify which hosts run as app/desktop sharing servers. Note that you can run multiple app/desktop servers on a single host by specifying a host multiple times. For instance if `share_host` was assigned the value `kanga kanga roo`, the host named kanga would run two servers and roo would run one. Also, be aware that you would need to define two distinct IP addresses on kanga because both servers use port 80 for tunneling through firewalls.

4b Configure the port to use for each share server using the `share_port` array. This port can remain 2182 since the IP addresses must be distinct for each share server. Port 2182 does not conflict with any default Linux service.

B.2 Configuring Web Services

You can implement the web portal for the system across multiple hosts. When you use multiple web services the meeting archive repository must reside in a file system accessible to all HTTP daemons. For instance, it may reside on a NAS box or via an NFS exported file system on one of the cluster hosts. In any event, the shared file system must be accessible via `/usr/local/apache2/htdocs/repository/mtgarchive` on all the machines hosting the HTTP daemon. Also, you are responsible for configuring a load balancer for HTTP requests to these machines.

When configuring the external API HTTP daemon(s), administrative functions are performed via HTTP on the external API hosts. For added security, these hosts may be placed behind a firewall. However, the hosts assigned to run the web portal must be able to connect to the external API hosts via port 8000 in order for the admin console to function properly.

1. Configure web portal host(s):
   - **1a** Modify the `portal_hname_local` array to specify all the cluster hosts for web service.
   - **1b** Ensure that `/usr/local/apache2/htdocs/repository/mtgarchive` is the same-shared file system for all cluster hosts in `portal_hname_local`.
   - **1c** Modify the `portal_ip` array to include the IP addresses that the HTTP daemon should listen on for connections.
   - **1d** Modify the `portal_hname` variable to define the hostname used in URLs to the web portal.
2. Configure external API host(s):
   - **2a** Modify the `extapi_hname_local` array to specify all the cluster hosts for the external API service.
   - **2b** Modify the `extapi_portal_ip` array to specify the IP addresses on which an external API HTTP daemon listens.
   - **2c** Modify the `extapi_portal_hname` to specify the hostname in URLs to the external API.

B.3 Configuring the Mailer

By default, the system is configured to assume that the cluster node assigned to the mailer is able to perform mail delivery. If that is not the case for some reason, you can configure the mailer to use an external SMTP host for mail delivery. You can use the variables `smtp_host`, `smtp_user`, and `smtp_pswd` in `global-config` for this purpose.

B.4 Using Port Forwarding

By default, each cluster host running either an XML router or app/desktop sharing servers forwards ports 1270 and 443 to the respective service ports. If you have an installation that is running a load balancer that provides port forwarding, set the global-config variable `iptables_port_forwarding` to `no` and configure your load balancer accordingly.

Editing the dialing.xml File

C

This section applies only to those clusters that are running a voice bridge.

The role of the `dialing.xml` file is to specify the rules whereby a given phone number is transformed into the set of digits dialed by the voice server. For example, default area codes that must be appended to all 7-digit phone numbers. Most of the file consists of a collection of attributes and their values. The following table lists the attributes and their role:

Attribute	Description
areaCode	This attribute is a default area code to use when none is present in a phone number.
tollPrefix	This attribute is the prefix to dial in order to place a toll call. In the US, a 1.
i18nPrefix	This attribute is the prefix to use when placing international calls. In the US, 011.
country	A short description of the country the bridge is located in (e.g. US).
countrycode	This is the international country code of the voice bridge. This code is used to decide whether a number requires that an international call be placed. For the US, the value is 1.
dialingMode	The attribute may be one of the following values: ◆ normal - Do not dial area code except for long distance calls. ◆ dialAreaCodeAlways - The phone numbers always have an area code. The area code of the bridge may be used to supply missing area codes. ◆ DialAreaCodeOnLD - Only dial an area code for long distance numbers (see areaCodes/exchanges lists below).

The remaining components of the file are two lists: area codes and exchanges. The role of these lists is to determine whether a specified phone number requires a toll call by specifying a default condition (either local or long-distance) for area codes or exchanges. The list itself is a set of exceptions to the default. For instance, to specify that all area codes are long distance except for 978, the following may be used:

```
<areaCodes default="ld">
      <local>978</local>
</areaCodes>
```

Similarly with exchanges, you could, for example, specify that most exchanges are long distance, but 865 is local:

```
<exchanges default="ld">
      <local>865</local>
</exchanges>
```

Updating Meeting Invitation Web Pages

D

The image that appears at the top of meeting invitation web pages can be found in `/usr/local/apache2/imidio/images/instant.jpg`. On the web portal host(s), you can replace that file with another logo. Be aware that this file is not preserved during updates or reconfigurations and has to be restored once the upgrade or reconfiguration is complete.

If the dimensions of the new logo are different from the default, you may need to adjust the `<img>` element in `/usr/local/apache2/htdocs/imidio/invite/frame_header.php`.

You can modify the body of the meeting invitation web pages by updating `/usr/local/apache2/htdocs/imidio/invite/*.html`

NOTE: These files are not saved after upgrades or reconfigurations.

LDAP User Authentication

E

NOTE: The password for `admin` always comes from the Conferencing internal database so that an administrator is able to log on even if directory servers are not available. Because the password must be passed over the network in plain text, we recommend deployment using SSL.

LDAP User Authentication Input File

You can modify the `sitescape-conferencing/cluster-prototype/ldap.xml.in` input file to use ActiveDirectory synchronization instead of eDirectory synchronization and to map additional LDAP attributes to Conferencing contact fields.

To use ActiveDirectory synchronization, you need to comment out the eDirectory section in the file and uncomment out the Active Directory section, see examples below:

eDirectory Section:

```
<!-- configuration for eDirectory and generic LDAP server -->
<attributes>
  <attribute>
    ...
  </attribute>
</attributes>
```

Move the closing XML comment tag (`-->`) after the `...generic LDAP server` comment so that it follows the `</attributes>` tag under the eDirectory section:

```
<!-- configuration for eDirectory and generic LDAP server
<attributes>
  <attribute>
    ...
  </attribute>
</attributes>
-->
```

ActiveDirectory Section:

```
<!-- configuration for ActiveDirectory
<attributes>
  <attribute>
    ...
  </attribute>
</attributes>
-->
```

Move the closing XML comment tag (`-->`) after the `</attributes>` tag so that it follows the `configuration for ActiveDirectory` comment:

```
<!-- configuration for ActiveDirectory -->
<attributes>
  <attribute>
    ...
  </attribute>
</attributes>
```

Conferencing Field Names

Use these names to configure the mapping of LDAP attributes to Conferencing contact fields:

“screenname” - “title” - “firstname” - “middlename” - “lastname” - “suffix” - “company” - “jobtitle” - “address1” - “address2” - “state” - “country” - “postalcode” - “aimname” - “email” - “email2” - “email3” - “busphone” - “homephone” - “mobilephone” - “otherphone” - “extension” - “msnscreen” - “yahooscreen” - “aimscreen” - “user1” - “user2” - “defphone”

NOTE: For eDirectory, the `uid` attribute is mapped to the Conferencing `screenname` by default. If you want to use the `cn` LDAP attribute instead of the `uid` attribute, you can change this mapping to map the `cn` attribute to the Conferencing `screenname`.

Address Book Configuration (Synchronization)

Execute `/opt/iic/bin/ldap-sync.sh <portal-server-hname>` to perform the initial synchronization.

NOTE: After starting the server, wait 20 seconds or so before executing this command; if you do not get an XML message back, you probably did not wait long enough.

This script displays an XML message if it fails (the fault message is clearly visible); if it succeeds, the XML data contains a single number that is the number of users actually synchronized. You can run this script manually as needed, or configured to run periodically using `cron` (the default setting is for it to run daily).