Installation Guide
For SiteScape Zon

Publishing Date:	August, 2005
Software Version:	SiteScape Zon Version 7.3

Table of Contents

Preface

This manual provides task-oriented and reference information to be used by those who need to install the Zon cluster software. This manual provides information on configuring and installing the Zon Cluster software.

Audience

The audience for this manual are experienced programmers who:

- Have experience installing and administering Linux software.
- Have an understanding of network architecture.
- Have experience with `ssh(1)` administration and implementation.

Conventions

The following table presents conventions used in this manual:

When you see...	**It means...**

`command options`
`syntax examples`
`code examples`
	These elements are presented in monospace font. Include these identifiers in your code as they are shown in the documentation.

`variable command parameters`	This manual presents variable parameters in *`italicized monospace font`*. In your code, replace these variable names with your own programming identifiers.
`?parameter?`	In syntax examples, this manual delimits optional parameters using question marks (?). Include these parameters in your code only if you need them.
Command names **Hyperlinked text** **Button text**	This manual presents references to these elements in **bold** font.
Defined terms	This manual presents new terms that are being defined in *italic* font.
BODY INPUT BGCOLOR CLASS	This manual presents HTML tags and their attributes in UPPERCASE LETTERS.

More Information

Customers with maintenance contracts can participate in SiteScape's support, Help, and customization forums. These forums provide a greater level of detail, collaborative exchanges with SiteScape engineers, and the most up-to-date information available about SiteScape's products and services.

To access the forums, use the following URLs:

Support: http://support.sitescape.com/forum/support/dispatch.cgi/support

Help: http://help.sitescape.com/

Customization: http://support.sitescape.com/forum/support/dispatch.cgi/custom

Home page: http://www.sitescape.com/

Chapter 1: System Overview

This section provides an overview of the Zon architecture as well as a description of the system components and prerequisites.

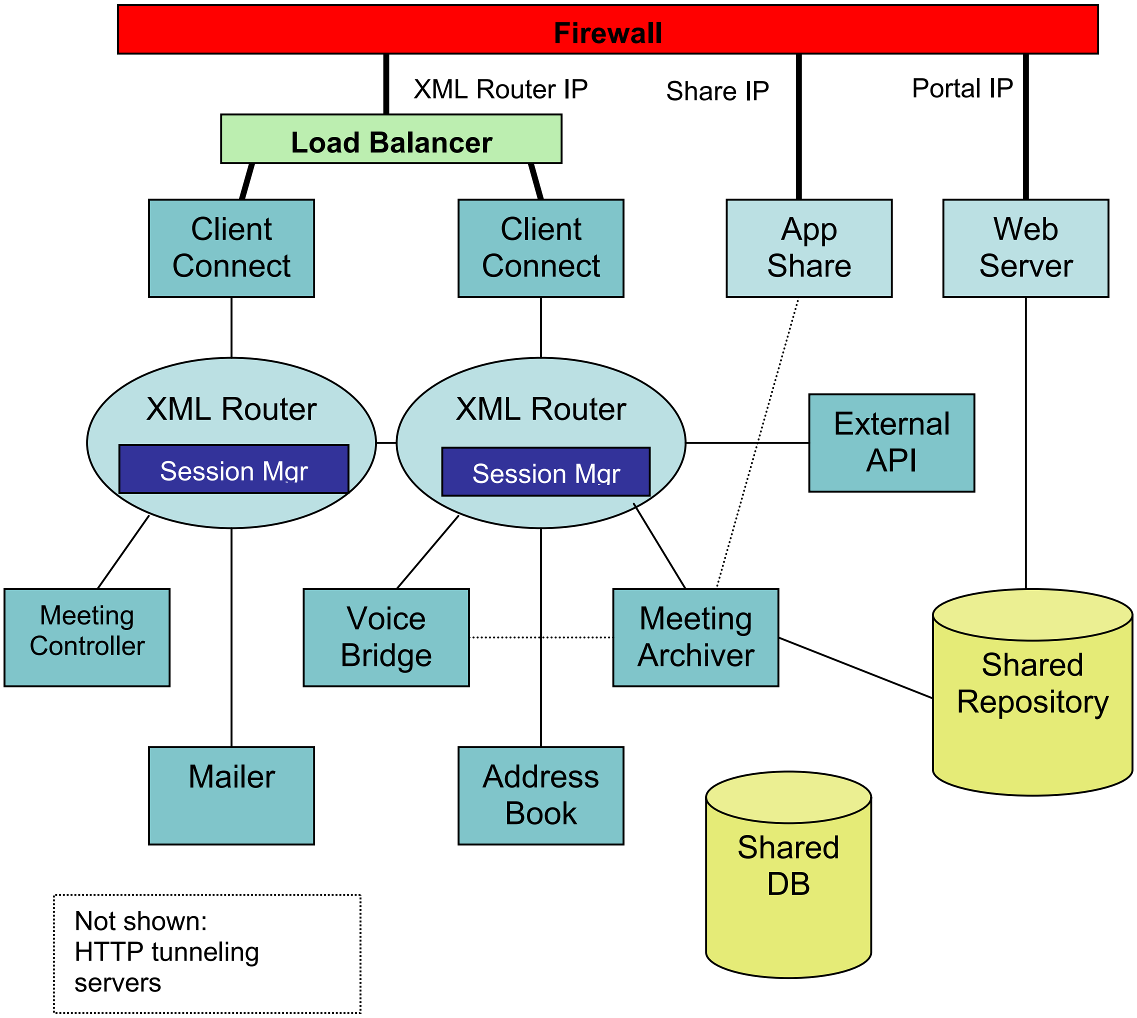
System Components

The Zon Server is a highly modular suite of components that can be configured 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 client, and establishes user sessions with session manager.
- 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.
- Mailer - Sends notification e-mails on behalf of meeting controller and schedule server.
- Address Book/Schedule Server - Stores and retrieves community and personal address books, and system profile information. Also stores and retrieves meeting schedule, options, and participant information.
- Meeting Archiver Server - Collects audio, app/desktop sharing images and chat sessions to create Macromedia Flash-based meeting archives stored in a web accessible repository.
- Desktop/App Share Server - Forwards desktop and application sharing data from meeting presenter to meeting participants, and manages remote control access to presenter desktop.
- External Web Service - Provides web service API for external parties as needed for integration with existing service provider systems. Also provides service for the meeting invitation web application.
- Voice Bridge – Interconnects phone calls for the audio portion of a meeting.

Cluster Diagram

A *cluster* is a set of components providing services to a community of users. The following diagram illustrates the architecture of a cluster.



Chapter 2: Installation Procedures

The following chatper describes the installation requirements and procedures.

Installation Overview

The Zon installation or upgrade process occurs using the following tasks.

Zon Cluster Components

Installation or upgrade of the Zon Cluster Components is comprised of the following:

1. Verify the installation prerequisites are in place.
2. Unzip/untar the file.
3. Unpack the files.
4. Backup the sitescape-zon 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

Zon Client Components

Administration and installation of communities and new users is comprised of the following steps:

1. Launch the Administration Console.
2. Create a New Community with the Administration Console.
3. Install a Zon Client.
4. Use the Zon Client to create users and perform other administrative tasks.

Installation Prerequisites

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

Zon Server Requirements:

- **RedHat Enterprise Linux 3.4** - Each Zon server host must be running RedHat Enterprise Linux 3.4.
- **PostgreSQL** - The PostgreSQL database server must be installed on one of the Zon hosts. A default RedHat Enterprise Linux 3.4 installation **will not** install the PostgreSQL database server. You must choose to install it explicitly. When installing the PostgreSQL software, select the rh-postgresql server software. Once you have installed the PostgreSQL software, the Zon installation will initialize the database. **NOTE**: Ensure that you do not have any existing PostgreSQL databases on any of the servers in the Zon cluster.
- **Time synchronization** - All Zon hosts must be time synchronized and the system time zones must all be consistent. To maintain accurate system time, you can configure reliable timeservers in `/etc/ntp.conf` and `/etc/ntp/step-tickers` (see the `ntpd(1)` man page).
- **Emacs** - During the installation, you will 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 RedHat Enterprise Linux 3.4 installation and must be explicitly installed.

Network Requirements:

- **IP addresses** - You must define at least three IP addresses that will be used by Zon clients to connect to Zon services. The services that Zon 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 per instance. If any Zon client is outside your firewall, the IP addresses must be externally reachable.

Firewall Requirements:

- **XML router IPs** - The XML router and desktop/application sharing IP addresses. IP address have ports 1270, 443 and 80 open.
- **Port 80 open** - The web portal IP address must have port 80 open.
- **DMZ Configuration (optional)** - If you choose to run Zon services in the DMZ, and are concerned about database security, you can run the database inside the firewall. XML routers, Address Book and web portal HTTP servers will connect to the database using port 5432.

DNS and hostname requirements:

- **Three hostnames** - The XML router, web portal and desktop/application sharing IP addresses each require a hostname resolvable by Zon clients.
- **Fully qualified domain name** – The web portal host requires a fully qualified domain name. For example, www.mycompany.com or webportal.zoninstall.com
- **Unique hostnames (multiple machines)** - Multiple-machine Zon installations require each machine to have a distinct host name. These host names do not need to be resolvable outside the local network.

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.
- Zon 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 that web portal IP address.

Preparing for Installation

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 Zon hosts. Otherwise, you will need to enter the root password for the Zon hosts numerous times during the installation. See the appendix on configuring `ssh(1)` public/private key authentication.

Unpacking the Files

You should have the SiteScape Zon distribution file in a compressed `.tar` archive named `sitescape-zon-<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 (can be one of the Zon hosts) using:

```
      tar –zxvf sitescape-zon-<version>.tar.gz
```

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

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

Backup the Directory

After performing the following cluster configuration, backup the sitescape-zon directory, as it will become the location where future upgrades and reconfigurations are performed.

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

Installing the Zon Cluster Components

Perform these steps after extracting the Zon server distribution file `sitescape-zon-<version>.tar.gz` (where *<version>* is the version of the system you received) on an installation-staging host (may be a Zon host):

1. Open the sitescape-zon directory
2. Run: `./install.sh`
3. The installation script will prompt you for the configuration information and install the software

During the installation process, you will be asked whether you want to modify the associated templates. Refer to "Chapter 4: Modifying Template Files" for further information.

New Zon Cluster Components Installation Process

The installation script will take you through the following to install and configure a new Zon Server instance:

Initial Installation

1. Create a new Zon installation.
2. Name the installation.

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

   Ensure that you have created the PostgreSQL database prior to installation. Refer to the "Installation Prerequisite" section above for additional information.
4. Identify a Single-Host or a Multiple-Host installation.
5. Provide the IP and hostname for the XML Router.

   This 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.
6. Provide the IP and the hostname for the Web Portal.
7. Provide the IP and the hostname of the Desktop/App Server.
8. Install a Zon Voice Bridge (optional).

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

Mailer Configuration (Optional)

The mailer is used to notify Zon 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.

Database Backup Configuration (Optional)

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

1. Identify the directory where the database backups will be stored.

   SiteScape recommends 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 will be kept.
3. Define when backups will be performed.

Meeting Archive Repository Configuration (Optional)

The Meeting Archive Repository is monitored daily at 4:00 a.m. to ensure that it has not reached a size of 2500MB. When the 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 will be 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 the meeting archive repository reaches the specified maximum.

To modify the default maintenance procedure:

1. Determine the repository maximum size. Set the repository size in MBs.
2. Identify the action to take if the meeting 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 time since accessed was set to 60 days, the automated clean up procedure would not delete archives that had 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.

Document Sharing Archive Repository Configuration (Optional)

The Document Sharing (DocShare) Archive Repository is monitored daily at 4:00 a.m. to ensure that it has not reached a size of 2500MB. When the repository exceeds 2500MB, archives that have not been accessed within the last 120 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 will be 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 the meeting archive repository reaches the specified maximum.

To modify the default maintenance procedure:

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:

   D. Determine the minimum target repository size after automatic clean up.

   E. Identify the minimum days-since-accessed that an archive can be deleted during the automated clean up procedure. For example, if the minimum time since accessed was set to 60 days, the automated clean up procedure would not delete archives that had been accessed within the past 60 days.

   F. Determine if the archives should be permanently deleted, or moved into another designated folder, which must be monitored manually by the system administrator.

Chat Audit Log Configuration (Optional)

Chat audit logging can be configured at system installation or reconfiguration time using the `install.sh` script.

1. The chat audit logs will be placed in `/var/iic/chatlog` on the hosts assigned to run the XML router and meeting controller(s). Zon IM and Zon 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. The participant ID is assigned to each meeting participant and is sent in meeting invitations.
`from_name`	String	The displayed name of the meeting participant who sent the chat message.

Field	Type	Description
`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 will be empty unless delivery is `ToOne`.
`to_name`	String	The displayed name of the meeting participant who received the chat message. This will be empty unless delivery is `ToOne`.
`message`	String	The contents of the chat message.

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. These logging levels can be modified at any time from the Administration Console:

- **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: SiteScape recommends 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 Zon 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 are occur so that they may be consumed by third-party systems (for example, a billing system or cost accounting system, management reporting systems or user directory database). The records are provided to event record consumers via a TCP connection to Zon server hosts.) Real time event logs are stored in the /`var/iic/cdr` directory.

   Note: Real-time event logging cannot be modified from the Administration Console. If you wish do not install real-time event logging during installation, you will need to re-run the installation script when you want to install real-time event logging.

Port Forwarding (Optional)

The Zon 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).

XML Router Security

In order for a Zon service (e.g. 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**”.

Template Configuration (Optional)

You can modify the e-mail templates that are used to communicate with Zon users. For additional information on the modification and configuration of these templates, refer to Chapter 4: Modifying Template Files.

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.

Summary of Configuration

Once you have completed the installation script, you will be presented with a summary of the choices you've 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 will be saved, and when you rerun the install script, will be used for the default values during the reconfiguration.

Zon Administration Console

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

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

Logging on to the Administration Console

The initial installation will create the screen name '**admin**' with password '**admin**'. You can use these values to log on, and change them later. Refer to the "Zon Operations Guide" for further information on using the Zon Administration Console

Creating Zon Communities

Refer to the "Zon Operations Guide" for information on adding Zon Communities.

Zon Client Installation

Install the client on a Windows machine by performing the following steps:

1. Download the Zon client on a Windows machine using the URL http://*webportalhostname*>/imidio/downloads/imidiolaunch.exe
2. Save the file `imidiolaunch.exe`.
3. Open the sitescape-zon directory
4. Run `imidiolaunch.exe` to install the client.

   Once the client is installed, you can use either the 'admin' screen name to sign on with the Zon client or you can use the screen name of the first user of the first community created earlier.

   Once you have signed on, you can add Zon users to the community. Refer to the "*Zon Operations Guide*" for information on adding users.

Chapter 3: Reconfiguring and Upgrading

The following section discusses both reconfiguration and upgrading the Zon servers and clients.

Backing Up and Restoring the Database

Before doing any reconfiguration or upgrade of the Zon 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 will be that of all committed transactions at the time `pg_dump(1)` is run. Any updates done after the backup is started will be 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`.

Reconfiguring Zon Hosts

Follow these steps to reconfigure the installation:

1. Make a backup copy of the sitescape-zon directory (e.g. `cp –r sitescape-zon sitescape-zon.bk`)
2. Open the sitescape-zon directory
3. Run: `./install.sh`
4. The installation script will prompt you for the configuration information. The prior configuration will be used as the default values for the new configuration.

You will also be 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 will result in all of the data being lost. Only initialize a database once on a database host.

Upgrading the Zon Client

Follow these steps to upgrade the Zon client:

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

Zon users will automatically be upgraded the next time they log on.

Upgrading the Zon Servers

Follow these steps to upgrade the Zon servers:

1. Make a backup copy of the sitescape-zon directory (e.g. `mv sitescape-zon sitescape-zon.bk`)
2. Extract the new distribution file using `tar zxvf sitescape-zon-<`*`version`*`>.tar.gz.`
3. Open the sitescape-zon directory
4. Copy the prior configuration directory to the current location (e.g. `cp –r ../sitescape-zon.bk/myzon`)
5. Run: `./install.sh`
6. The installation script will prompt you for the configuration information. The prior configuration will be used as the default values for the upgrade.

You will also be 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 will result in all of the data being lost. Only initialize a database once on a database host.

Starting and Stopping Zon Services

Starting and Stopping the Cluster

Zon services for the entire cluster may be started and stopped using the `control-cluster.sh` script described in the *Zon Installation Manual*.

To Stop Zon Services:

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

To Start Zon Services:

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

Use the `--single-host` argument to 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 Zon Services with `control-services.sh`:

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

To Start Zon Services with `control-services.sh`:

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

Chapter 4: Modifying Template Files

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

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.

Modifying the Meeting Invitation Template

The meeting invitation template has two roles. The first role is to fill the body of 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. An example of how to use this operation is:

```
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 echos. If the template designer wants a line break at a particular point, they 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. The following tags may be used:

Tag	Description
`<TITLE>`	This tag is replaced with the title of the meeting to which the participant is invited.
`<HOST>`	This tag is replaced with the host of the meeting to which the participant is invited.
`<TIME>`	This tag is replaced with the scheduled start time of the meeting to which the participant is invited.
`<DESCRIPTION>`	This tag is replaced with the description of the meeting to which the participant is invited.
`<MESSAGE>`	This tag is replaced with the invite message (if any) that the host provided when creating the meeting to which the participant is invited.
`<INVITEE-NAME>`	This tag is replaced with the name of the participant invited to the meeting.
`<INVITEE-PHONE>`	This tag is replaced with the phone number of the participant invited to the meeting.
`<INVITEE-PIN>`	This tag is replaced with the pin of the participant invited to the meeting.
`<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 to which the participant is invited.
`<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 to which the participant is invited.

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 a variable is 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.

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 tags are available:

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.

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 Zon. You can tailor the body of this e-mail by modifying the file `sitescape-zon/<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 tags available:

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.

Appendix A: Configuring `ssh(1)` private/public key authentication

The installation script will use ssh(1) and scp(1) to copy files to and execute scripts on the Zon hosts. In order to avoid typing the root password for the Zon 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) will get a authentication token generated using the private key. It will authenticate the token on the Zon host using the root user's list of authorized public keys.

Follow these steps to configure private/public key authentication:

1. Generate a private/public key pair.
2. Configure the ssh key agent to hold the private key for generating authentication tokens.
3. Add the public key to the list of authorized keys for the root user on the Zon hosts.

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 will be 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).

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 log back into the staging host. You will be prompted for the private key pass phrase entered when the key pair was generated. After successfully entering the pass phrase, the private key will be available for generating authentication tokens.

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 Zon 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 will need to repeat the above steps for all the Zon hosts.

Appendix B: Editing the `global-config` File

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

The overall cluster configuration is in the file `global-config`. The following steps are required to configure a Zon server cluster. A later section will describe optional configuration steps that you may wish to consider. You should review these optional steps, however.

Assigning Services to Nodes

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

1. Configure the database server

   G. Change the `db_host` variable assignment to specify the database host.

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

   I. Define the host access to the database. The servers that will 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 will specify a range of IP addresses that are allowed to connect to the database. For instance, 10.1.1.1/255.255.255.0 will allow 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

   A. Set `external_hname` to the hostname used by Zon clients to connect to XML router services.

   B. 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

   A. 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.

   B. 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.

   C. 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.

   D. Configure the voice bridge (s). Multiple voice bridges may be configured for scaling purposes.

      i. Specify the cluster host(s) and XML router listen ports by setting the voice_host array and the voice_host array.

      ii. 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".

      iii. Also, specify the phone numbers allocated to each bridge using the voice_phones array. Multiple phone numbers may be assigned to a single voice bridge by separating the phone numbers by 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")

   E. Configure the meeting archiver service (s). Multiple meeting archivers may be configured for scaling purposes.

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

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

   F. Configure the external API service.

      i. Specify the cluster host and XML router listen ports by setting the `extapi_host` and `extapi_port` arrays. Multiple external API hosts may be used.

4. Configure the app/desktop sharing servers

   A. Configure the `share_host` array to specify which hosts will run as app/desktop sharing servers. Note that multiple app/desktop servers may be run 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 two distinct IP addresses would need to be defined on *kanga* because both servers use port 80 for tunneling through firewalls.

   B. 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 Red Hat 9 service.

Configuring Web Services

The web portal for the system may be implemented across multiple hosts. When multiple web services are used 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 will be 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).

   A. Modify the `portal_hname_local` array to specify all the cluster hosts for web service.

   B. Ensure that `/usr/local/apache2/htdocs/repository/mtgarchive` is the same-shared file system for all cluster hosts in `portal_hname_local`.

   C. Modify the `portal_ip` array to include the IP addresses that the HTTP daemon should listen on for connections.

   D. Modify the `portal_hname` variable to define the hostname used in URL's to the web portal.

2. Configure external API host(s).

   A. Modify the `extapi_hname_local` array to specify all the cluster hosts for the external API service.

   B. Modify the `extapi_portal_ip` array to specify the IP addresses on which an external API HTTP daemon will listen.

   C. Modify the `extapi_portal_hname` to specify the hostname in URL's to the external API.

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 isn't the case for some reason, you can configure the mailer to use an external SMTP host for mail delivery. The variables `smtp_host, smtp_user` and `smtp_pswd` in `global-config` can be used for this purpose.

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.

Appendix C: Editing the `dialing.xml` File

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 to be dialed by the voice server. For example, default area codes that must be prepended 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` – Don't dial area code except for long distance calls. • `dialAreaCodeAlways` – The phone numbers will always have an area codes. 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>
```

Appendix D: Updating Meeting Invitation Web Pages

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 will have 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`

The body of the meeting invitation web pages can modified by updating `/usr/local/apache2/htdocs/imidio/invite/*.html`. Note that these files will not be saved after upgrades or reconfigurations.